JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

"Comparing Consensus in Vehicular Ad Hoc Networks : An Analytical Review"

[1]Devang Borkar [2]Param Chaudhari, [3]Sagar Khedekar, [4]Suhasini Itkar

Department of Computer Engineering, Progressive Education Society's
Modern College of Engineering, Shivajinagar, Pune, 411005,
Maharashtra, India.

Abstract : The aim of this study is to provide a comprehensive review of the blockchain technology and its application in vehicular ad hoc networks (VANETs). This study not only provides a comprehensive overview of the blockchain technology and its application in VANETs, but also presents a historical account of the evolution of VANETs, from their inception to recent advancements, thereby providing a contextual framework for understanding the current state-of-the-art in this domain. This paper addresses the usage of different consensus mechanisms in the context of VANETs. It also makes comparisons between them based on the advantages that they offer, along with their downsides. The paper also explores the integration of blockchain applications in the Internet of Vehicles (IoV) and identifies open issues for future research. This study aims to summarize the advances in Vehicular Communication Systems using the decentralized communication model of blockchain.

***Index Terms* - Vehicular Ad Hoc Networks, Blockchain technology, Consensus Mechanism, Microtransaction, Software Defined Networks**

I.INTRODUCTION

This paper addresses the usage of different consensus mechanisms in the context ofVANETs. It also makes comparisons between them based on the advantages that they offer, along with their downsides. Modern automobiles are equipped with software and hardware infrastructure, allowing them to communicate with each other and interact with their surroundings. Such vehicles are able to establish a network consisting of Vehicle to Vehicle (V2V) as well as Vehicle to Infrastructure (V2I) communication, forming a spontaneous ad hoc network called Vehicular Ad-Hoc Network (VANET). A VANET is a type of Mobile Ad-Hoc network (MANET) in which the vehicles communicate with each other and with roadside infrastructure. IEEE 802.11p has introduced Wireless Access for Vehicular Environments(WAVE) through On Board Units (OBU), Global Positioning System (GPS) receivers, Dedicated-Short Range Communications (DSRC) modules, and sensing capabilities, thus enabling Vehicle to Everything (V2X) communication. VANETs provide many serviceable applications like driver assistance and transport safety. It is designed for the network nodes that are constantly in motion and are supported by a road-side infrastructure.

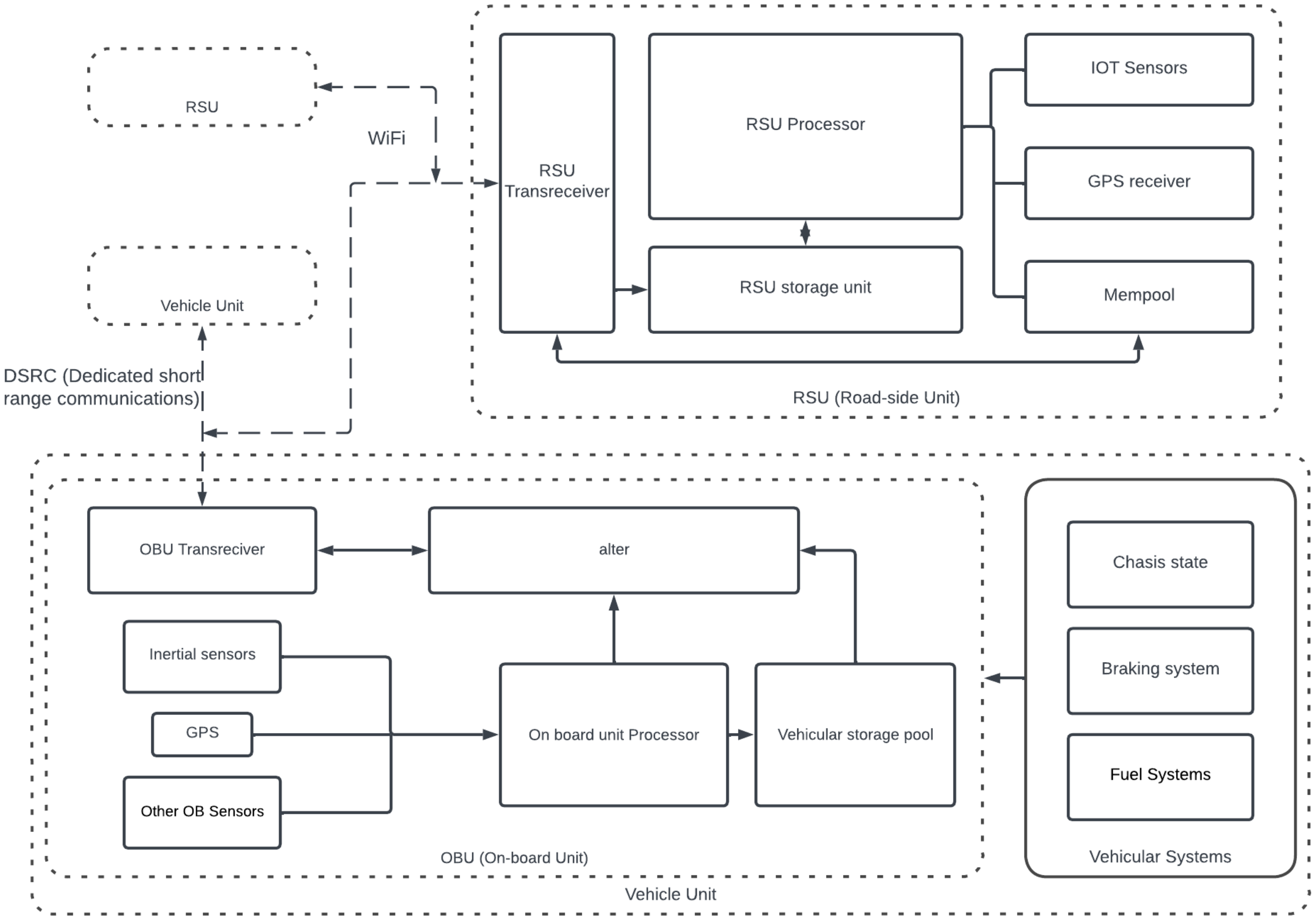

Fig. 1 Architecture of Vehicles and RSU part of the network

Vehicular-Cloud makes use of distributed computing resources to bring the benefits of cloud computing to vehicular networks. Utilizing a Network-As-A-Service (NAAS) model [1], it creates a highly adaptive and flexible ad-hoc network, where traffic-related data can be efficiently stored in the cloud, thereby enabling cost-effective scalability and ensuring seamless access to computing resources .However the significant drawback of Vehicular-Cloud is the issue of data security, as a compromised node can potentially result in unauthorized access to sensitive user information or even data tampering, posing a significant threat to the integrity and confidentiality of the system. Software Defined Networking (SDN) represents a model framework that fundamentally transforms the way networks are managed and controlled. By separating the control plane from the data forwarding functions, SDN provides a secure and efficient means of managing communication throughout the network. The integration of the SDN framework into Vehicular Communication Systems[2] enables centralized management of data transmission, making it possible to detect network intrusions and track malicious nodes through the use of the OpenFlow Protocol. However, a potential drawback of this approach is the creation of a Single Point of Failure (SPoF), as the SDN controller assumes the critical responsibility of defining the network's rules and routing protocols.

In a traditional VANET architecture, security and privacy are the major concerns. The decentralized and trustless nature of Blockchain technology can be taken advantage of in order to tackle these issues. Blockchain technology, which is based on distributed ledger technology (DT), is a major shift from the existing trust model which requires a trusted central authority. Thus, the decentralized, blockchain-enabled architecture for VANETs helps to achieve the efficient collaboration of entities, such as vehicles and RSUs, whilst preserving privacy and security.

II. BACKGROUND KNOWLEDGE

Various studies, research and surveys have been conducted on the optimization of Vehicular AdHoc Networks. We have grouped these studies together and referenced them in the forthcoming section. [3] introduces the concept of Cooperative Collison Avoidance through DSRC architecture and its implementation requirements in the context of a high speed wireless communication network. The term Vehicular Adhoc Network was coined where the network is self-organizing and adaptive[4] laying the foundation for Intelligent Transport Systems.[5] touches upon the topic of localization in VANETs without the presence of GPS data. It further elaborates how smartphone sensors and the information shared by neighboring vehicles with undetermined locations can be utilized in order to allow vehicles to improve or estimate their position. In [6],authors introduced a blockchain-based architecture designed to preserve both identity and location privacy in VANETs, outperforming traditional centralized implementations in terms of efficiency and efficacy. The authors in [7] have put forth a novel data structure Merkle Patricia Tree to enhance the conventional blockchain structure in a blockchain based privacy preserving authentication scheme(BPPA) for VANETs. The concept of edge computing, as presented in [8], seeks to revolutionize the current data processing paradigm by addressing a critical challenge - the overburden on data transmission. By shifting the processing to the end nodes, this proposal seeks to mitigate the transmission strain and enable real-time processing of data. Furthermore, the integration of a consortium blockchain[9] adds an additional layer of security and reliability to the system, ensuring a high level of data protection through tamper-proof storage and management. [10]

Describes the concepts of micropayments, microtransaction, Ethereum smart contracts, and proposes a model on how the Proof of Stake (POS) consensus can be conducted. Furthermore, it states the benefits and limitations of the proposed model.

[11] states the architecture for road traffic events management in Vehicular Adhoc NETworks (VANETs) which makes use of a permissioned blockchain. It describes how a permissioned blockchain can help in reducing the cyber attacks and enhance Quality of Service (QoS) without affecting the integrity of the data. It also describes the concept of microtransactions to minimize the problems related to data storage and communication. It also talks about the integrity, traceability, simulation results and limitations of the proposed architecture.

This comprehensive review delves into the utilization of diverse consensus mechanisms in permissioned and permissionless blockchain in order to make comparisons between them on the basis of efficiency and data security while preserving the trustless nature of blockchain networks. Rather than using a centralized cloud-based architecture for transactions, this study explores the benefits of performing computation at the end nodes and further analyzes the implementation of microtransactions aimed at alleviating the burden of data transmission and providing better scalability. This study also explores the benefits of performing computation at the end nodes instead of using a centralized cloud-based architecture and further analyzes the implementation of microtransactions aimed at alleviating the burden of data transmission and providing better scalability.

III. METHODOLOGY

3.1 Vehicular Communication Systems

Vehicular Communication architectures enable the vehicles in a network to communicate with each other and with the surrounding environment to achieve cooperative collision avoidance, traffic management, infotainment systems and many other benefits through real time data sharing[12]. Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) data sharing are critical components of Intelligent Transportation Systems (ITS), enabling the development of a comprehensive and effective communication system.

3.2 IEEE 802.11p

The IEEE 802.11p provides a communication standard - Wireless Access for Vehicular Environments(WAVE) specifying protocols for data transfer through Digital Short Range Communication(DSRC) modules[13]. A WAVE Beacon Service Set(BSS) is introduced where the BSS is available at all times to reduce the connection overhead which allows instantaneous data exchange proving crucial for safety related applications.

3.3 AdHoc Networks

Ad hoc refers to actions that are taken temporarily or rapidly. An ad hoc network does not depend on any pre existing infrastructure and is decentralized in nature. Here, each node in the network participates in the routing process by forwarding data for other nodes. The decision of which nodes forward data is made dynamically, based on the connectivity of the network. All devices in an ad hoc network have equal status and are free to connect with any other ad hoc network devices in link range.

3.4 VANETs

Vehicular ad-hoc network (VANET) is a subcategory of MANET (Mobile ad-hoc network). It is designed for the network nodes that are constantly in motion and are supported by a road-side infrastructure. In VANETs, the vehicles act as mobile nodes. A VANET consists of a network of vehicles which have the ability to communicate among themselves, thus enabling them to share important traffic-related data with each other. The use of VANETs has several advantages, including security, privacy, and ease of communication.

3.5 SDN Based VANETs

The main idea behind Software Defined Networking(SDN) is the separation of control planes from the information plane to easily manage the traffic flow within the network[14] by using programmable controllers. In SDN based VANETs the controller is used to manage the routing, flow control and access control of Safety Beacon Messages(SBM).

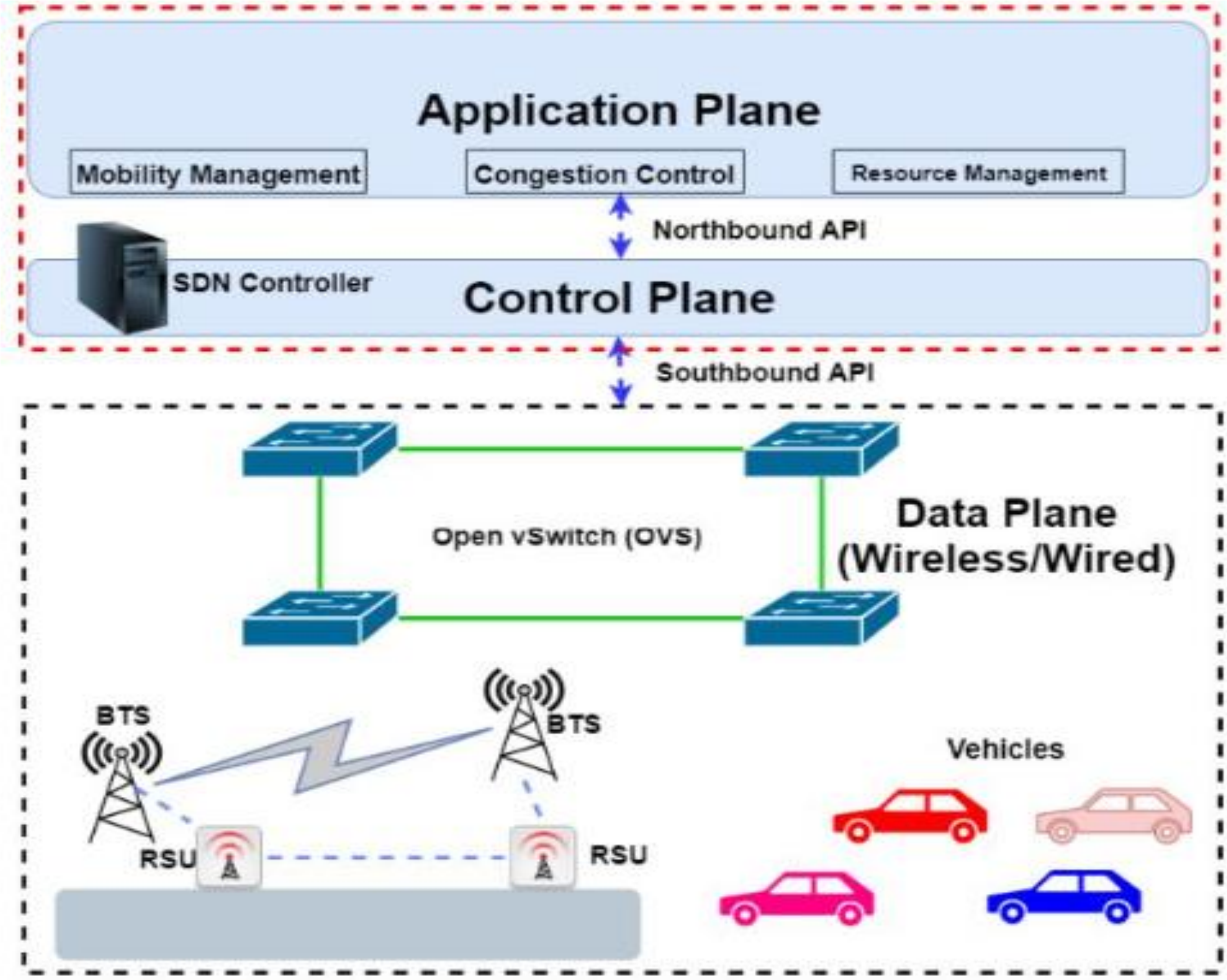

Fig. 2 SD-VANET Framework

[15] proposes a VANET based architecture coupled with fog computing where the SDN controller is operated in a hybrid manner connected with Base Stations(BS) and Road Side Unit Centres(RSUC) via a wireless medium to improve the load balancing techniques and reduce latency.

3.6 Blockchain Technology

Blockchain technology is a safe immutable ledger which facilitates transparent transactions without any dependence on the third party. It is also called distributed ledger technology. Blockchain can be termed as a distributed database of records which stores data in a block which is linked to a previous block by a cryptographic hash forming an immutable decentralized network. It keeps a transparent history of records between two or more organizations or individuals working together which do not trust each other.

3.7 Blockchain Based VANETs

Blockchain based VANETS are Vehicular networks operating in a large scale decentralized environment. This distributed network enables sharing of necessary services, records and data in V2V and V2I networks. [16]Vehicles participating in the VANET are well equipped with the necessary infrastructure i.e. GPS, DSRC radios, smart sensors etc to interact in the Ad Hoc network. Other components include entities such as Certifying Authority(CA) and Road Side Units (RSUs) which are equipped with necessary receivers and transmitters along with adequate data storage capacity. Thus, such decentralized VANETS ensure the secure and efficient data transmission throughout the network with minimizing the risk of data modification or any malicious attacks on the network.

3.8 Comparing Consensus

Blockchains are self-governed and operate in a trustless manner where there exists only one true state of the ledger. A consensus provides a reliable, fair, real-time, efficient and transparent mechanism to ensure that transactions are fair and genuine.
Whenever a new block is added to the blockchain, who adds it is defined with the help of a consensus mechanism. This section compares the use of different consensus mechanisms in Vehicular Networks.

3.8.1 Proof of Work(PoW)

PoW is the first consensus mechanism introduced in 2009 [17] where the transaction data is validated by having nodes compete with each other to solve a complicated mathematical problem using powerful computers. The node which solves the problem first is elected to add the transaction in the block and is issued a reward for its efforts that ensures the integrity of the blockchain. [18] provides a methodology for implementing Proof of Work consensus in VANETs where the Road Side Units(RSU) act as nodes and perform validation on the data shared by vehicles and add it to the blockchain.

However, PoW requires entire blockchain history replication on each node being unviable for Vehicular Social Networks as enormous amounts of data is generated by vehicles therefore [19] put forth a lightweight blockchain for resource constrained Vehicular Social Networks using Directed Acyclic Graph(DAG) where the redundant historical data is pruned to improve the scalability and availability of the network.

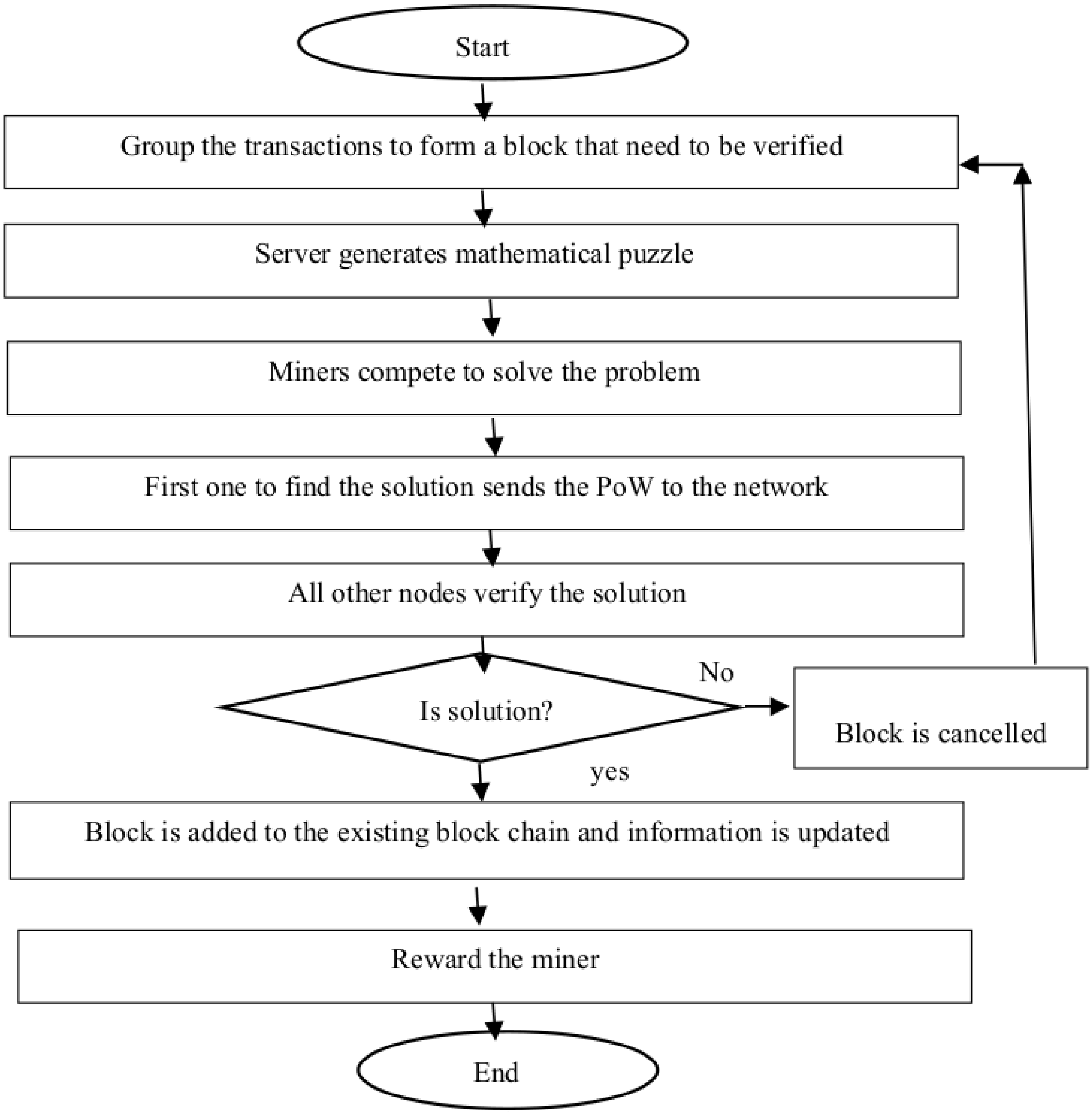
Start
Group the transactions to form a block that need to be verified
Server generates mathematical puzzle
Miners compete to solve the problem
First one to find the solution sends the PoW to the network
All other nodes verify the solution
Is solution?
No
Block is cancelled
yes
Block is added to the existing block chain and information is updated
Reward the miner
End

Fig. 3 Working of Proof of Work Consensus

3.8.2 Proof of Stake

Proof of Stake(PoS) is a consensus protocol which was designed as an alternative to Proof of Work (PoW) algorithm which eliminates the potential drawbacks i.e. high computation power and high energy usage of the Proof of Work (PoW).In PoS one random node from the VANET is selected and validators of the node are elected on the basis of no. of tokens or quantity of stake they are holding. More the no. of tokens they hold, more is the chance of being elected as a validator. Thus the network will be validated by one single node which has the highest tokens in it. Validators get some fees as a reward for validating the node. In VANETs RSU and vehicles can act as a node considering the VANET as the network. Thus, RSU with the maximum votes(tokens) will win and act as a validator for the network.

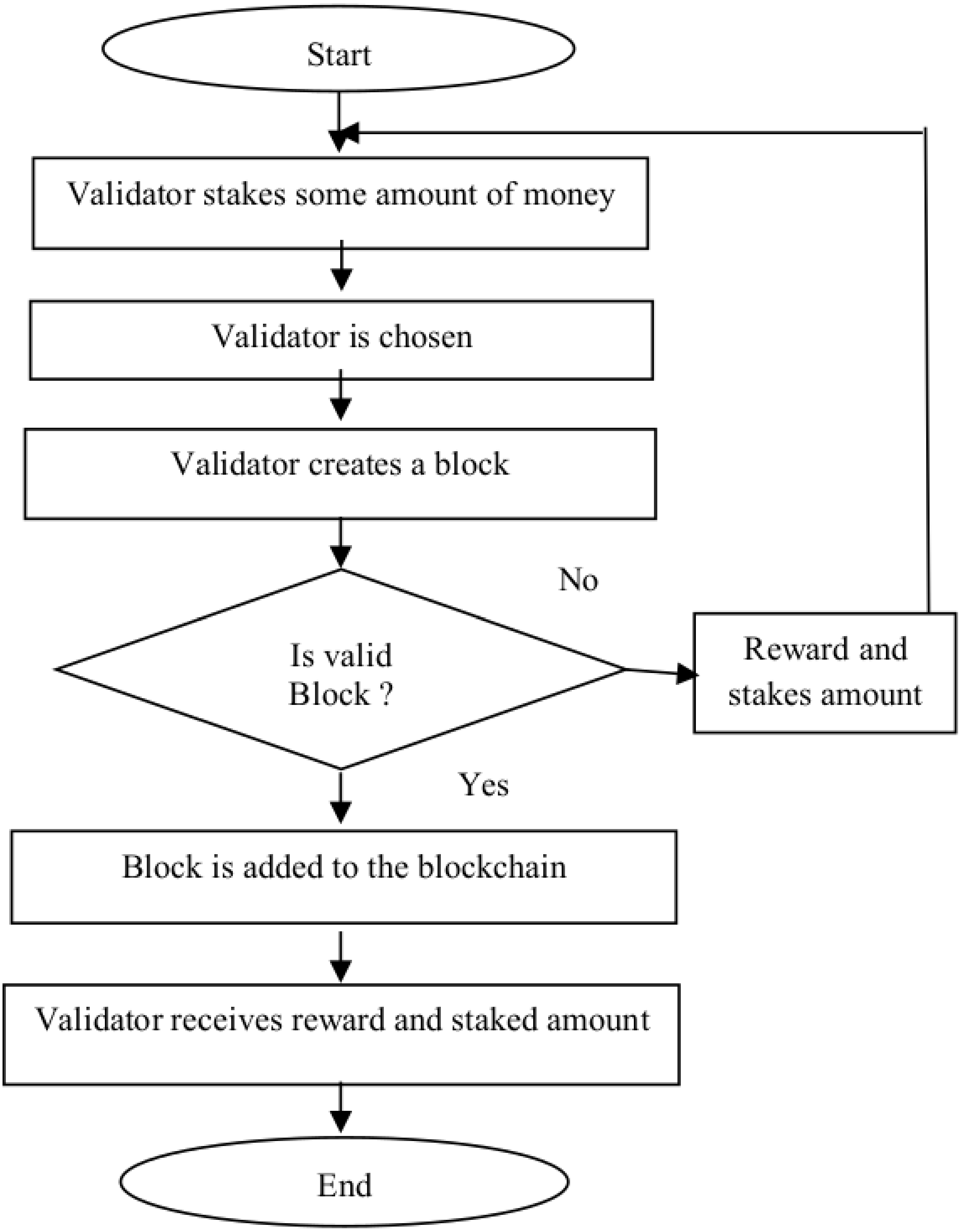
Start
Validator stakes some amount of money
Validator is chosen
Validator creates a block
No
Is valid Block ?
Reward and stakes amount
Yes
Block is added to the blockchain
Validator receives reward and staked amount
End

Fig. 4 Working of Proof of Stake Consensus

3.8.3 Delegated Proof Of Stake(DPoS)

The PoS consensus favors the nodes which hold the most amount of tokens thus reducing the fairness in the election process. Delegated Proof of Stake(DPoS) makes a small alteration in the process of selecting the mining nodes resulting in lower transaction costs and higher scalability. In DPoS, voting is carried out within the network to choose the miner from a fixed set of validator nodes that reduces the energy consumption throughout the network.

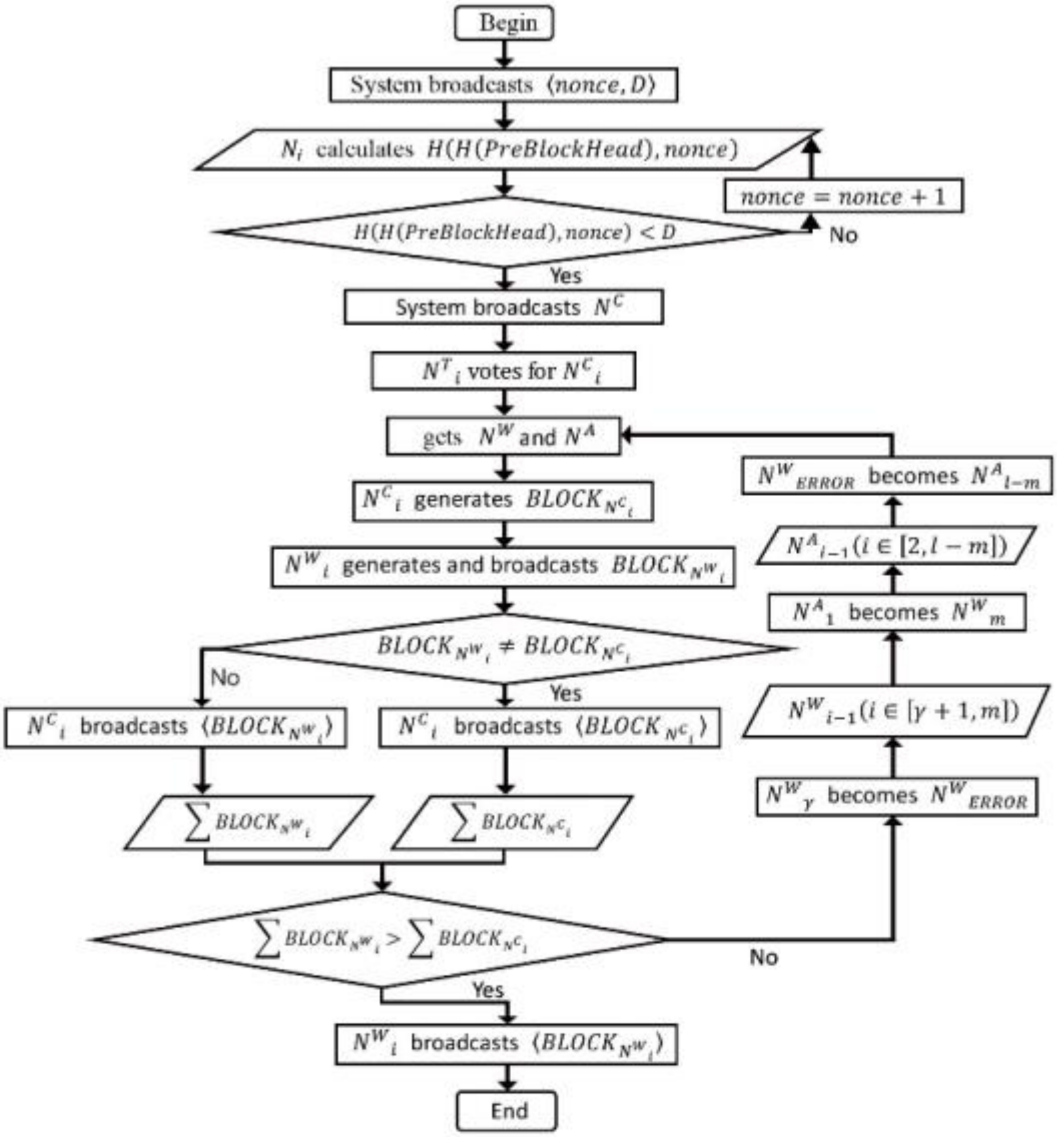
Begin
System broadcasts $\langle nonce, D\rangle$
N_i calculates $H(H(PreBlockHead), nonce)$
$nonce = nonce + 1$
$H(H(PreBlockHead), nonce) < D$
No
Yes
System broadcasts N^C
$N^T{}_i$ votes for $N^C{}_i$
gets N^W and N^A
$N^W{}_{ERROR}$ becomes $N^A{}_{l-m}$
$N^C{}_i$ generates $BLOCK_{N^C{}_i}$
$N^A{}_{i-1}(i \in [2, l-m])$
$N^W{}_i$ generates and broadcasts $BLOCK_{N^W{}_i}$
$N^A{}_1$ becomes $N^W{}_m$
$BLOCK_{N^W{}_i} \neq BLOCK_{N^C{}_i}$
No
Yes
$N^W{}_{i-1}(i \in [\gamma+1, m])$
$N^C{}_i$ broadcasts $\langle BLOCK_{N^W{}_i}\rangle$
$N^C{}_i$ broadcasts $\langle BLOCK_{N^C{}_i}\rangle$
$N^W{}_\gamma$ becomes $N^W{}_{ERROR}$
$\sum BLOCK_{N^W{}_i}$
$\sum BLOCK_{N^C{}_i}$
$\sum BLOCK_{N^W{}_i} > \sum BLOCK_{N^C{}_i}$
No
Yes
$N^W{}_i$ broadcasts $\langle BLOCK_{N^W{}_i}\rangle$
End

Fig. 5 Working of Delegated Proof of Stake Consensus

The authors of [20] propose a Blockchain-enabled IoV altering the traditional DPoS mechanism by using the reputation score of vehicles calculated based on historical interactions in the voting process to select the mining nodes.Meanwhile the standby miners are incentivized to take part in block verification to improve the security within the network.The high mobility of vehicles ensures even if a malicious node is elected as miner it will be able to compromise only a small subset of vehicles and is identified within a short amount of time.

3.8.4 Practical Byzantine Fault Tolerance

PBFT is a fault tolerant consensus mechanism which considers the software errors and malicious behavior by faulty nodes during the mining process. PBFT requires less than one third of all the nodes in the network to be faulty(malicious) to function correctly[23]. The authors of [24] exploit the immutability of blockchain to maintain a record of all the traffic related data to reduce the communication overhead. The architecture is based on Ripple blockchain which protects the network stability against 20 percent of all nodes being attackers/faulty. [25] alters the conventional PBFT mechanism by introducing a scoring system(SG-PBFT) which encourages the candidate nodes to provide honest results thus improving the consensus efficiency.

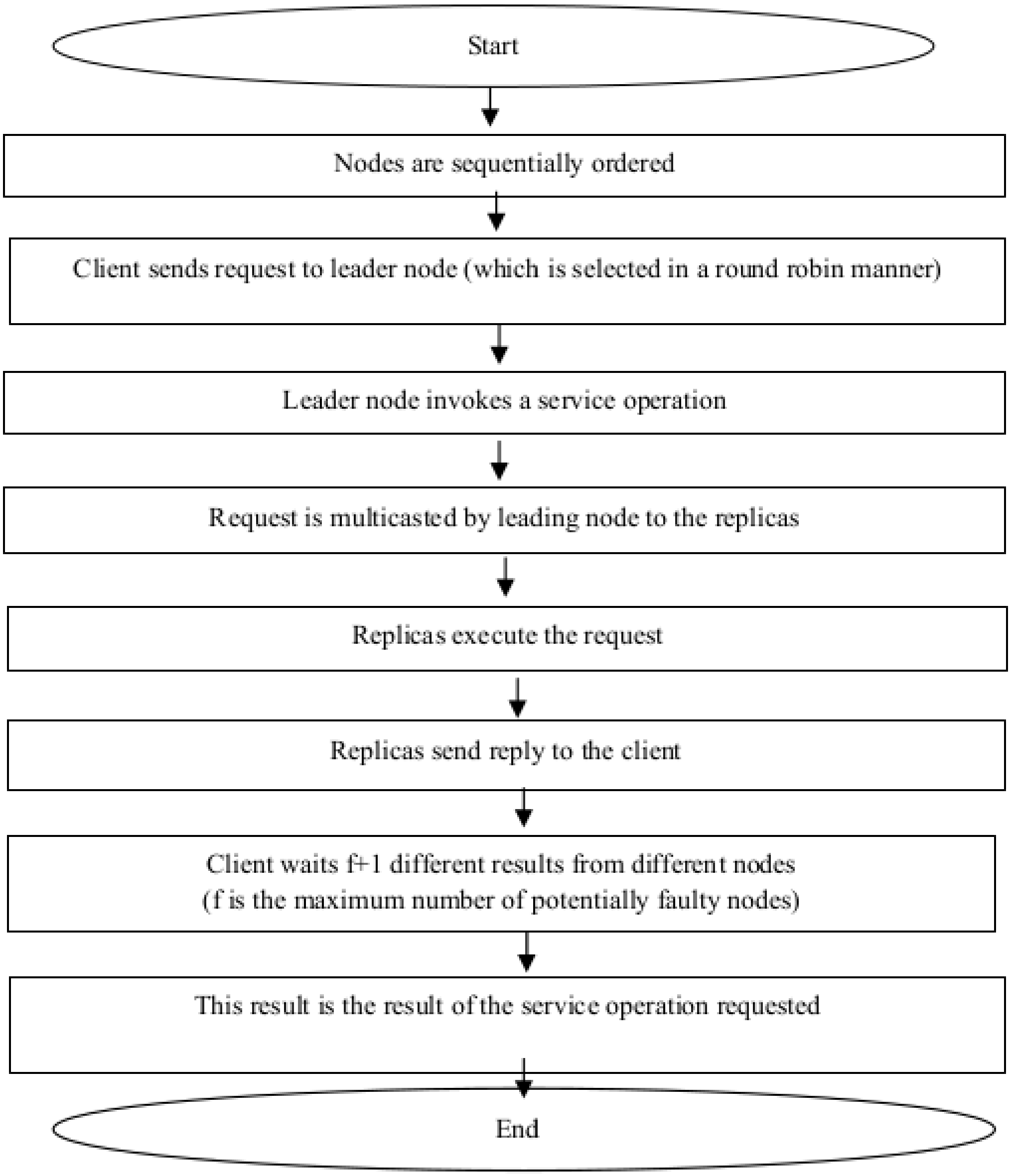
Start
Nodes are sequentially ordered
Client sends request to leader node (which is selected in a round robin manner)
Leader node invokes a service operation
Request is multicasted by leading node to the replicas
Replicas execute the request
Replicas send reply to the client
Client waits f+1 different results from different nodes
(f is the maximum number of potentially faulty nodes)
This result is the result of the service operation requested
End

Fig. 6 Working of Practical Byzantine Fault Tolerance Consensus

3.8.5 Proof of Reputation

Proof of Reputation assigns a reputation score to each network participant based on its history of interactions within the network and the consensus group consists of nodes with highest reputation values which determine the next state of blockchain[21]. Chai et al. have proposed a lightweight blockchain model using Proof of Reputation for resource sharing in Internet of Vehicles(IoV)[22]. The reputation scores are calculated through a smart contract which are completely auditable and only the RSUs with high reputation are allowed to publish the block.

3.8.6 Other Consensus Mechanisms

Authors of [26] propose the Ripple consensus in Vehicular Networks where the identity of verifying nodes is disclosed facilitating the identification of any malicious nodes. Additionally, the authors have discussed a novel key distribution scheme based on blockchain where the registration information of a vehicle is verified by a trusted third party authentication authority and issues a digital certificate of admission for the vehicle. To tackle the intensive computations involved in PoW and the lack of decentralization in PoS, [26] put forth Proof of Online Duration consensus allowing nodes to stake the amount of time they are active in the network rather than a specific amount of cryptocurrency and the node with higher online duration stands a better chance to be chosen as a block validating node. This approach encourages the vehicles to actively participate in the network activities and share the gathered traffic related data.

3.9 Edge Computing

Large amount of information is generated by sensors and vehicles in VANETs which has to be stored and processed throughout the network proving computationally expensive. Instead the raw data generated by network participants can be processed at end nodes using edge computing to reduce latency and enhance network reliability. Cui et al.[24] put forth a novel data downloading scheme where the frequently requested data is stored in Edge Computing Vehicles(ECV) so nearby vehicles can download directly from these ECVs.

3.10 Microtransactions

Microtransactions are a curtailed form of the transactions which lacks the non-essential components and keeps only the required components associated with the payment. Microtransaction can be used as a reliable service charging option in a peer to peer network. It contains only the essential content of the micropayment. For. E.g. Only the hash value and other necessary components associated with it. These components themselves are capable of the verification of the completed transaction. It is an efficient and sophisticated method of payment and can be used as a substitute to the traditional transaction methods.

IV. Conclusion

In this paper, we systematically reviewed the literature relating to different VANETs schemes and classified consensus algorithms for decision making in vehicular networks.We also identified a number of potential research opportunities based on the
review of the existing literature. Not surprisingly, security and privacy, for example, those relating to the vehicle (owner), remain a key challenge, particularly as vehicles become more digitized and systems are more interconnected. Moving forward consortium based blockchain with consensus algorithms which verify the identity of publishing nodes prior to adding them in the network can be used to reduce the computational overhead of processing each transaction.

REFERENCES

1. Mamun, Al, Khairul Anam, Fakhrul Alam Onik and A. M. Esfar-E.-Alam. “Deploy-ment of Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture.” (2012).

2. Hammad Shafiq, Rana Asif Rehman, Byung-Seo Kim, ”Services and Security Threats in SDN Based VANETs: A Survey”, Wireless Communications and Mobile Computing, vol. 2018, Article ID 8631851, 14 pages, 2018. https://doi.org/10.1155/2018/8631851

3. S. Biswas, R. Tatchikou and F. Dion, ”Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety,” in IEEE Communications Magazine, vol. 44, no. 1, pp. 74-82, Jan. 2006, doi: 10.1109/MCOM.2006.1580935.

4. Toh, Chai K. Ad Hoc Mobile Wireless Networks: Protocols and Systems. N.p.: Pearson Education, 2001.

5. S. B. Cruz, T. E. Abrudan, Z. Xiao, N. Trigoni and J. Barros, ”Neighbor-Aided Localization in Vehicular Networks,” in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 10, pp. 2693-2702, Oct. 2017, doi:10.1109/TITS.2017.2655146.

6. Li, H., Pei, L., Liao, D. et al. Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. Peer-to-Peer Netw. Appl. 12, 1178–1193 (2019). https://doi.org/10.1007/s12083-019-00786-4

7. Z. Lu, Q. Wang, G. Qu, H. Zhang and Z. Liu, ”A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs,” in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2792-2801, Dec. 2019,doi: 10.1109/TVLSI.2019.2929420.

8. J. Kang et al., ”Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks,” in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660-4670, June 2019, doi: 10.1109/JIOT.2018.2875542.

9. H. Chai, S. Leng, K. Zhang and S. Mao, ”Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles,” in IEEE Access, vol. 7, pp. 175744-175757, 2019, doi: 10.1109/ACCESS.2019.2956955.

10.Galal, Hisham Elsheikh, Muhammad. (2019). An Efficient Micropayment Channel on Ethereum. 10.1007/978-3-030-31500-9-13.
11. S. A. Jayalath, C. Rajapakse and J. M. D. Senanayake, ”A microtransaction model based on blockchain technology to improve service levels in public transport sector in Sri Lanka,” 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE), Colombo, Sri Lanka, 2020, pp. 82-89, doi: 10.1109/SCSE49731.2020.9313037.

12. Anand Paul, Naveen Chilamkurti, Alfred Daniel, Seungmin Rho, Chapter 1 Introduction: intelligent vehicular communications, Editor(s): Anand Paul, Naveen Chilamkurti, Alfred Daniel, Seungmin Rho, Intelligent Vehicular Networks and Communications, Elsevier, 2017

13. D. Jiang and L. Delgrossi, ”IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments,” VTC Spring 2008 - IEEE Vehicular Technology Conference, Marina Bay, Singapore, 2008, pp. 2036-2040, doi: 10.1109/VETECS.2008.458.

14. D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, ”Software-Defined Networking: A Comprehensive Survey,” in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015, doi:10.1109/JPROC.2014.2371999.

15. Arif, M., Wang, G., Wang, T., Peng, T. (2018). SDN-Based Secure VANETs Com-munication with Fog Computing. In: Wang, G., Chen, J., Yang, L. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS2018. Lecture Notes in Computer Science(), vol 11342. Springer, Cham.

16. El-hacen Diallo, Omar Dib, Khaldoun Al Agha, A scalable blockchain-based schemefor traffic-related data sharing in VANETs, Blockchain: Research and Applications,Volume 3, Issue 3, 2022.

17. Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

18. E. -h. Diallo, O. Dib, N. R. Zema and K. Al Agha, ”When Proof-of-Work (PoW) based blockchain meets VANET environments,” 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, 2021, pp. 336-343, doi: 10.1109/ICICS52457.2021.9464609.

19. J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim and J. Zhao, ”Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory,” in IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2906-2920, March 2019, doi: 10.1109/TVT.2019.2894944.

20. Aluko, Oladotun and Kolonin, Anton, Proof-of-Reputation: An Alternative Consensus Mechanism for Blockchain Systems (July 27, 2021). International Journal of Network Security Its Applications (IJNSA) Vol.13, No.4, July 2021, Availableat SSRN: https://ssrn.com/abstract=3906383

21. H. Chai, S. Leng, K. Zhang and S. Mao, ”Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles,” in IEEE Access, vol. 7, pp. 175744-175757, 2019, doi: 10.1109/ACCESS.2019.2956955.

22. Castro, Miguel Liskov, Barbara. (2002). Practical Byzantine Fault Tolerance and Proactive Recovery. ACM Trans. Comput. Syst.. 20. 398-461.10.1145/571637.571640.

23. Y. Yao, X. Chang, J. Mišić, V. B. Mišić and L. Li, ”BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services,” in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3775-3784, April 2019, doi: 10.1109/JIOT.2019.2892009.

24. Guangquan Xu, Hongpeng Bai, Jun Xing, Tao Luo, Neal N. Xiong, Xiaochun Cheng, Shaoying Liu, Xi Zheng, SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles, Journal of Parallel and Distributed Computing, Volume 164, 2022, Pages 1-11, ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2022.01.029.

25. H. Li, D. Han and M. Tang, ”A Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing,” in IEEE Systems Journal, vol. 15, no. 3, pp. 3189-3200, Sept. 2021, doi: 10.1109/JSYST.2020.3009447.

26. J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu and L. Liu, ”Edge Computing in VANETs-An Efficient and Privacy-Preserving Cooperative Downloading Scheme,” 16in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1191-1204, June 2020, doi: 10.1109/JSAC.2020.2986617.