# Analysis of the Use of Blockchain Consensus in VANET

Georgi Iskrov



July 16, 2021

# Analysis of the use of blockchain consensus in VANET

Georgi Iskrov
*PhD student in Technical University of Sofia-branch Plovdiv*
*Plovdiv*, Bulgaria
*g.iskrov@std.tu-plovdiv.bg*

***Abstract*** **— The article aims to look at existing blockchain conversion models in VANET environments. To expose the advantages and disadvantages and to outline a sensible approach to the use of blockchain for VANET. Analyzes existing blockchain models using the PoW consensus, which require two main approaches: Using less energy-intensive consensus such as Proof of Authority or using cloud services to export PoW's heavy calculations to MeC (Mobile Edge Computing). Last but not least, an adequate legal framework must also be provided.**

***Keywords — VANET, Blockchain, Proof of stake (PoS), Proof of authority (PoA), Proof of work (PoW), MeC***

## I. Introduction

Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) – arise by spontaneously creating a wireless vehicle communication network (V2V). VANET uses vehicle-to-vehicle communication architecture to ensure road safety, navigation and other roadside services. VANET is a key part of the Intelligent Transport Systems (ITS) system. VANETs are sometimes called Intelligent Transportation Networks. In the case of Vehicle Ad-hoc NETworks (VANET), the effectiveness of communication between vehicles is of utmost importance for drivers. The main purpose of the automotive network is to disseminate accurate information about life-threatening events such as traffic jams and accident reports for a short time [1].

Traditional VANET networks face several security issues. Due to false and unreliable information sent by malicious vehicles, some important messages cannot be distributed accurately in real time [2]. This can be solved by creating a local blockchain to exchange real-time messages between vehicles within a given road section using the VANET network. This public blockchain that reliably stores messages in a distributed ledger is suitable for secure and guaranteed message distribution [3, 4].

In the Vehicle Ad-hoc NETworks (VANET) distributed network, car nodes can join and leave the network dynamically - Mobile Ad-hoc NETwork (MANET) [1, 2, 3, 4]. Blockchain technology can be used to resolve critical issues with the dissemination of information in VANET. In the case of VANET, blockchain can be used to control the main vehicle information chain, as each vehicle can access the history of information about events in the public blockchain [5, 6]. For better scalability, there is no need for the chain to exceed the area of interest for observation. So information about traffic and accidents in a particular area or area is not necessary for the entire territory of the country. It is therefore more appropriate to maintain a separate blockchain [5, 6, 7] that takes into account only the level of confidence of the vehicle node and the reliability of messages in each country on the basis of the geographical location. The consensus mechanism plays an important role in determining the security and scalability of blockchain [1, 3, 7, 8]. The Proof of Work Consensus Mechanism (PoW), which has strong and verifiability and security and is suitable for public blockchain. The delay in distribution can be reduced using cloud periphery calculations [9, 10]. Blockchain can be defined as a disseminating and decentralised public database of all transactions or digital events that have been executed or shared between the participating nodes [11, 12].

A critical disadvantage of existing VANET models is adherence to the classic blockchain version, as well as the use of the PoW consensus. It is true that PoW solves unmuseful problems, such as the presence of malicious participants (compromised nodes), but the cost of this is expensive hardware, the need for a significant amount of energy for the reliable operation of ASIC equipment. And since here we are talking about transmitting messages about events on the roadway, that is, events that are registered and transmitted by other road users too. Thus, the basic presumption of the first block to receive the prize is lost. In this case, it is more important that the event is credible and quickly transmitted to as many users as possible on the road side. PoW has emerged as a hard-to-work, expensive and energy-intensive consensus. Consensus such as PoS or PoA would be far more suitable for use in MANET.

## II. VANET Basics

VANET has two types of communication: vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I) [14]. Vehicle-to-Everything (V2X) where a pedestrian, cyclist can communicate with the vehicle. In the case of V2I communication, vehicles communicate with road units (RSU) that are installed on both sides of the road [15, 16, 17]. The Wireless Access Protocol in vehicle Environments (WAVE) provides the main radio frequency channel for special small-range communication (DSRC) operating in the 5.9 GHz band. WAVE is based on the IEEE 802.11p standard [18]. Vehicles communicate with adjacent vehicles using on-board devices (OBU) and form an ad hoc network that allows communication in a distributed manner [19, 20].

Technology overview: 802.11p Special Small-Range Communication (DSRC). The original version uses WLAN technology between vehicles connected to the ad hoc network. As no infrastructure is required, this technology is suitable for contributing to traffic safety in structurally weak areas. It is also possible that the Car2Car-specific device for transporting WLAN into the vehicle supports not only the 802.11p standard, but also 802.11 in variants a, b and g.

The new V2X communication uses cellular networks and is called cell V2X (or C-V2X) to distinguish it from the WLAN V2X-based. The C-V2X was originally defined as LTE in 3GPP version 14 and is designed to work in several modes:

(1) Device to device (V2V or V2I) and

(2) Device to network (V2N).

Typical problems are: for example, the uncoordinated "semi-permanent schedule" for channel access on the C-V2X network requires more complex and error-prone algorithms than the already proven CSMA/CA that is used by the DSRC-based car2X version.

Criticism of accident prevention applications: The lack of distinction between network communication and non-network communication (DSRC) makes it difficult to assess costs, benefits and risks. The interests of network operators are not identical to the interests of drivers of vehicles. Any network support is first and foremost a burden on technical performance and does not bring profit to local operation. Confidentiality and security: In order to prevent intentional falsification or manipulation of messages, messages sent must have an electronic signature and the messages received must be verified for a valid signature. However, the anonymity of the users of the vehicle must be maintained. Each vehicle must have its own digital certificate, which may also be revoked in case of doubt. Each vehicle shall send a cyclic message every few seconds containing a vehicle identification number and information on speed, direction and position. On the basis of this information, driving profiles can be created, but also electronic parking tickets for speeding or passing a red traffic light. The same is possible if there are devices for receiving traffic lights or in (police) vehicles that can receive data from Car2Car. The sending of these cyclical messages, also known as 'beacons', is therefore critically considered. In this context, the signature of the messages sent relating to a vehicle must also be critically assessed.

One of VANET's main goals is to communicate with other vehicles using safety messages to report events such as accident information, safety warnings, congestion information, weather reports, road ice reports, etc. spread quickly and accurately, with minimal delay. Node trust and trust of event messages are among the main issues used to provide communication in VANET.

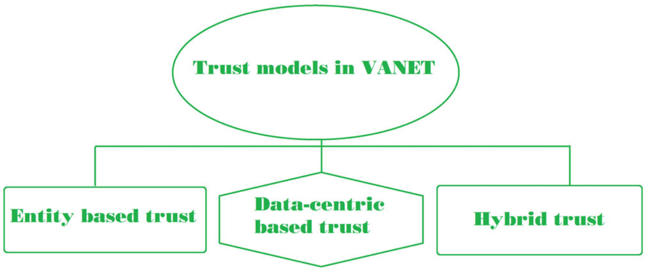


Fig. 1. Trust models in VANET

Existing trust models can be classified into three main categories:

- models of trust based on entities
- data-oriented confidence models, and
- hybrid models of trust.

Entity-based trust models focus on assessing the reliability of each vehicle, taking into account the views of partner vehicles [1, 21]. However, the reliability of the message may not align with the reliability of the node itself each time. It is usually very difficult to gather all the information to assess the confidence of the nodes in real time on the vehicle nodes due to their high mobility. Similarly, data-oriented confidence models focus on assessing the reliability of events obtained from adjacent vehicles rather than the reliability of the car unit itself [1, 22].

Potential vulnerabilities and attacks:

- 51% attack, if the attacker has more than half of all computing power in the network, then he can only confirm his own blocks, while ignoring the competing blocks, as well as blocking the transactions of the other participants. Alternatively, an attacker can rewrite the entire history of generating blocks, starting from a certain point in the past. As a result, it can catch up and overtake the current blockchain, making its version valid.

- Race Attack: The attacker completes transaction X while transferring transactions to the other fork with transaction Y. If the system could not confirm the first transaction there is a 50% probability that transaction Y can enter the real chain and this probability increases if the attacker intentionally selects network nodes for this or that operation.

- Finney's attack is this: an attacker tries to find the block that contains the Y transaction. However, as soon as the block is opened, the attacker sends transaction X. The system is waiting for transaction confirmation X. If at this point a block with transaction Y appears, then a split situation is created in which the validators must select one of two blocks to continue the blockchain chain. When a large amount of computational resources is concentrated in the hands of an attacker this can significantly increase the likelihood of selecting a block with Operation Y. Thus, a confirmed transaction is not guaranteed to be valid.

- Selfish mining: the aim of the attacker is control of the network, despite the fact that it has a total power of computing resources of less than 50%. This is achieved due to the fact that the attacker organizes a pool and imposes it as more profitable to extract than others, which attracts validators. The attacker posts blocks in such a way that other participants' computer resources are distracted/wasted.

- Sybil Attack: provides undue influence to an object simply because this object controls many aliases. Sybil's successful attack on a blockchain or file transfer network would allow bad actors disproportionate control over the network. If these fake identities receive recognition from the network, they may be able to vote on behalf of various proposals or disrupt the flow of information on the network. This usually takes the form of a reputational system where only established, long-term users can invite or guarantee new entrants to the network. Other variations rely on a trial system where new accounts are possible, but they must remain active and unique for a certain period before receiving voting privileges. Many blockchains use different "sequence algorithms" to protect against Sybil attacks, such as Proof-of-Work, Proof-of-Stake и Delegated-Proof-of-Stake. These consensual algorithms do not actually prevent an attack on Sybil, but simply make it impractical if the attacker successfully completes it.

Furthermore, the reliability of car nodes does not guarantee the reliability of the message itself, as reliable vehicles can transmit false messages when compromised by malicious vehicles. A hybrid trust model that combines entity-based and data-driven trust models should therefore be introduced in order to assess the reliability of the communication. The reliability of the node is assessed using a recommendation and functional trust. However, these mechanisms do not take into account the dilutedness of VANET data.

## III. View Blockchain Technology

Blockchain is a distributed public database for all digital events that are achieved and shared between participating nodes. It contains a definitive and verifiable record of every single event that has ever occurred. Each event in the blockchain database is confirmed by the consensus of the majority of nodes on the network [1, 5, 21]. The blockchain root is a genesis block that is the first block in the blockchain. This is the total origin of all blocks and contains the information that is commonly known on all nodes. The block consists of cryptographic hash of records, each block containing the hash information of the previous block, forming a data chain and creating blockchain. The structure of each block contains a block header and a block body. The header of the block consists of hash, nonce, hash of a previous block, as well as Merkle. The block body contains lists of transactions and some additional data, depending on the blockchain requirements. Each current block is interconnected with the previous block, using the hash of the previous block. For immutability transactions must be hashed, they are included in the header of the block. Merkle's hash is derived from Merkle's algorithm, which is a cryptographic algorithm that hashed out all transactions on the block to get merkle's hash. The Merkle tree is the hash of all hash of all transactions and is eventually added to the header of the block [1, 21].

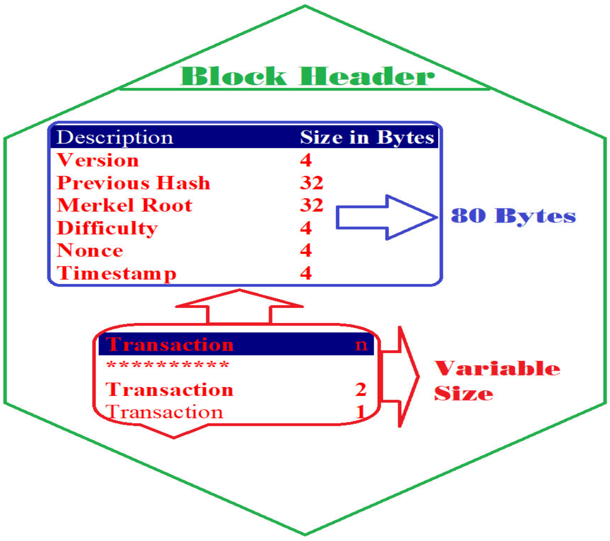


Fig. 2. Block Header Size

Immutability: One of the important characteristics of blockchain is invariability. Once some of the information has been saved and confirmed in blockchain, it cannot be modified or deleted from the network. Additionally, the information cannot be added arbitrarily [23]. Distributed and unreliable environment: In blockchain, each node that can be added can synchronize and validate all blockchain content in a distributed way without central control.

Privacy and anonymity: Blockchain provides privacy to users. The user can join the network anonymously. i.e. user information cannot be known to other users. This means that personal information is personal, secure and anonymous.

Faster transactions: It's very easy to set up blockchain and transactions are confirmed very quickly. Transactions or events only take a few seconds to process. Reliable and accurate data: Due to the decentralized network, blockchain data is reliable, accurate, consistent, timely and widely available. It can withstand malicious attacks and there is not a single point of failure. Transparency: It is completely transparent as it stores details of each individual transaction or event that occurs on the blockchain network. Anyone on the network can see transactions transparently [24].

## IV. VANET BLOCKCHAIN SCHEME

The solution to the listed problems would be the use of blockchain based on a reputation already created (the more created and reliably confirmed blocks with faithfully reflected road events the specific participant has, the higher the reputation rating will have).

The use of a hashed digital signature (a mandatory blockchain attribute) will reliably identify the user on the network, but at the same time keep their identity from being disclosed to third parties. Certain pieces of information about events, such as traffic jams, road accidents, environmental hazards are relevant for a particular geographical location [25]. Local information is not of particular interest to other regions or countries. All vehicles can know their positions using a location certificate based on proof of location (PoL). Vehicles will be able to communicate with other objects using communication Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) and that vehicles can be connected effectively to the internet [26]. All vehicles need to have necessary equipment such as OBU sensors and GPS. Critical event messages will be disseminated within a region of interest (RoI) at a specific geographical location [27]. Critical messages are not encrypted so that they are available to any nearby vehicle.

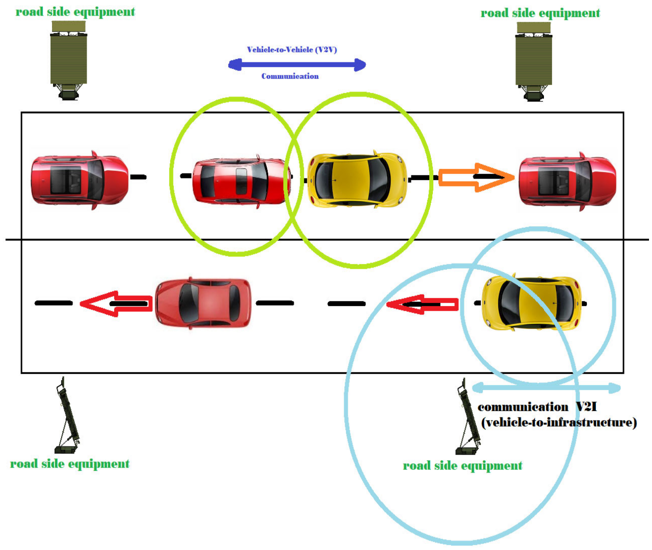


Fig. 3. VANET Scheme

RSU are used for V2I communication and are responsible for certifying and providing a vehicle location certificate within its scope of communication [28]. RSU will create a genesis block based on local events. Vehicles are the main elements of the VANET blockchain system. They generate event messages, extract new blocks, and store event messages in blockchain after auditing [29]. There are two types of car nodes: full node and normal node.

The full node has a high level of trust and strong computing power, which is responsible for the extraction of the blocks. And other nodes are normal nodes that help generate messages during accidents, as well as forwarding and checking received messages [30].

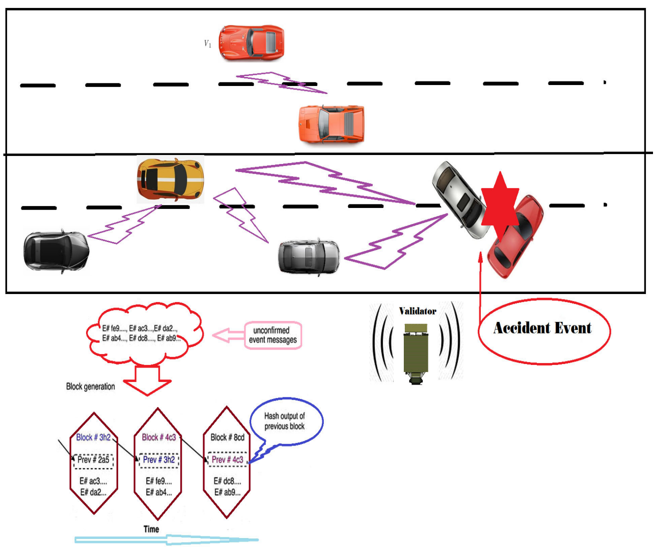


Fig. 4. Accident Event

VANET has two types of messages. They are beacon messages and safety event announcements.

- Beacon messages shall be broadcast periodically to inform neighboring vehicles of the driving status and vehicle positions in order to achieve awareness of cooperation between other motor nodes on the road for traffic management.

- Safety event messages are broadcast when critical events occur on the road, such as traffic accidents and road hazards, etc. [31] Depending on the severity of the accident, event reports are categorized at different levels based on priority, such as level 1, level 2 and level 3.

Where level 1 displays highly critical messages about the highest priority events, etc. Since beacon messages are frequently broadcast, they take the form of a flag when each beacon message is signed and authenticated.

Receiving Location Certificateficulty, time stout and Merkle tree of the previous block. The block body consists of a list of safety event messages that are held as transactions in the body of the block [32]. The PoL-based location certificate is used to provide proof of the location of a vehicle at a time. Each vehicle requires the PoL to confirm that the vehicle is located near the site of the event. In addition, PoL is used as proof of location in an event message. RSU acts as a validator to provide a vehicle location certificate within its range of communication. All vehicles and RSU are considered to have their own pairs of public and private keys.

The requesting vehicle sends a start message with its public key $\left(K_{vpub}\right)$ to RSU and then RSU sends any session ID $\left(sign\left(S_{id}\right)\right)$ to the vehicle. The vehicle sends back the signed session ID $\left(S_{id}\right)$ to RSU. RSU shall verify the authenticity of the signature $\left(sign\left(S_{id}\right)\right)$ of the vehicle's public key $\left(K_{vpub}\right)$ and check the time elapsed to exchange the session ID [7, 10, 11]. If the time difference between sending and receiving the session ID is less than a few milliseconds, RSU shall publish a location certificate $\left(LC\right)$, which shall include the location, time and public key of the vehicle $\left(K_{vpub}\right)$, which is signed by the RSU private key $\left(K_{R_{pr}}\right)$ as shown in Figure 4. GPS cannot be used because it can be easily seasoned [12, 13 14, 15 ]. PoL is protected because vehicles cannot create a fake location certificate without a valid RSU signature. However, using PoL alone does not guarantee the reliability of messages, so there is a need for a blockchain mechanism to make the message more reliable. The vehicle that encounters an event, such as an incident, will broadcast the event message with several parameters next to adjacent vehicles on the blockchain network [33]. When other vehicles receive a new event message, they first check that it is in the same area based on the LC embedded in the event message [34]. Vehicles examine the event message and check that it belongs to the same area. Neighbouring vehicles then check the other parameters of the event message. Each vehicle independently checks each event message before distributing it further to prevent Spam, DoS, and other attacks on the system. Whenever there are events , nearby car nodes will broadcast an event message $M_i$. Neighbouring vehicles will collect information from transmission vehicles. The event message contains all related information, such as event type, pseudo ID, event ID, trust level, time stamp, PoL, etc. Vehicles receiving the event message first check the level of confidence of the transmitting vehicle from the blockchain and then check the event message [33, 35]. They check each event message based on evidence regarding the level of trust of the transmitting vehicle, the location of the event, the event ID, direction of travel, PoL, speed, time check mark, etc., and store the message in the local memory pool if the message is considered reliable. Otherwise, the message is discarded. The event message is broadcast on the local blockchain network, and each vehicle on the network checks the event message [30 -34]. Vehicle forming blocks collect different event messages from an unconfirmed pool of event messages and check that the parameters of the accepted messages are valid. In the future perspective, it is envisaged to introduce extreme blockchain calculations that can reduce the delay in block generation by unloading high computing PoWs to end servers to form the blocks of custom vehicles. In addition, the delay in the distribution of the block can be reduced using the calculations of the cloud periphery.

## V. Mobile Edge Computing (MEC)

Mobile Edge Computing (MEC) can provide edge cloud services for VANET nodes and offload resource-intensive work from car nodes to end servers [35]. The use of a cloud structure is a way to offload the vehicle itself from the energy-intensive activity in the formation of the PoW consensus blocks. Administration of MEC in blockchain VANET is shown in Figure 6.

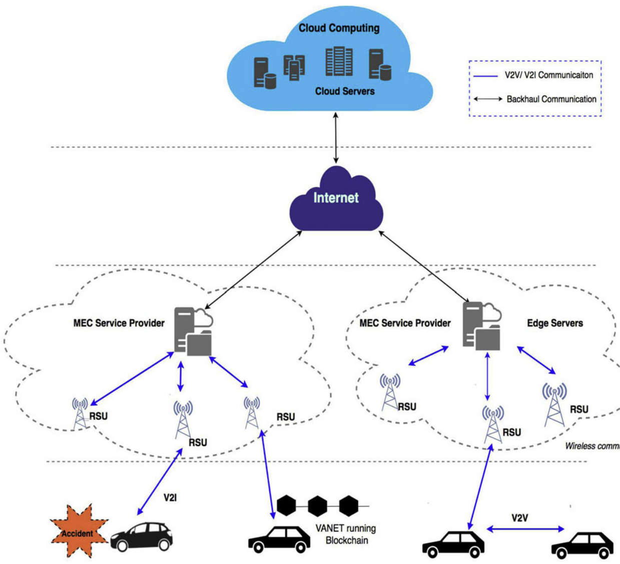


Fig. 5. MEC for blockchain in VANET

MEC can be used to distribute block messages between the nodes of the forming beneficiary, which may reduce the delay in distribution [36]. In addition, car nodes unload the block generation process to MEC servers to speed up the block formation process, which helps with frequent block generation, which is suitable for VANET [37]. As emergency messages are available, timeliness of message distribution is a high priority. Final calculations can be used to form the blocks more quickly in the proposed scheme. It is assumed that MEC service providers will deploy their end servers on automotive platforms [38]. The generating unit can unload the computational intensive PoW to the MEC. MEC servers accept and calculate PoW and provide solutions for users' nodes. The mining nodes then broadcast the PoW solution to the network [39]. Cloud structure is an alternative to the other approach when using lighter consensus such as PoS, PoA or PoC.

## VI. Conclusion

The purpose of this article is to analyze the most common VANET models. A new approach is needed in the use of blockchain in VANET, adapting lighter and scalable consensus, such as PoA (Proof-of-authority) and PoS (Proof-of-space). The use of communication between (V2V) vehicle-to-infrastructure communication (V2I) Vehicle-to-Everything (V2X) to the IEEE 802.11p standard. Currently, the standards for different networks (V2V), (V2I) and (V2X) are individual for each network. This difference affects communication speed and reliability.

MEC (Mobile Edge computing) is a solution that will unload vehicles from the need for the expensive equipment needed to mine the blockchain blocks. The use of cloud structures will make projects practical and easily applicable.

## References


**[1]** Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, Seung Yeob Namb *A new type of blockchain for secure message exchange in VANET* Digital Communications and Networks Volume 6, Issue 2, May 2020, Pages 177-186

[2] Adnan Shahid Khan, Kuhanraj Balan, Yasir Javed, Seleviawati Tarmizi and Johari Abdullah *Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET* Journals Sensors Volume 19 Issue 22 (8 November 2019)

[3] Karuna Nidhi Pandagre, Apoorva Joshi, Jayanti Jharia *Vehicular ad-hoc networks (VANETs)* International Journal of Research in Computer Applications and Robotics (IJRCAR) ISSN 2320-7345 Vol.4 Issue 2, Pg.: 29-32 February 2016

[4] Sabih ur Rehman, Arif Khan, Tanveer Zia, Lihong Zheng *Vehicular Ad-Hoc Networks (VANETs)* An Overview and Challenges Journal of Wireless Networking and Communications 2013

[5] Taoufik Yeferny and Sofian Hamad *Vehicular Ad hoc Networks: Architecture, Applications and Challenges* IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.2, Fabruary 2020

[6] Shivam Vats, Sanjay Kumar, Siddharth Shukla, Shiv Shankar Vanet: *A Future Technology* International Journal of Scientific and Research Publications, Volume 7, Issue 2, 378 ISSN 2250-3153 February 2017

[7] Jiyao An, Yingjun Yu, Jie Tang, and Jiawei Zhan *Fuzzy-Based Hybrid Location Algorithm for Vehicle Position in VANETs via Fuzzy Kalman Filtering Approach* Hindawi Advances in Fuzzy Systems Volume 2019, Article ID 5142937

[8] Asim Rasheed, Saira Gillani, Sana Ajmal and Amir Qayyum Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications Advances in Intelligent Systems and Computing · March 2017

[9] Le Liang, Hao Ye and Geoffrey Ye Li *Towards Intelligent Vehicular Networks: A Machine Learning Framework* supported in part by a research gift from Intel Corporation and in part by the National Science Foundation under Grants 1443894 and 1731017. Jun 2019

[10] Khondokar Fida Hasan, Yanming Feng and Yu-Chu Tian *GNSS Time Synchronization in Vehicular Ad-Hoc Networks: Benefits and Feasibility* supported in part by the ICTDivision, Bangladesh, and in part by the Australian Research Council under Grant DP160102571 and Grant DP170103305. 1524-9050 © 2018 IEEE

[11] Ullah Ihsan, Robert Malaney and Shihao Yan *Neural Network Architectures for Location Estimation in the Internet of Things* © 2020 IEEE 19 Oct 2020

[12] Ming Lin , Jaewoo Yoon and Byeongwoo Kim *Self-Driving Car Location Estimation Based on a Particle-Aided Unscented Kalman Filter* journal Sensors 2020, 20, 2544;

[13] Mustafa Maad Hamdi, Lukman Audah, Sami Abduljabbar Rashid, Ahmed Shamil Mustafa, Mohammed Salah *Abood A Survey on Data Dissemination and Routing Protocol in VANET: Types, Challenges, opportunistic and Future Role* International Journal of Advanced Science and Technology Vol. 29, No. 5, (2020), pp. 6473 – 6482

[14] Felipe Lobo, Danilo Grael, Horacio Oliveira, Leandro Villas, Abdulaziz Almehmadi and Khalil El-Khatib *Cooperative Localization Improvement Using Distance Information in Vehicular Ad Hoc Networks* journal Sensors 2019

[15] Alex-Radu Malan *How to tackle bandwidth scarcity in vehicular communication* School of Computing, Mathematics and Digital Technology Master's Project 6G7Z1015_1819_9Z6 September 2019

[16] K D Ibrahem, A N Rashid and F S Mubark *A New Deployment Schema Using Dynamic Relay Vehicle to Improve VANETs Connectivity in Urban Environment* 2nd International Scientific Conference of Engineering Sciences (ISCES 2020)

[17] S Deivanayagi, N Gopinath, Dr V Nagaraju, Kanagaraj Venusamy *Chapter 25: Vehicular Ad-Hoc Networks* Technical Research Publications ISBN: 978-93-5419-211-1 10 February 2021

[18] Debjyoti Saha, Pravin Wararkar, Shashikant Patil *Comprehensive Study and Overview of Vehicular Ad-HOC Networks (VANETs) in Current Scenario with Respect to Realistic Vehicular Environment* International Journal of Computer Applications (0975 – 8887) Volume 178 – No. 15, May 2019

[19] Navneet Kaur, Sandeep Kad *Data Dissemination In VANETS A Review* International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P), Volume-6, Issue-4, December 2016

[20] Mariam Elazab, Aboelmagd Noureldin, Hossam Hassanein I*ntegrated cooperative localization for Vehicular networks with partial GPS access in Urban Canyons* Vehicular Communications 9 (2017)

[21] Amal Hbaieb, Samiha AYED, Lamia CHAARI *Internet of Vehicles and Connected Smart Vehicles Communication System Towards Autonomous Driving* Creative Commons Attribution 4.0 International License 03 Jun, 2021

[22] Sakshi Rathi, Paras Chawla *Data Dissemination in VANET: A Review* International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 10 | Oct -2017

[23] YiRen Shi, Hao Wu *Data Aggregation for Road Functionality Detection Based on Machine Leaning and VANET* Journal of Computers Vol. 29 No. 2, 2018, pp. 161-173

[24] Siegel and Joshua E, *A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas.* IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 8, Aug. 2018, pp. 2391–406.

[25] Waqas Ahmad, Nasir Saeed, Dost Muhammad Saqib Bhatti *Localization of Vehicular Ad-Hoc Networks with RSS Based Distance Estimation* 2018 International Conference on Computing, Mathematics and Engineering Technologies - iCoMET 2018

[26] Rathin Chandra Shit, Suraj Sharma, Kamakhya Narain Singh, Shankar Sharan Tripathi Overview and Perspective of Localization Accuracy for Persistent Autonomous Vehicle Systems International Conference on Information Technology (ICIT) 2019

[27] Sami Abduljabbar Rashid, Lukman Audah, Mustafa Maad Hamdi Reliable and efficient data dissemination scheme in VANET: a review International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 6, December 2020, pp. 6423~6434

[28] Keyvan Golestan, Sepideh Seifzadeh, Mohamed Kamel, Fakhri Karray, Farook Sattar Vehicle Localization in VANETs Using Data Fusion and V2V Communication DIVANet'12, October 21–22, 2012, Paphos, Cyprus.

[29] Sabih ur Rehman, Arif Khan, Tanveer Zia, Lihong Zheng Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges Journal of Wireless Networking and Communications 2013, 3(3): 29-38

[30] Sony Guntukaa, Elhadi Shakshukia, Siddardha Kajaa, Ansar Yasarb Queue based Vehicular Ad Hoc Network Prognostic Offloading Approach The 11th International Conference on Ambient Systems, Networks and Technologies (ANT) 2020

[31] Madhusudan Singh, Shiho Kim Blockchain Based Intelligent Vehicle Data sharing Framework Cryptography and Security (cs.CR) 20 Jul 2017

[32] Dinh C. Nguyen, Pubudu Pathirana, Ming Ding, and Aruna Seneviratne Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges IEEE COMMUNICATIONS SURVEYS 2019

[33] Benjamin Leiding, Parisa Memarmoshrefi, Dieter Hogrefe Self-managed and Blockchain-based Vehicular Ad-hoc Networks 2016 ACM International Joint Conference

[34] Arash Bozorgchenani, Setareh Maghsudi, Daniele Tarchi and Ekram Hossain Computation Offloading in Heterogeneous Vehicular Edge Networks: On-line and Off-policy Bandit Solutions IEEE Transactions on Mobile Computing · May 2021

[35] Juan Fang, Jiamei Shi, Shuaibing Lu, Mengyuan Zhang and Zhiyuan Ye *An Efficient Computation Offloading Strategy with Mobile Edge Computing for IoT* Micromachines 2021, 12, 204

[36] Nasir Abbas Mobile Edge Computing: A Survey architecture, applications, approaches and challenges Master's Thesis Autumn 2016

[37] Adnan Shahid Khan, Kuhanraj Balan, Yasir Javed, Seleviawati Tarmizi and Johari Abdullah *Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET* journal Sensors 2019, 19, 4954

[38] Gabriel Orsini, Dirk Bade, Winfried Lamersdorf *Computing at the Mobile Edge: Designing Elastic Android Applications for Computation Offloading* 2015 8th IFIP Wireless and Mobile Networking Conference

[39] Uzair Javaid, Muhammad Naveed Aman, and Biplab Sikdar Driv Man: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)