Düzce University
Journal of Science & Technology

Review Article

A Review on Vehicle To Vehicle Communication Using BlockChain

Şükrü OKUL [a,*], Fatih KELEŞ [b], M. Ali AYDIN [b]

[a] *BTE, TÜBİTAK BİLGEM, Kocaeli, TURKEY*
[b] *Department of Computer Engineering, Istanbul University Cerrahpaşa, Istanbul, TURKEY*
* *Corresponding author's e-mail address: sukruokul@gmail.com*

DOI: 10.29130/dubited.1117691

ABSTRACT

In this study, there are theoretical information about security in communication between block chain and vehicles. When talking about block chain, its types, features and content are mentioned. In the light of all this theoretical information, the studies made using block chain in inter-vehicle communication are examined. In addition, information about the methods used and their contents related to these studies are given. The theoretical background of this information is explained under general headings. In addition, the methods used by the studies examined are also categorized and explained together with the studies. In the study, first of all, detailed information is given about the block chain as stated. Afterwards, VANET (Vehicles Ad-hoc Network) security is mentioned. Afterwards, the studies in the literature are explained, and finally, future studies are mentioned in the conclusion section.

Keywords: *Block Chain, VANET, Security*

Araç Araç Haberleşmesinde Blokzincir Kullanımı Üzerine Bir İnceleme

ÖZ

Bu çalışmada blokzincir ve araçlar arası iletişimde güvenlik ile alakalı teorik bilgiler yer almaktadır. Blokzincirden bahsedilirken çeşitlerinden, özelliklerinden ve içeriğinden bahsedilmektedir. Tüm bu teorik bilgiler ışığında araçlar arası haberleşmede blok zincir kullanılarak yapılan çalışmalar incelenmektedir. Ek olarak incelenen bu çalışmalar ile alakalı olarak kullanılan yöntemler ve içerikleri hakkında bilgiler verilmektedir. Bu bilgilerin teorik alt yapısı genel başlıklar altında açıklanmaktadır. Ayrıca incelenen çalışmaların kullandıkları yöntemler de çalışmalarla birlikte kategorize edilerek açıklanmaktadır. Sırasıyla çalışmada öncelikle blok zincir ile ilgili belirtildiği üzere detaylı bilgi verilmektedir. Sonrasında VANET(Vehicles Ad-hoc Network) güvenliğinden bahsedilmektedir. Sonrasında literatürde geçen çalışmalar açıklanmakta ve son olarak sonuç bölümünde gelecek çalışmalardan bahsedilmektedir..

Anahtar Kelimeler: *Blokzincir, VANET, Güvenlik*

Received: 17/05/2022, Revised: 15/03/2023, Accepted: 12/05/2023

I. INTRODUCTION

There are many studies on vehicle networks, especially recently. Communication between vehicles and the security of these communications are important issues. Blockchain, which is very up-to-date on this important issue, has also been working on it for the last few years. Blockchain is a node-to-node, decentralized, distributed and peer-to-peer technology. It keeps track of transactions made to every node or some nodes that have occurred. In other words, it is called the distribution of central trust in the internet environment by allowing a central server or a trusted authority to be removed. Blockchain technology is commonly known as the technology underlying virtual currencies such as Bitcoin and Etherium. When the capacity of a block is full, a new block is generated immediately and new data is recorded by going through the same processes that we have explained above. In other words, the new block is added to the previous block. This situation continues in a continuous loop and an infinite chain of interconnected data blocks is formed. The hash of the previous block is one of the data it keeps in the next new block. As a result, it creates a data chain and a blockchain as seen in Figure 1 [1]. Each data has a timestamp. This data is recorded in the blocks in the system, most of the other participants in the network verify this data, and also this data is stored in blocks by end-to-end encryption [2]. Since each block can have limited data capacity, a fixed-length output of the full block, called a hash, is generated corresponding to all the data saved in the block [3]. Each block in blockchain technology consists of a body and a header. Information contained in the block header: Block version, merkle tree root hash, Timestamp, threshold information for a valid block hash, Nonce (usually a 4-byte field that increments for each calculation starting with 0), and Hash field in previous block Corresponding to previous block An incoming 256-bit hash value is kept in the chain [4]. Blockchain has significant advantages and disadvantages. If we look at the advantages of the blockchain; all data is stored as a copy on all stakeholders involved in the blockchain. In this way, both erroneous data and data loss are prevented. In this way, it becomes a structure that can work without a central authority. In addition, thanks to digital signing or verification processes, trust can be provided without intermediaries. Because all stakeholders can see both their own transaction status and the details of all transactions. In addition, the information contained in the blockchain cannot be changed or deleted [5].

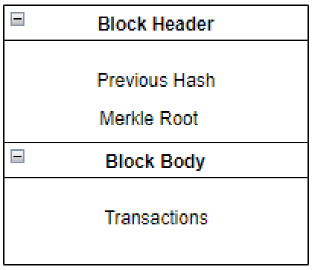


Figure 1. *General Block Data Structure*

It is important which type of blockchain will be used with the blockchain. Blockchain is of three types when considering access methods. These are Public, Private and Consortium blockchain. Public Blockchain network, anyone can join the network. This system is considered to be a completely independent and central authority-free blockchain system. Private Blockchain system, only authorized users can join the network. Engagement in consensus within the network can be defined publicly or in a permissioned form. If those who are authorized in the private blockchain system and who settle in the system enter the consensus structure without permission, these systems are called partially permission-requiring systems. In these networks, a central authority has the authority to change the rules and reverse transactions based on need. It is used to set up special systems, reduce costs and increase efficiencies. Consortium blockchain networks are considered a mix of public and private blockchain networks. It is a system that the node can pre-select by the authorized person or institution. The data in this blockchain can be public or private. The ability to read and write on a consortium blockchain can be extended to a certain number of nodes. This situation can be used by institutions or organizations that come together and cooperate with each other to develop different models [6,7].

The advantages of the blockchain are provided by its components and digital signature. These components defined as Blockchain, Ledger, Peer Network, Membership Services, Smart Contract, Wallet and Events. If we define the ledger, it is a decentralized and immutable collection of records that stores all transactions of the Blockchain. Depending on the type of blockchain, this ledger is available to all or some members. Peer Network, on the other hand, provides operations such as keeping the ledger and updating it. A copy of the ledger resides on all or some of the nodes in the used blockchain's network. This situation varies according to the type of blockchain used. With each data added to the ledger, in other words, with every ledger update, the nodes that hold the ledger in the network of the blockchain used make an agreement between them. Thanks to this method used, the nodes responsible for keeping the ledger in the used blockchain network can keep a copy of the relevant ledger without a central authority. Membership Services is an authority that all members or some members have, depending on the type of chain. That is, membership services are used by the authorized nodes in the blockchain to verify and authorize blocks. The concept of Smart Contract, on the other hand, can be characterized as a program or script that can be run on the blockchain. Initially, blockchains have limited configurations, so they are designed to record and store financial transactions in the historical ledger. Recently, contracts have been developed for the distributed operation of blockchains. The wallet, on the other hand, stores the identity information of the members in the chain. In Blockchain, the wallet is also used to store and track other details associated with members' accounts. The term defined as events is when the peer-to-peer network and the blockchain ledger update its state on the nodes that hold it. Smart contract notifications in blockchains are also considered events [7].

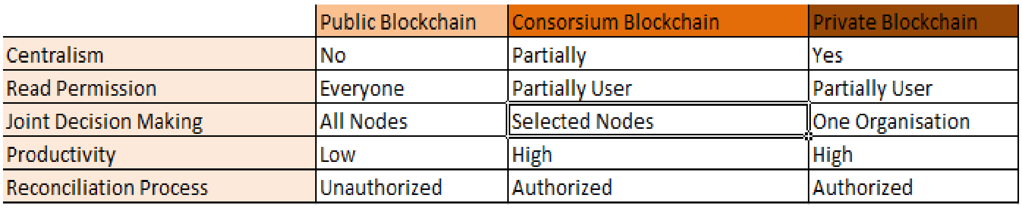
As for the digital signature side; each user has two different keys, a private key and a public key. A private key is used to sign transactions. All digitally signed transactions are accessed using public keys in a way that can be accessed by anyone in the network. The digital signature consists of two stages: signing and verification. For example, for the transaction of X that wants to sign a hash, a hash value is generated from the transaction. This hash value is then encrypted using the private key and the encrypted hash information is delivered to Y. Y decrypts the encrypted digest with the public key sent by X and generates the hash of the message. The control operation is provided by the transaction received by comparison between the hash value derived from the message of X [8-10].

The last point that we can specify as important in the use of blockchain is consensus algorithms. For the block to be added to the end of the blockchain, the majority of the miners in the network must achieve consensus. After the consensus is reached, the block is added. For this, there are some negotiation methods in the blockchain.

Proof of Work (PoW) As the name suggests, it is a labor-intensive reconciliation method to add blocks. PoW is a method used by the Bitcoin cryptocurrency. It is based on cryptographic riddles that are not easy to calculate. The node in the network trying to solve these riddles is called a miner. The first node to obtain the specified hash value has the right to add a block to the end of the blockchain. A fork occurs if more than one miner simultaneously obtains the same hash value and sends it to the network. In this case, both forks will continue to exist until a new block is produced in one of the forks. In the long fork, whichever a new block is added, miners continue their work. Due to the difficulty of mathematical solutions, it requires a lot of computer power and takes a lot of time [8-10].

Proof of Stake (PoS) PoS consensus has been introduced as an alternative to the PoW algorithm, which consumes a lot of electricity. In this settlement method, those who have a surplus of assets among the miners in the network get the right to add blocks. Therefore, he has to prove the amount of cryptocurrencies. It does not require much processing power, as it does not require solving a cryptographic puzzle like in PoW. However, since the node with the most shares can always be dominant, solutions are presented by looking at information such as the creation time of the assets to propagate the next block. Another alternative solution option is to make the nodes passive by adding a time limit to the digital currencies deposited by the nodes. After a certain period of time, the right to create a block is given and the miner is activated [8-10].

Proof of Authority (PoA) It has several important advantages over other consensus methods. It is more scalable because it has a certain number of block validators compared to PoW and PoS methods. Blocks are validated with digital IDs. So they use their own reputation instead of the amount of cryptocurrency. The time interval during which new blocks are produced can be estimated. This time varies for PoW and PoS reconciliation. It has a high transaction rate. Blocks are created in a sequence in a time interval determined by authorized network nodes. This, in turn, increases the speed of confirmation of transactions. Microsoft Azure is an example where PoA is used. It is offered as an alternative solution to private networks, so there is no need for mining [8-10].



	Public Blockchain	Consorsium Blockchain	Private Blockchain
Centralism	No	Partially	Yes
Read Permission	Everyone	Partially User	Partially User
Joint Decision Making	All Nodes	Selected Nodes	One Organisation
Productivity	Low	High	High
Reconciliation Process	Unauthorized	Authorized	Authorized

Figure 2. *Comparisons of Blockchain Types*

Comparisons of blockchain types are shown in Figure 2. Security is at the forefront in studies on vehicle networks, also called VANET. The security elements that need to be addressed in VANET, as the reason why security is at the forefront, can be listed as Data Consistency, High Mobility, Fault Tolerance, Latency Control and Key Management. Data Integrity is the accidental or other leak of important information. Considering this situation, such structures should be designed to prevent data inconsistency. All information received from various nodes needs to be cross-checked to avoid such malicious transactions. If High Mobility is to be explained: Nodes in wired communication and nodes in inter-vehicle communication are similar in terms of energy source and information processing capabilities. However, due to their high mobility, they need to process transactions in less time by running a security protocol that is shorter than normal as execution time for similar output. In other words, time should be considered as an important factor while developing and designing security protocols. Fault Tolerance: Security protocols must be fault tolerant due to the fast ingest and response action in VANET. Latency Control: All implementations of VANET are latency sensitive. To realize these real-time applications, security algorithms need to be faster and more efficient. Key Management: Cryptographic algorithms used in VANET security depend on keys. In such a dynamic scenario, careful creation, maintenance, and distribution of keys is desirable [11-13].

VANET applications are shaped depending on the interactions between vehicles. During this interaction, mutual information is transferred. Incorrect information contained in the transmitted information may cause problems with the physical or cyber security of the transferred vehicles. Due to the nature of communication in VANET, it has a multi-hop structure. For this reason, security-related information emitted during communication can become problematic by intermediate nodes and cause traffic jams, road accidents, etc. can cause problems. VANET applications should be designed with security algorithms to ensure the protection of data in communication and the confidentiality of user identity information [14].

The attacks that occur in VANET can be classified. This classification is made taking into account the security requirements and the affected layers. To ensure security against all these identified attacks, security standards in the network must be met. The important elements that can be considered related to security can be listed like that: Authentication, Confidentiality, Availability, Non-Repudiation and Data Integrity. Depending on these security requirements, attacks can be divided into some classes as follows [15,16]:

- Authentication attacks
- Attacks on usability
- Attacks on privacy(Confidentally)
- Attacks on data integrity.

II. LITERATURE

Shrestha et al., work is being done to address the immutability security challenge. In his studies, data is obtained through VANET messages. General blockchain is used as blockchain. Mining can be produced in each of the independent elements. Proof of Work is a consensus mechanism used as consensus. To summarize, the scalability of the messages sent to communicate in VANET is seen. At the same time, a native blockchain independent of other related chains was deployed to improve the timing of related messages. This blockchain is the public blockchain. At the same time, it is used to manage and store the reliability of the communication of the nodes in the chain [17].

Chen et al., work is being done to address data tampering, information transparency, data trade security challenges. In his studies, data is obtained through VANET messages. Consortium blockchain is used as blockchain. It can be produced in mining roadside units (RSU). Proof of Work is used as a consensus [18].

Mostafa et al. work to address security challenges of data integrity, authenticity, and non-repudiation. In his studies, data is obtained through VANET messages. General blockchain is used as blockchain. Mining can be produced in each of the independent tools. Proof of Work is used as a consensus [19].

Khan et al., security and privacy, threats such as DDoS, data modification, impersonation, Sybil and replay attacks are working to address security challenges. In their studies, data is obtained from VANET data. As blockchain, public and private blockchains are used. Mining can be produced in roadside units. A distributed consensus is used as a consensus. In summary, blockchain technology is used to increase security and privacy to reduce MAC layer attacks such as DoS, Sybil and data manipulation and transfer attacks [20].

Malik et al. work to address security challenges of data privacy, integrity, non-repudiation, and mutual authentication. In their studies, their data is obtained from VANET data. Private blockchain is used as blockchain. Mining can be produced in a central authority. Proof of Authority is used as a consensus. In a nutshell, by distributed storage A smart contract-based approach is used to update and query stored and maintained nodes [21].

Li et al., work is being done to address the security challenges of usability, authenticity, and undeniability. In their studies, their data is obtained from VANET data. Private blockchain is used as blockchain. Mining can be produced in roadside units. Proof of Authority is used as a consensus. They use the merkle tree with smart contracts to achieve the "proof-of-take-advertising" feature in their vehicle network. The purpose of this is to prevent any tool from cheating or to ensure that it can transact without increasing storage costs. In addition, they can ensure the confidentiality of the vehicles with the method they propose [22].

Zheng et al. have worked to address the security challenges of integrity, non-repudiation, and scalability of data storage. In their studies, their data is obtained from VANET data. General blockchain is used as blockchain. Mining can be produced in roadside units. Proof of Work is used as a consensus [23].

Lai et al. use bulk message authentication code and one-time password technology to reduce delay and cost factors in the authentication process. Thanks to these used ones, they propose a blockchain-based group mobility management. This proposed method is defined as more efficient and safe than its counterparts [24].

Kaur et al. propose a method that includes a lightweight and considered VFC setup. The scheme they propose includes authentication and key scheme between data centers. In the method, elliptic curve cryptography is used together with blockchain. Blockchain is used here to protect information [25].

Gao et al. are trying to ensure the effective operation of VANET systems by using blockchain and SDN technologies. With shared responsibilities between the chain and SDN, the processing load is lightened. A trust-based model is proposed to prevent malicious attacks on the network used [26].

Hu et al. use blockchain technology to complement consensus with authentication. In addition to blockchain technology, a Byzantine consensus algorithm based on time series and gossip protocol is used. The technologies and algorithms used here increase the efficiency and communication security of the nodes [27].

The model proposed by Liu et al features a blockchain-based trust management model for VANETs combined with a conditional privacy-preserving announcement scheme. First, there is an anonymous mass vehicle announcement protocol designed to allow vehicles to send messages anonymously in a completely untrusted environment to ensure vehicle privacy. Secondly, it implements message synchronization and reliability with a blockchain-based trust management model. In addition, roadside units and trusted authority are also used in this model [28].

The model proposed by Singh et al includes a blockchain-based decentralized trust management scheme using smart contracts. Blockchain sharding is used to reduce the load on the original blockchain and increase transaction volume. This model has two important contributions. Its primary contribution is to maintain reliable and consistent values of trust throughout the network. The other is that it performs well compared to its pers [29].

The model proposed by Lu et al increases the credibility of messages based on the reputation of the sender, based on both direct historical interactions and indirect views about the sender [30].

Table 1: *Literature Review Summary*

Paper	Blockchain Type	Storage or Communication Mechanism
[19]	Consortium	RSU
[20]	Public	RSU
[21]	Public	RSU
[22]	Consortium	RSU
[23]	Consortium	RSU
[24]	Consortium	RSU
[25]	Public	RSU
[26]	Consortium	RSU
[27]	Public	RSU and Data Storage
[28]	Private	RSU and Trusted Authority
[29]	Private	Etherium
[30]	Public	RSU and Vehicles
[31]	Public	Vehicles
[32]	Private	Vehicles and Data Storage
[33]	Private	Data Storage

The blockchain-based V2I authentication (B-TSCA) scheme proposed by Wang et al enables rapid re-authentication of vehicles through secure transfer of ownership between infrastructures. Reliable scalable computing is supported by blockchain to ensure decentralization and immutability of the scalable computing result. Security analysis shows that the B-TSCA scheme is a CDH secure scheme [31].

According to the model proposed by Umoren et al., it is a system that directly connects producers with consumers to meet temporary energy demands. With the support of blockchain technology, it is developing an application to create a reliable energy trading ecosystem and remotely monitor energy trading activities between commercial entities. Experimental results show that the energy trading system is effective in finding, relating and directing consumers to consumers [32].

In their study, Xie et al. investigate the security and privacy issue in the transportation system in 5G-VANET with SDN. The proposed security framework uses blockchain technology for decentralization and immutability while designing vehicle IoT services, i.e. real-time cloud-based video report and trust management in vehicle messages [33].

As can be seen in the table 1, although the type of blockchain used varies, communication and data transfer is generally carried out over the roadside unit.

III. FUTURE WORKS

In future studies, it is foreseen that costly vehicles such as roadside units will be disabled. Roadside units dependency is costly. Because when it comes to communication between vehicles, roadside units are created within the scope of smart city studies. Depending on the length of the wireless technology used in roadside units, the number and naturally the cost of roadside units increase. If roadside units are phased out, a huge cost and dependency on wireless technologies can be avoided. Today, the fact that vehicles have an internet connection and they are described as connected cars paves the way for this situation.

In addition, if future studies will continue on blockchain technology, more efficient consensus algorithms may emerge. We also foresee that the type of blockchain used will be either a consortium or a hybrid model. Because, as can be seen in the literature review, consortium blockchain is a faster and more efficient technology in areas such as communication between vehicles with high mobility.

IV. CONCLUSION

As a result, when we look at the studies put forward, each study tries to create defense mechanisms against certain attack threats. In addition, in these studies, blockchain applications differ according to the types and contents specified under the block chain title.

When we examine the studies in the table in the literature section in detail, while blockchain is used especially in devices with high mobility, consortium blockchain is now used. The reason for this is that the public blockchain is very slow and the private blockchain behaves like a centralized structure. In private blockchain, the collection of the security element in one hand and the fact that all transactions go through a single device may cause some data not to be processed in the large systems. For this reason, consortium blockchain is preferred because it is easy to use in a distributed logic and is very fast when used with lightweight algorithms.

In addition, we are carrying out a study that will ensure a secure communication between vehicles by using light encryption algorithms without units such as roadside units. In this study, we also benefit from blockchain technology. In future studies, we will reveal the similar and different aspects of our study and the studies we examined in this study.

V. REFERENCES

[1] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, "Untangling blockchain: a data processing view of blockchain systems", *IEEE Transactions on Knowledge and Data Engineering*., vol. 30, no. 7, pp. 1366-1385, 2018.

[2] Üstün, Ece Su, *TBK Kapsamında Geleneksel Sözleşmeler ile Mukayeseli Olarak Akıllık*

Sözleşmeler Blokzincir Teknolojisi, Seçkin Yayıncılık, Ankara, 2021, s. 21.

[3] Bilgili, Fatih/Cengiz M. Fatih, "Bitcoin Özelinden Kripto Paralarının Eşya Niteliği Sorunu", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, c. 23, s. 2, ss. 3-23, 2019.

[4] V. Jindal and P. Bedi, "Vehicular ad-hoc networks: introduction, standards, routing protocols and challenges", *International Journal of Computer Science Issues*, vol. 13, pp. 44-55, 2016.

[5] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaria, "To Blockchain or Not to Blockchain: That Is the Question", *IT Professional*, vol. 20, no. 2, pp. 62–74, 2018.

[6] V. Buterin. (20.04.2022). *On Public and Private Blockchains, Ethereum Blog Crypto renaissance salon* [Online] Available: https://blog.ethereum.org/ 2015/08/07/on-public-and-private-blockchains/

[7] M. Hajar, C. Soumaya, K. Lyes, "An IoT blockchain architecture using oracles and smart contracts: the use-case of a food supply chain", *in: 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE*, pp. 1–6, 2019.

[8] M. Murat, "Blockchain ile güvenli elektronik sağlık sistemi", Yüksek Lisans, Bilgisayar Mühendisliği, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, 2018.

[9] S. Kardas, "Blokzincir teknolojisi: Uzlaşma protokolleri", *DÜMF Mühendislik Dergisi*, c. 10, s. 6, ss. 481–496, 2019.

[10] D. Meijer, "Consequences of the implementation of blockchain technology", M.S. thesis, Computer Science, Delft University of Technology, Delf, Netherlands, 2017.

[11] M. Zhou, L. Han, H. Lu, C. Fu, "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant", *Computer Networks*, vol. 172, pp. 107174, 2020.

[12] O.A. Wahab, A. Mourad, H. Otrok, J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks", *Expert System Applications*, vol. 50, pp. 40–54, 2016.

[13] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F.J. AparicioNavarro, A. Argyriou, H. Janicke, "A novel intrusion detection system against spoofing attacks in connected electric vehicles", *Array* vol. 5, pp. 100013, 2020.

[14] A.K. Malhi, S. Batra, H.S. Pannu, "Security of vehicular ad-hoc networks: a comprehensive survey", *Computers & Security* vol. 89, pp. 101664, 2019.

[15] M.R. Ghori, K.Z. Zamli, N. Quosthoni, M. Hisyam, M. Montaser, "Vehicular adhoc network (VANET)", *in: 2018 IEEE International Conference on Innovative Research and Development (ICIRD), IEEE*, pp. 1–6, 2018.

[16] M. Arif, G. Wang, M.Z.A. Bhuiyan, T. Wang, J. Chen, "A survey on security attacks in vanets: communication, applications and challenges", *Vehicular Communications* vol. 19, pp. 100179, 2019.

[17] R. Shrestha, R. Bajracharya, A.P. Shrestha, S.Y. Nam, "A new type of blockchain for secure message exchange in VANET", *Digital Communications and Networks*. vol. 6, no. 2, pp. 177–186, 2020.

[18] C. Chen, J. Wu, H. Lin, W. Chen and Z. Zheng, "A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110-9121, 2019.

[19] A. Mostafa, "VANET Blockchain: A General Framework for Defecting Malicious Vehicles", *Journal of Communications*, vol. 14, pp. 356-362, 2019.

[20] A.S. Khan, K. Balan, Y. Javed, S. Tarmizi, J. Abdullah, "Secure trustbased blockchain architecture to prevent attacks in VANET", *Sensors*, vol. 19, no. 22, pp. 4954, 2019.

[21] N. Malik, P. Nanda, X. He and R. Liu, "Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach," *2019 18th IEEE International Conference On Trust, Security And Privacy*

In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 34-41, 2019.

[22] M. Li, J. Weng, A. Yang, J. -N. Liu and X. Lin, "Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11248-11259, 2019.

[23] D. Zheng, C. Jing, R. Guo, S. Gao and L. Wang, "A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs," in *IEEE Access*, vol. 7, pp. 117716-117726, 2019.

[24] C. Lai and Y. Ding, "A Secure Blockchain-Based Group Mobility Management Scheme in VANETs," *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, pp 340–345, 2019.

[25] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon and S. H. Ahmed, "Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure," *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1-6, 2019.

[26] J. Gao *et al*., "A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks," in *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278-4291, 2020.

[27] W. Hu, Y. Hu, W. Yao and H. Li, "A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles," in *IEEE Access*, vol. 7, pp. 139703-139711, 2019.

[28] X. Liu, H. Huang, F. Xiao, and Z. Ma, “A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101– 4112, May 2020, doi: 10.1109/JIOT.2019.2957421.

[29] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat and S. Nandi, "Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3616-3630, 2021.

[30] Z. Lu, Q. Wang, G. Qu and Z. Liu, "BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),* pp. 98–103, 2018.

[31] C. Wang, J. Shen, J. -F. Lai and J. Liu, "B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs," *in IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1386-1396, 2020.

[32] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis and H. Ahmadi, "Blockchain-Based Energy Trading in Electric-Vehicle-Enabled Microgrids," *in IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 66-71, 2020.

[33] L. Xie, Y. Ding, H. Yang, and X. Wang, “Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets,” *IEEE Access*, vol. 7, pp. 56 656–56 666, 2019.