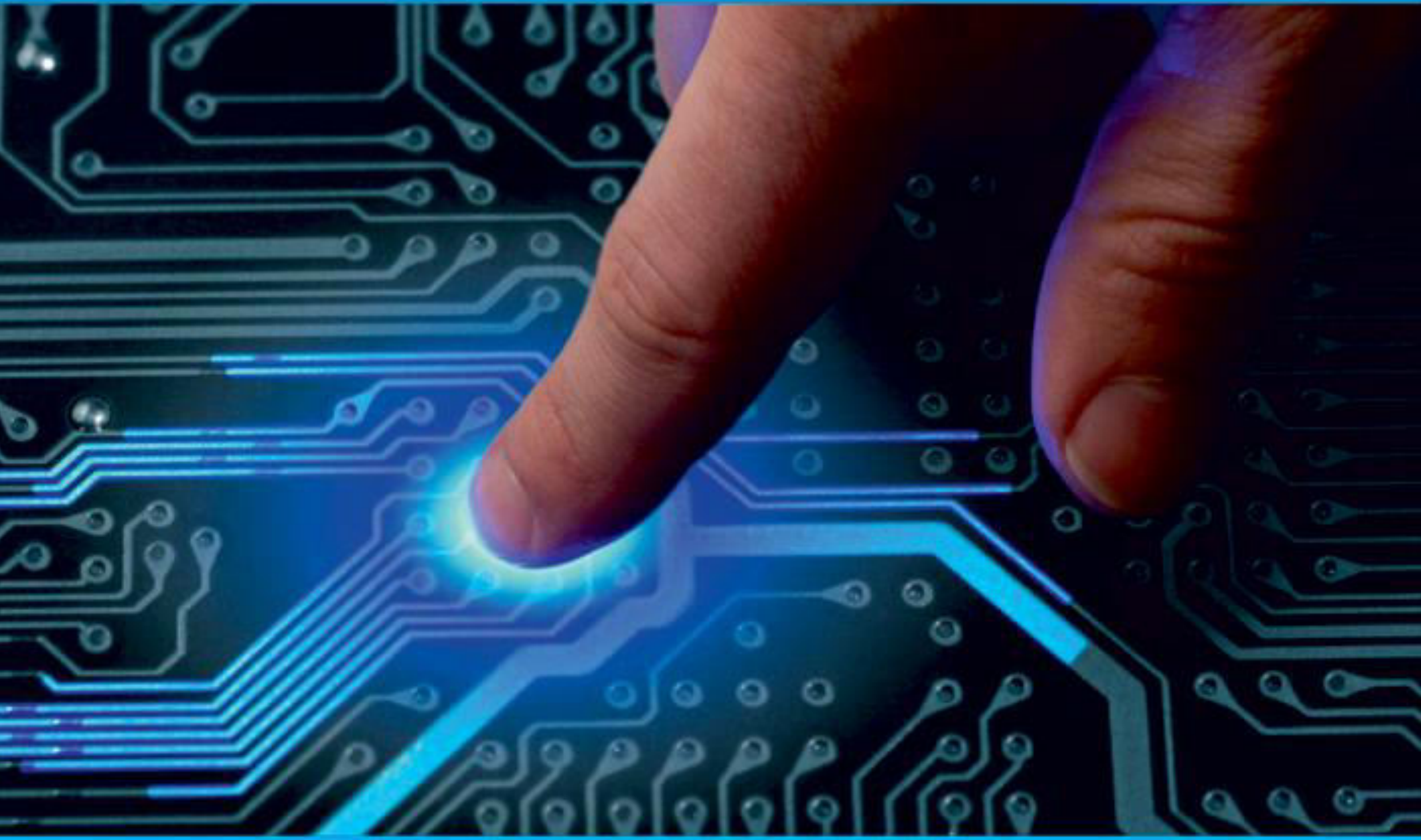
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006240|

Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract

Abhinav E, **Suriya Aakash V**, **Manikavasagan V**

U.G Scholar, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

U.G Scholar, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

Assistant Professor, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

ABSTRACT: In the Internet of Vehicles (IoV), vehicles com- municate wirelessly with other vehicles, sensors, pedestrians, and roadside units. IoV is aimed at improving road safety, driving comfort, and traffic efficiency. However, IoV is exposed to a range of threats to security and privacy. The presence of dishonest and misbehaving peers in the system is of a major concern, which may put lives in danger. Thus, establishing trust among these probable untrusted vehicles is one of the most significant challenges of such a network. The critical pitfalls of existing and traditional mechanisms are scalability, a single point of failure, maintaining the quality of service, verification, and revocation and dealing with sparsity, consistency, availability, efficiency, robustness, privacy concerns are some of the biggest challenges to be addressed. Blockchain technology, with its great success in applications like cryptocurrencies and smart contracts, is considered as one of the potential candidates to build trust in IoV. In this paper, we propose a blockchain-based decentralized trust management scheme using smart contracts. Specifically, we introduce the concept of blockchain sharding for reducing the load on the main blockchain and increasing the transaction throughput. Our proposal has two key contributions: blockchain to maintain and update reliable and consistent trust values across the network and incentive scheme to encourage peers to perform well. We also conduct extensive experiments, which demonstrate the implementation feasibility of proposed mechanisms in the real world.

I. INTRODUCTION

THE Internet-of-Vehicles (IoV) is now on the verge of deployment in the real world because of various advance- ments in radio access, core network, and automotive technologies . Vehicles nowadays are equipped with powerful sensors, communication, storage, and computational capabili- ties. The three main radio access technologies, which are being integrated with the vehicles are Dedicated Short Range Communication (DSRC), cellular and Wi-Fi .DSRC is the key radio technology used for vehicular communication in the USA and Europe [5]. Cooperative Intelligent Transportation Systems (C-ITS) [6] in Europe and Wireless Access in Vehicle Environments (WAVE) [7] in the USA are two well-known protocol stacks developed for vehicular communications and use DSRC at the physical layer [8]. IoV allows communication not only between Vehicle-to-Vehicle (V2V) but also between Vehicle-to-Infrastructure (V2I) and facilitates a variety of safety and non-safety applications. The safety applications can be of type collision warning, spot warning, intersection movement assistant, work-zone warning, etc. It also allows vehicles to share information about traffic and road condi- tions with their neighbors. The non-safety applications are mainly related to mobility (route guidance, traffic updates, navigation, etc.), and infotainment (streaming, VoIP, media download, etc.)

All the messages related to safety applications are broad- casted over the control channel (CCH) of the DSRC via V2V communication, which can be of type periodic bea- cons or event-based alarms. Cooperative Awareness Message (CAM) in Europe and Basic Safety Message (BSM) in the USA are the two popular safety messages which are broad-casted periodically for safety and awareness [10]. The decentralized environmental notification message (DENM) [11] is an event- driven message which is transmitted to notify some hazards or warning such as road accidents. In IoV, when a vehicle receives a DENM for some incident, it uses the information to avoid an unwanted situation such as accident, congestion, or some dangerous situation by effectively reacting to it. Consequently, the reliability and trustworthiness of the received messages are of paramount significance as the

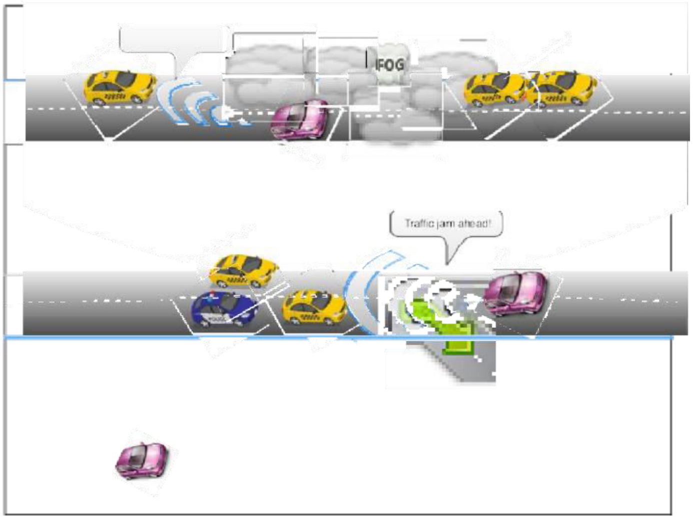


Fig. 1. Example scenarios of misbehavior in IoV.

system's acceptance and efficacy depend on them because they can affect driving decisions, and any wrong decision can have disastrous consequences.

Fig. 1 demonstrates misbehavior scenario in IoV. A mali- cious or misbehaving vehicle in low visibility conditions can send a fake message (using the protocol semantics) to other vehicles and conveys that the road ahead is clear while there is a road accident. Similarly, it can also generate a fake message claiming that there is traffic congestion ahead. Such misbehaviors can lead to catastrophic situations, reduce traffic efficiency, and as a whole lower the trust level on IoV.

Trust management in IoV implements the reputation of vehicles based on both the trust value scored from its past behavior (reputation) and neighbors opinion about the received message broadcasted by the alarmer vehicle for an event. Trust management can also facilitate incentives mechanism for the peers who behave well in the system and have earned a better trust score. There can be punishments forthe dishonest or misbehaving peers in terms of trust score reduction and revocation after a certain limit of misbehavioris crossed or defined threshold has been reached .

Different trust management systems proposed for IoV fall into the following two classifications: centralized and decentralized. There are a fair amount of works available in both categories, which are discussed in Section II. However, the key pitfalls of existing works in these categories are as follows. In the centralized approach, trust management is done on the central server; therefore, scalability, single point of failure, maintaining the quality of service, verification, and revocation are some of the most significant challenges. In the decentralized approach, trust management is performed either at the vehicular plane or the roadside unit (RSU) plane. However, dealing with sparsity, consistency, availability, efficiency, robustness, privacy concerns [13], and faults at the RSU plane remain open issues in the decentralized approach. The blockchain is one of the disruptive technology in the financial industry, first proposed as the underlying technology for

Bitcoin by Satoshi Nakamoto in 2008 [14]. Blockchain hasbecome one of the driving forces of industrial IoT or Industry 4.0 [15], [16]. It is attracting a lot of attention from indus- tries, academia, and research organizations. Its remarkable features such as high security (Merkel tree, hash function), decentralization, consensus (Proof of Work (PoW)), consis- tency, and reliability make it one of the potential candidates for establishing and managing the trust model in IoV [17].

In the literature (Section II), there are blockchain-based works proposed for solving trust management and privacy-related issues in IoV. However, addressing the scalability issue of the blockchain used remains a significant concern while implementing it in IoV. Our work is an extension of existing work, where we introduce the concept of sharing to solvethe scalability problem while managing trust in the IoV. Our framework is adaptive because it can be integrated with various existing misbehavior detection strategies (discussed in the literature) for trust management and also establish the process of revocation of misbehaving vehicles in IoV.

In this paper, we propose a blockchain-based decentralized trust management system for IoV. The primary goal of the proposed mechanism is effective trust establishment and man- agement in a distributed fashion. The main contributions of this paper are as follows:

We propose a scheme for trust management at the edge, i.e., at the roadside units (RSU) plane of IoV, which is decentralized in nature and based on the blockchain technology. RSUs at the edge collaboratively maintain vehicle trust values that are updated, reliable, and consistent, helping to accomplish our objective in a decentralized manner.

We incorporate the idea of shards for reducing the work- loads from the main maintained blockchain. We use an open-source platform, Ethereum block- chain [18], that facilitates smart contracts to demonstrate the feasibility of implementation and strength of our proposed decentralized trust management strategy. The outline of the rest of the paper is as follows. Section II present the survey on various techniques of trust management used in a vehicular network. Section III presents the detail of the system framework consisting of the architecture and system model. In Section IV, we discuss the details of our basics of the blockchain platform of trust management in IoV. Experiment details, case study algorithms are present in Section
The obtained results and discussion about it are present in Section VI. Finally, Section VII presents the final conclusion.

II. SYSTEM MODEL

We formalize the IoV architecture in this section and discuss the key entities of the system.
Architecture
Fig. 3 shows the IoV architecture having three vital planes [45]: vehicular plane, set of RSUs as Edge Computing plane (to facilitate blockchain), and central services plane. Thecentral services plane includes certificate authority (CA), ITS services, Internet services, cloud-based services [46], etc.
Key Entities

Roadside Units (RSUs):
In our proposed scheme, we considered the flourished stage of IoV, where RSUs are equipped with powerful computing and storage capacity, reliable and secured backhaul links to service plane, sensors, and secure wireless communication technologies for V2I/I2V con- nectivity. We can refer to it as the edge node, which can facilitate required caching, storage, communication, and computation to our proposed blockchain-based mecha- nism. It is also responsible for updating vehicle categories based on their sensing capacity, profile, and past behavior.

Vehicles: Vehicles in the IoV are equipped with an on- board unit (OBU) that runs WAVE protocol stacks for vehicular communication. OBUs of the vehicles have communication, computation, storage, and navigation capabilities. We call them intelligent vehicles.

Traffic Authority (TA): TA is the supreme authority and plays a crucial role in IoV as doing the registration of the vehicles and deployment of the Regional Authorities. TA collects the information from the vehicles and issues them certificates via the Certificate Authority. It also assigns initial trust value to the registered vehicles.In any system, there is always a hierarchy of trust levels. Vehicles can earn trust value by performing well. Vehicles who behave badly in the network are put into the Misbehaving Vehicle (MV) category.

Certificate Authority (CA): CA uses the collected credentials and information of the vehicles by the TA registration and issues them certificates (certified keys) for communications security and privacy. The role of CAis defined in detail in [47].

Regional Authority: The entire vehicular environment is divided into a number of regions based upon the geo-locations. RA works in accordance with the TA and is responsible for deploying and maintaining the infrastructure in its territory. RA is also responsible for providing vehicles entering its territory with a set of short term keys for communications within the territory.
Note: The trust value is dynamic and may increase or decrease based on their behavior in the network.

III. FRAMEWORK FOR TRUST MANAGEMENT

Vehicles at the vehicular plane participate in a number of events at the vehicular plane. For each event, a vehicle exchanges a number of messages with its peers. A vehicle checks for the integrity and authenticity of each message received for an event. If any inconsistencies in the messages are detected, it is reported to the RSU for action. The RSUsare edge nodes in our IoV framework and are capable of running a distributed consensus of blockchain for trust man- agement. Based on the smart contract logic that we deployed, RSUs execute the operation and update the trust score of vehicles depending on their behavior. More details about the mechanism, platform, implementation are given in subsequent sections.

Blockchain Platform for Trust Management

A blockchain is a decentralized, distributed, unalterable,and append-only ledger that guarantees transparency in the chain's transactions. Blockchain can be used as a platform to build trust among untrusted parties. It facilitates storing the state in a distributed fashion among nodes of the network and continues to exist as long as a network of nodes exists [48]. We propose a decentralized system for trust management inIoV, taking into account the core concepts of the blockchain. The core contribution of our work is designing, implementing, and evaluating an application using smart contracts for trust management in IoV. Before providing details of implementa- tion, we provide an abstract overview of the smart contract, and ethereum platform and discuss some key features of the blockchain.

Sharding in Blockchain

The current blockchain-based system with Proof-of-Work as the consensus mechanism faces the problem of scalability. The two most popular public blockchain platform Bitcoin and Ethereum has an average transaction throughput of 8 txps(transactions per second) and 15 txps, respectively. In contrast, its counterpart VISA offers transaction throughputof around 1700 txps. Blockchain sharding is an upcom- ing blockchain research domain that aims at improving the blockchain scalability in terms of transaction throughput by dividing the transaction loads on the full blockchain into several sub blockchains where each sub blockchain main- tains a localized set of transactions. In blockchain sharding,the entire blockchain network is divided into some shards.A shard is a sub blockchain maintained by a subset of nodes, also known as the committees from the global blockchain network. Each shard collects and processes a disjoint set of transactions. A shard is maintained by a committee of k members. Generally, k is significantly small in number as compared to the participants in the global blockchain network.Having a smaller k facilitates to execute BFT based consen- sus algorithms; however, challenge-response based consensus algorithms can also be used here. Smaller k also facilitates better use of network bandwidth for propagating the blocks as the committee members are mostly localized.

Smart Contract

A smart contract is a component of blockchain 2.0 that extends the capability of the earlier use-case specific blockchain, by allowing code snippets defining business logic to be deployed on top of the blockchain. The smart contract ensures fraud-free contract execution without any trusted third party. It is a programmed logic having a predefined set of rules [49]. It enables users to execute a script in a verifiable manner on a blockchain network and enables several issuesto be solved in a way that minimizes the need for trust. In essence, smart contract functions as an autonomous entity on the blockchain and can execute logic deterministically asa function of the data provided to the blockchain.

Ethereum Platform

Ethereum is an open-source blockchain platform that sup- ports smart contracts. The platform facilitates the use of various programming languages to write the smart contract [18]. These smarts contracts can be converted into bytecode andare executed on Ethereum Virtual Machine (EVM). Ethereum facilitates the execution of its private and permissioned blockchain instance. In such an instance, only peers that are allowed to enter the network can view transaction data. Among those, only nodes that are granted special rights can participate in the mining.

Ethereum Blockchain Accounts: An entity holding an internal state is associated with an account in Ethereum. Ethereum distinguishes between two kinds of accounts, accounts owned externally and contract accounts. An externally owned account contains a private key making it a personal account. The key owner can send transactions to otherexternally held accounts or contract accounts from his/her account.

Features

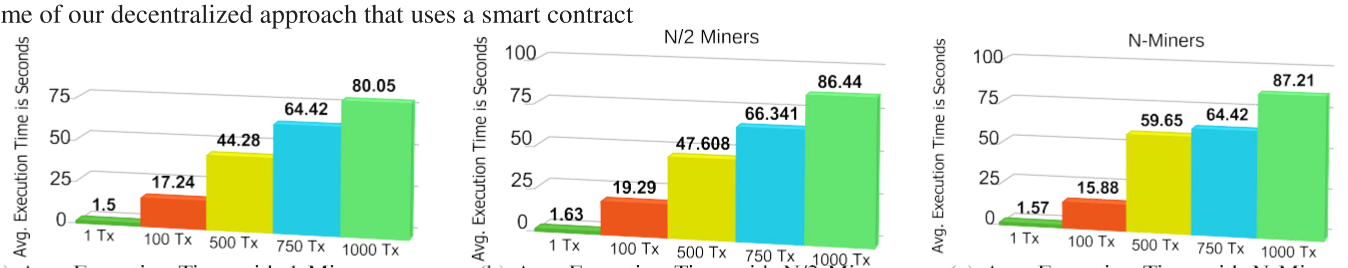
Decentralization: Decentralization is one of the primary objectives of blockchain technology. Blockchain inherently keeps its data stored in multiple copies over multiple geo- graphical locations making it highly available and lowering any successful attempts to the modification of on chained data.It will require a malicious entity to have a hold on at least 51%of computing power in the blockchain network to execute a data alteration attempt successfully .

Irreversibility and Immutability: Transactions once recorded in the blockchain cannot be reversed. The immutabil- ity property of the transactions recorded on the chain increases with each successive block being added in the chain. Once committed, the transactions can not be altered.

Digital Signature: Digital Signature is a facility provided by Public Key Infrastructure(PKI) that allows a party to prove the authenticity of data. Data is digitally signed by the sender party with their private key and is verified by the receiving party by the globally available public key of the sender. Each transaction in the blockchain network is digitally signed by the executor's private key and is verified by the miners with the available executor's public key ensuring non-repudiation against the execution of the transaction. The elliptic curve digital signature algorithm (ECDSA) is the standard algorithm used in blockchain .IoV. The maintenance and control of a territory's infrastruc-ture is the exclusive responsibility of the Regional

IV. RESULTS AND DISCUSSION

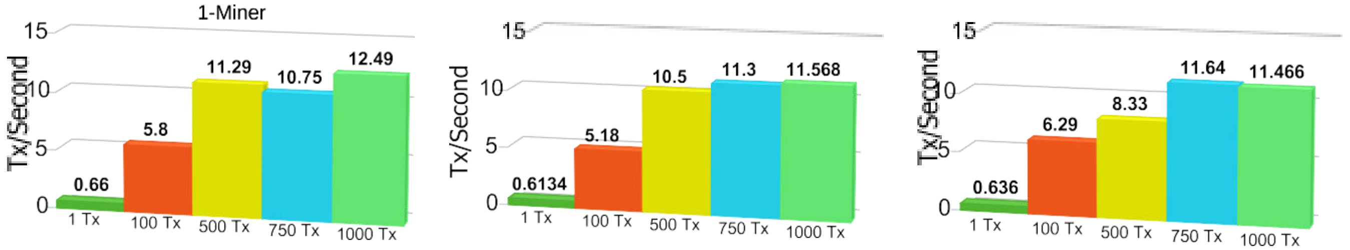
The performance of the blockchain testbed is presented in this section. We show the average throughput and execution time of our decentralized approach that uses a smart contract



(a) Avg. Execution Time with 1-Miner (b) Avg. Execution Time with N/2 Miners (c) Avg. Execution Time with N Miners

N/2Miners
N-Miners

Fig. 9. Avg. execution time performance.



(a) Avg. Throughput with 1-Miner (b) Avg. Throughput with N/2 Miners (c) Avg. Throughput with N Miners

Fig. 10. Average throughput performance.

1-Miner
100

on Ethereum Blockchain for trust management at RSU plane of IoV.

A. Performance Evaluation of Blockchain Framework
Values collected for each transaction in order to assess the performance of our configured private blockchain are as follows. Transaction (Tx) Deployment Time (t1): Unix time when transactions were deployed. Transaction (Tx) Comple- tion Time (t2): Unix time when the blockchain confirmed transactions. The transaction completion time was collected through web3.js APIs that returns transaction details.
We choose transaction execution time and throughput as parameters for evaluating our set up the private blockchain.

Execution Time: The execution time is the total amount of time (seconds) during which all transactions in the dataset were executed and confirmed by the blockchain. It is the dura-tion of time elapsed when the first transaction was deployedto the time when the last transaction is mined.

Throughput: It is defined as the number of successful transactions per second from the first deployment time of the transaction. Average throughput is the average over execution time.

Comparing Average Execution Time: The performance is compared to the differences in execution time of vary-ing transactions with three distinct sets of miners: 1, N/2, and N
(in our case, N 4), as =shown in Fig. 9a, Fig. 9b,and Fig. 9c, respectively. The execution time grows as the number of transactions in the dataset increases. For a batchof 1000 transactions, the blockchain takes 80.05, 86.44, and
87.21 seconds with 1, N/2 and N miners.

Comparing Average Throughput: Fig. 10a, Fig. 10b, and Fig. 10c shows the average throughput plot for varying sets of transactions with 1, N/2, and N miners, respectively. For a batch of 1000 transactions, the average throughput is found to be 12.49, 11.568, 11.466. Besides, one can see that as the number of transactions in a set increases, the rate of throughput increase decreases. Thus, for a huge set of transactions, the average throughput will become some constant value.

Discussion: As we can see from the average execution time plot and the average throughput plot, increasing the number of miner nodes does not have a significant impact on improving system performance. However, an increased number of miner nodes will definitely help in making the system decentralized in a true manner, which comes at the cost of higher power consumption.

What We Achieved?: Through our proposed mechanism for trust management using blockchain, we achieved the following goals.

Encourage to behave well: We introduced an incentive mechanism for vehicles behaving well and helping in detection of misbehavior and reporting of true informa- tion to RSU. The incentives scored can be redeemedfor various services such as insurance premiums, main- tenance, etc.

Revocation: Authorized peers who misbehave continu- ously will lose their reputation in terms of trust score and will eventually be removed from the system. However, the TA can do the root cause analysis for misbehavior, and if it finds that it was intentional, then appropriate action must be taken.

Decentralized Approach: In the proposed mechanism, most of the tasks such as verification, computation, result calculation, proof of work, mining, etc. are done at the edge level of IoV in a decentralized manner, i.e., in a distributed fashion at the RSU plane. This approach will minimize the delay incurred in communication between vehicle and CA or TA, maximize scalability, reliability, and can deal with fault tolerance.

Consistency: The distributed RSUs executing blockchain technology maintains a consistent trust database. Any changes made in the database at any RSU propagated across all other RSUs via the blockchain in the network.
Availability: The consistent information about the trust and its reward is always available at the edge of the IoV. Vehicles requesting that information can easily access them.

V. CONCLUSION

In this paper, we proposed mechanisms that manage trust using blockchain in IoV. We have provided a survey of existing works available in this increasingly important area. We proposed a blockchain-based decentralized approach in which CA/TA deployed the smart contract, and all RSUs workin a distributed manner to maintain consistent vehicular trust database and enhance reliability, availability, and consistency. We introduced the idea of maintaining sharded blockchains, that will not only reduce the propagation delay of transactions but will also increase the throughput and efficiency of the entire system. We also introduced incentive strategy for the vehicles participating in event detection, i.e., their contribution in the detection of a true event and its accurate reportinghelps them to get rewards, which they can redeem for various services and payments. The proposed incentive mechanism encourages participating peers to perform well and get wallet points. However, if they do not perform well, they can be revoked from the system. We demonstrated the performance of our framework in terms of average throughput and execution time by deploying the private blockchain on the testbed, thus demonstrating its feasibility.
In this work, we have not considered the misbehavior detection and local detection checks using plausibility fac- tors, filters, consistency (position, speed, heading), beacon frequency, etc. at the vehicular plane of IoV. As future work, we will try to integrate the misbehavior detection processand the privacy part. We will look for the role of AI in the misbehavior detection and efficient consensus algorithms in the RSU plane of IoV for decentralized trust management.

VI. ACKNOWLEDGMENT

The authors would also like to thank the editorial team and all the anonymous reviewers for their valuable suggestions and comments, which helped to improve the quality of the work.

REFERENCES

1. K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRCand cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.
2. F. Chiti, R. Fantacci, Y. Gu, and Z. Han, "Content sharing in Internet of vehicles: Two matching-based user-association approaches," *Veh. Commun.*, vol. 8, pp. 35–44, Apr. 2017.
3. H. D. Abdulkarim and H. Sarhang, "Normalizing RSS values of Wi-Fi access points to improve an integrated indoors smartphone positioning solutions," in *Proc. Int. Eng. Conf. (IEC)*, Jun. 2019, pp. 171–176.
4. H. S. Maghdid, A. Al-Sherbaz, N. Aljawad, and I. A. Lami, "UNILS: Unconstrained indoors localization scheme based on cooperative smart- phones networking with onboard inertial, Bluetooth and GNSS devices," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2016, pp. 129–136.
5. Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys & Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart., 2008.
6. C. Campolo, A. Molinaro, and R. Scopigno, "From today's VANETs to tomorrow's planning and the bets for the day after," *Veh. Commun.*, vol. 2, no. 3, pp. 158–171, Jul. 2015.
7. R. A. Uzcategui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 126–133, May 2009.
8. K. Z. Ghafoor, M. Guizani, L. Kong, H. S. Maghdid, and K. F. Jasim, "Enabling efficient coexistence of DSRC and C-V2X in vehicular networks," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 134–140, Apr. 2020.
9. G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.
10. A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.
11. *Intelligent Transport Systems (ITS); Vehicular communications; GeoNet- working; Basic Set of Applications; Part 3: Specifications of Decentral- ized Environmental Notification Basic Service*, Standard TS 102 637-3, ETSI, Tech. Spec., Sep. 2010.
12. J. Zhang, "Trust management for VANETs: Challenges, desired proper- ties and future directions," *Int. J.*
13. *Distrib. Syst. Technol.*, vol. 3, no. 1, pp. 48–62, Jan. 2012.
14. P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location pri- vacy in VANETs," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no.
15. 100183.
16. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"
17. Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
18. J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.
19. J. Huang *et al.*, "Blockchain based mobile crowd sensing in industrial systems," *IEEE Trans. Ind. Informat.*, to be published, Jan. 3, 2020, doi: 10.1109/TII.2019.2963728.
20. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
21. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.
22. S. A. Soleymani *et al.*, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 146, Dec. 2015.
23. F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in vehi- cles: A set of evaluation criteria for trust management in vehicular ad- hoc network," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Com- put. (CPSCom) IEEE Smart Data*
24. *(SmartData)*, Jun. 2017, pp. 44–52.
25. M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data- centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1238–1246.
26. N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, p. 9, Dec. 2009.
27. Wu, J. Ma, and S. Zhang, "RATE: A RSU-aided scheme for data- centric trust establishment in
28. VANETs," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2011, pp. 1–6.
29. S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information- oriented trustworthiness J. Kamel, F. Haidar, I. B. Jemaa, A. Kaiser, B. Lonc, and P. Urien, "A misbehavior authority system for Sybil attack detection in C-ITS," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf.*

30. *(UEMCON)*, New York, NY, USA, 2019, pp. 1117–1123, doi: 10.1109/UEMCON47517.2019.8993045.
31. U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.
32. F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, May 2012.
33. U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," *Proc. Comput. Sci.*, vol. 46, pp. 965–972, Jan. 2015.
34. X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reli- able data acquisition in

BIOGRAPHY

Abhinav E is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on Adaptive Trust Management inInternet of Vehicles Using Smart Contract.

Suriya Aakash V is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on Adaptive Trust Management in Internet of Vehicles Using Smart Contract.

Manikavasagan M.E, is Assistant Professor of Computer Science and Engineering Department in Velammal Institue of Technology, Panchetti.

.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com