A Privacy Preserving Hybrid Blockchain based Announcement Scheme for Vehicular Energy Network

Abid Jamal[1], Sana Amjad[1], Usman Aziz[2], Muhammad Usman Gurmani[1], Saba Awan[1], Nadeem Javaid[1,*]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Science, COMSATS University Islamabad, Attock 43600, Pakistan
Email: abid.jamal.turi@gmail.com, sanaamjad702@gmail.com,
usmanaziz91@gmail.com, usmankhangurmani@gmail.com, sabaawan046@gmail.com,
*Corresponding Author: nadeemjavaidqau@gmail.com; www.njavaid.com

Abstract*—The vehicular announcement is an essential component of the Intelligent Transport System that enables vehicles to share important road information to reduce road congestion, traffic incidents, and environmental pollution. Due to the multiple security issues like single point of failure, data tampering, and false information dissemination, many researchers have proposed Blockchain (BC) based solutions to ensure data correctness and transparency in the vehicular networks. However, these schemes suffer from high computational cost and storage overhead due to the use of unsuitable BC on the vehicular layer, costly authentication schemes, and inefficient digital signature verification methods. Moreover, the privacy leakage can occur due to publicly available reputation values and lack of pseudonyms update mechanism. In this paper, we propose a privacy-preserving hybrid BC based vehicular announcement scheme to enable secure and efficient announcement dissemination. We use IOTA Tangle to enable the benefits of BC on vehicular layer while reducing the storage and computational cost. We employ Elliptic Curve Cryptography based pseudonym update mechanism for hiding the real identities of vehicles. To prevent false information dissemination in the network, we propose a reputation-based incentive mechanism for encouraging the users to provide honest ratings about the announcement messages. Furthermore, we use Cuckoo Filter to enable lightweight trustworthiness verification of the vehicles without revealing their reputation values. We also employ a batch verification mechanism to reduce the delays caused by digital signature verification. Moreover, we use InterPlanetary File System, and Ethereum BC for ensuring data availability and secure trust management.

I. Introduction

Intelligent Transport System (ITS) plays a prominent role in enhancing smart cities by reducing traffic congestion and roadblocks and providing efficient routes to drivers. One of the ITS applications is Vehicular Energy Network (VEN). VENs are based on standards of Mobile Ad-hoc Network (MANET) and they enable vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication for energy trading and dissemination of useful information about road and weather conditions, roadblocks, alternative routes, etc. Vehicles in VENs are equipped with an On-Board Unit (OBU), which uses Dedicated Short-Range Communication (DSRC) protocol for communication. Along with many benefits, VENs are also vulnerable to different attacks like Single Point of Failure (SPoF), false information dissemination, privacy leakage, etc., due to the open and trustless environment. To overcome these issues, several researchers have proposed Blockchain (BC) based solutions for VENs.

In recent years, the Distributed Ledger Technology (DLT) has gained immense popularity in academia and industry due to its features like transparency, non-repudiation, tamper-resistance, etc. BC is a widely adopted DLT in which transaction data is stored in cryptographically linked blocks. The set of linked blocks is considered as a distributed ledger and it is shared with all the network participants. BC was initially introduced by Satoshi Nakamoto in 2008 as a backbone for the first ever digital currency named Bitcoin [1]. In BC, new blocks are added to the chain by the process of mining. BC provides captivating features like non-repudiation, data transparency, data availability, tamper-resistance, etc. Due to these features, BC is applied in many different sectors like healthcare, smart cities, supply chain, vehicular networks, etc.

Recently many researchers have employed BC to overcome the trust and security issues of the traditional VENs. Besides the many benefits of BC based VENs, it is susceptible to many potential flaws, which can limit the efficiency of the vehicular networks. Many of the existing BC based vehicular networks use Ethereum BC on the vehicle layer [2], [3], which increases the storage and computational cost on the vehicles. Some researchers have used Directed Acyclic Graph (DAG) based DLT named IOTA Tangle in vehicular networks [4], [5]. As IOTA Tangle relies on data pruning method for saving storage space, it can cause data unavailability due to which malicious users can repudiate sharing false announcements in the network. Generally, in BC based vehicular networks, pseudonym mechanism are used to preserve the vehicles' privacy [6], [7]. However, due to use of static pseudonym identity, the real identities of the users can be inferred by background knowledge attacks. These attacks are overcome by pseudonym update mechanism [8]. However, due to lack of vehicle traceability, the internal attackers can disseminate false

information in the network. To overcome this issue, BC based reputation schemes are introduced to identify the malicious users. As the reputation scores of the vehicles are publicly stored on BC, the adversaries can exploit the predictable patterns in the reputation values to perform vehicle tracing attacks.

To address the aforementioned issues, we propose a privacy-preserving vehicular announcement scheme based on hybrid BC. In our proposed scheme, we use IOTA Tangle to enable zero-value transactions, high throughput and low storage cost on vehicle layer. Moreover, to preserve the privacy of the vehicles, we use Elliptic Curve Cryptography (ECC) based dynamic pseudonyms mechanism to hide vehicles' real identities. Also, we use Cuckoo Filter (CF) for hiding the predictable patterns in the reputation values. To further enhance the efficiency of the proposed scheme, we use batch verification scheme to enable simultaneous verification of multiple vehicle rating messages. In addition, data storage and availability issues are resolved by using InterPlanetary File System (IPFS).

II. Related Work

A. Authentication

The vehicular networks require a secure and efficient authentication scheme to prevent malicious users from entering the network. The authors in [9] address the privacy leakage caused by centralized Public Key Infrastructure. They propose a distributed pseudonym management system that allows the users to create their own pseudonyms. However, their proposed scheme fails to ensure conditional privacy, making malicious vehicles untraceable. In [2], authors address the issue of SPoF in conventional centralized authentication scheme in vehicular networks. They use edge computing and local BC to efficiently store the registration and trust information of vehicles to ensure data transparency. However, their proposed scheme is prone to privacy leakage due to publicly available trust values. In [6], [8], the authors propose a certificate revocation mechanisms in vehicular networks to efficiently manage the Certificate Revocation List (CRL). The CRL is used for verifying whether a certificate of a certain user is revoked. The authors in [6] enable privacy preservation in BC based certificate revocation mechanism by introducing pseudonym shuffling mechanism. Moreover, authors in [8] reduce the cost of CRL management by using an efficient data structure called Merkle Patricia Tree. However, due to the use of inefficient signature verification mechanism, both schemes add unnecessary verification delays.

B. Trust Management

In [10], authors propose a BC based incentive scheme to motivate the users to share important traffic information in the network. However, their proposed scheme is vulnerable to privacy leakage due to the use of static pseudonyms. The authors in [11] propose a privacy-preserving incentive scheme to encourage user participation while preserving the privacy. They develop an anonymous vehicular announcement aggregation protocol to prevent unique identification of a vehicle in network. However, in addition to the delays due to inefficient message verification, this scheme also suffers from an overwhelming storage cost due to inefficient key management. Moreover, in [12], authors address the security and trust issues in BC based Industrial Internet of Things. They use a monetary incentive mechanism to encourage the honest contribution. However, due to the lack of a batch verification mechanism, their proposed scheme suffers from unnecessary verification delays. In [13]–[15], authors address the trust and authentication issues in Internet of Vehicles. They propose a decentralized trust management scheme based on Hyperledger Fabric to store the nodes' trust values. However, due to the open availability of trust values, this scheme is vulnerable to tracking attacks and privacy leakage. In [16], authors propose a consortium BC based data and energy trading scheme to enable decentralized trading. They use bloom filters to prevent data duplication and smart contracts to overcome trading disputes. In [17], authors propose a BC based food supply chain management scheme to enable users' trust and ensure products traceability. They use smart contracts to store the records in an immutable manner.

C. Privacy

The privacy preservation is of utmost importance in a vehicular network. The lack of privacy can allow malicious users to perform vehicle tracking attacks. In this regard, authors in [7] address the false information dissemination in vehicular network due to the lack of conditional anonymity. They develop a BC based pseudonym mechanism to hide the real identity of the vehicles. However, due to the use of centralized cloud server for storage, their proposed model is vulnerable to SPoF. Moreover, authors in [18] developed a pseudonym mechanism that allows vehicle users to generate and update pseudonyms for themselves without CA's intervention. However, the self-generated pseudonym scheme can allow malicious vehicles to spam the network with false information.

D. Efficiency

In [3], authors propose Proof of Event consensus mechanism to reduce consensus delays and ensure the validity of the events shared by the vehicles. However, their proposed scheme is susceptible to privacy leakage. In [19], authors develop a joint Proof of Stake and modified Practical Byzantine Fault Tolerance consensus algorithm for reducing the resource requirement to perform consensus. However, in their proposed scheme, privacy leakage can occur due to unrestricted access to the reputation values. In [20], authors address location privacy leakage in the smart parking applications due to publicly available location data of the users. Moreover, they address the issue of the existing centralized smart parking schemes that are vulnerable to SPoF. The authors use group signatures, bloom filters, and vector-based encryption to enable anonymous authentication and malicious users' traceability. However, their proposed scheme lacks a reputation mechanism which makes the system vulnerable to the internal attacks. Moreover, in the proposed scheme, an unsuitable BC is used on the vehicular

layer. The conventional BC schemes are not suitable for the vehicular layer due to the resource constrained OBU of the vehicles. The authors in [10], [21], use IPFS to efficiently store the transaction data. They also use a reputation management system to store the reputation values of the vehicles. However, their proposed scheme is susceptible to privacy leakage due to openly available reputation values and static pseudonyms. In [22], [23], authors have utilized consortium BC to store and share the data efficiently. However, these schemes lack batch verification mechanism and use unsuitable BC on the vehicle layer. In [4], authors address high cost of storing BC ledger on vehicles in vehicular social networks. They use a DAG based DLT on vehicle layer to efficiently reduce the storage cost of the ledger on vehicles. However, their proposed scheme does not preserve the privacy of the vehicles which can lead to reduced user trust.

III. Problem Statement

In [24], [25], BC based announcement schemes are proposed to enable secure and trustworthy announcement dissemination in VANETs. However, due to the use of unsuitable BC on the vehicle layer, these schemes incur excessive storage and computational cost on resource constrained vehicles. In [4], [5], a lightweight DAG based DLT is proposed for vehicular networks to overcome the excessive storage cost of conventional BC. In [4], DAG-chain is used, whereas in [5], IOTA is used for efficient and distributed storage of the transaction records on vehicles. However, due to the use of static pseudonyms in [4], the adversaries can identify a vehicle by performing background knowledge attacks. Moreover, due to lack of incentive mechanism in [5], the vehicles are not encouraged to give honest ratings about their peers. In [26], ABE-based authentication scheme is proposed to authenticate the vehicles while preserving their privacy. However, due to the high computational cost of ABE and use of inefficient message verification method, this scheme introduces excessive delays, which can reduce the overall efficiency of the network. In [12], [25], BC based reputation mechanisms are proposed to prevent false information dissemination in vehicular networks. In these schemes, the vehicles verify the trustworthiness of messages by accessing the reputation scores of other vehicles available on the BC ledger. However, due to the public availability of the vehicles' reputation scores on BC, the adversaries can trace a vehicle by utilizing the predictable patterns in the reputation values.

IV. System Model

A hybrid blockchain based announcement framework is proposed to improve efficiency, preserve privacy, and enable secure communication in VENs. The proposed model consists of three layers as depicted in Figure 1. The first layer is IOTA Tangle layer, wherein the vehicles communicate with each other and with Roadside Units (RSUs) via IOTA Tangle, which is a DAG based DLT. The second layer is the BC layer, which consists of RSUs and Certificate Authority (CA). RSUs are connected to each other via wired connection and they manage the overall network activities. The third layer is the storage layer which consists of IPFS. RSUs offload the excessive historical data to IPFS to reduce the storage cost and ensure the data availability. The proposed model in Figure 1 contains a mapping table of the identified limitations and their proposed solutions. The limitations addressed in this proposed model range from L1 to L6 and the solutions proposed range from S1 to S7. The L1 refers to the computationally complex authentication scheme. It is mapped with the solution S1 using Elliptic Curve Digital Signature Algorithm (ECDSA) based digital certification scheme. The L2 refers to the privacy leakage due to predictable patterns in publicly available reputation information of the vehicles. This limitation is mapped with S2 using CF for storing the reputation values. The L3 shows the use of sequential message verification method, which can cause delays in the message verification process. The proposed solution S3 overcomes this issue using batch verification method. L4 indicates the various shortcomings of the conventional blockchain schemes which makes them unsuitable for the vehicular layer of the VEN. These shortcomings include low transaction throughput, lack of microtransactions and high storage cost on vehicles. S4 and S7 overcome these issues by using IOTA Tangle and IPFS. The L5 refers to the lack of incentive mechanism, which can impede the vehicle cooperation in the network. This limitation is mapped with the solution S5 using of reputation based incentive scheme. The L6 refers to the privacy leakage due to the use of static pseudonym. This limitation is mapped with S6, which relates to updating the pseudonym on regular basis to minimize the risk of privacy leakage.

A. Entities

The following is a brief description of our proposed model's entities.

1) Certification Authority: In VEN, the CA is an essential entity which allows only the authorized users to join the network. The CA is assumed to be fully trusted and secure against any kind of attacks. In the proposed model, RSUs and vehicular nodes provide their true identity information to CA for registration. The CA generates pseudonym certificates for the vehicles. The CA keeps an encrypted copy of a mapping between true identity and the pseudonym of the vehicle to enable conditional anonymity. So that in case of disputes, the digital certificates of the malicious vehicles can be revoked and their true identity can be revealed to prevent them from rejoining the network.

2) Vehicles: In VENs, each vehicle is equipped with an OBU which enables V2V and V2I communication via DSRC protocol. The OBU of the vehicles is considered as a tamper-proof device and is used for storing the private keys of the vehicles. The V2V communication includes announcements related to traffic conditions, road incidents, and advertisements etc. To reduce false information dissemination in the network, the vehicles provide ratings about the received announcements. In return, the vehicles receive incentives for giving the honest

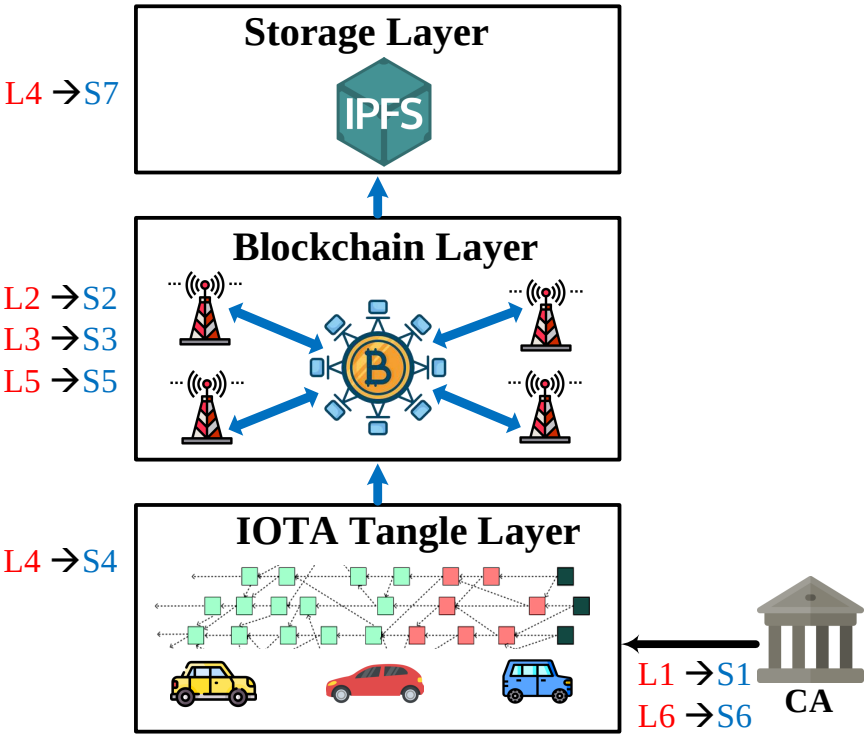

Fig. 1. Proposed System Model

ratings and punishment for the dishonest ratings and false announcements.

3) Roadside Units: In VENs, RSUs manage the overall network by providing different services to the vehicles. RSUs are connected to each other via wired connection and they have high computational capabilities. In our proposed model, RSUs are the part of both, the IOTA Tangle layer and the BC layer. On IOTA Tangle layer, the RSUs act as full nodes and store the vehicles' announcement record shared on Tangle to ensure data availability. In BC layer, the RSUs act as authorized node and are responsible for:

- vehicle reputation calculation based on Tangle record and user feedback,
- adding pseudo-IDs of malicious users to a CF,
- performing consensus,
- batch verification of message signatures, and
- uploading the historical data to IPFS.

4) IOTA Tangle: The conventional blockchain schemes are not suitable for vehicular networks due to multitude of reasons including, low transaction throughput, high storage requirement, lack of microtransaction etc. To overcome these limitations, IOTA Tangle is used in the proposed scheme. IOTA tangle is a DAG based distributed ledger technology, which supports microtransactions, provides high transaction throughput and reduces storage overhead. In the proposed model, IOTA is used for storing the announcement sharing records in a distributed ledger. In addition, it enables non-repudiation so that vehicles cannot deny sending any announcement message. Hence, the vehicles only disseminate accurate announcements in the network.

5) Blockchain: In the proposed scheme, Ethereum BC is applied on RSUs. The use of BC ensures data integrity, transparency and immutability. The complete Tangle record is backed up on IPFS and its hash is stored on BC to avoid data loss, which may occur due to data pruning on IOTA layer. Also, the CF generated by RSUs are stored on the BC for trust verification. The data in BC is accessed via smart contracts.

6) Cuckoo Filter: The CF is a new data structure proposed in [27] that replaces Bloom Filter as a method for testing whether an element belongs to a set or not. It uses Cuckoo Hashing and is designed to store items efficiently while targeting low false positive rate and requiring significantly lesser storage space than Bloom Filter.

7) InterPlanetary File System: IPFS is a distributed data storage system. In IPFS, a distinct hash value is generated for each file which is then used for file retrieval. In the proposed model, the historical Tangle data is uploaded to IPFS to enable system's scalability and efficiency. Whereas, only the hashes of the uploaded files are stored in the BC, which significantly reduces the storage cost.

V. Conclusion

In this paper, a hybrid Blockchain based vehicular announcement scheme is proposed for VENs. IOTA Tangle is employed to reduce the resource utilization on vehicle layer. The IPFS is used for ensuring the data availability while

reducing the overall storage cost of the system. The Ethereum BC is used on the RSU layer to store IPFS hashes of the sensitive data. The ECC-based pseudonym update mechanism is used to enable conditional anonymity. Moreover, a reputation-based incentive mechanism is utilized to encourage users to share the honest ratings. CF are implemented to prevent background knowledge attacks by hiding predictable patterns in the reputation values of the vehicles. In the future, the proposed scheme will be validated through simulations on the real-world networks.

REFERENCES

[1] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[2] Shrestha, Rakesh, Rojeena Bajracharya, Anish P. Shrestha, and Seung Yeob Nam. "A new type of blockchain for secure message exchange in VANET." Digital communications and networks 6, no. 2 (2020): 177-186.

[3] Yang, Yao-Tsung, Li-Der Chou, Chia-Wei Tseng, Fan-Hsun Tseng, and Chien-Chang Liu. "Blockchain-based traffic event validation and trust verification for VANETs." IEEE Access 7 (2019): 30868-30877.

[4] W. Yang, X. Dai, J. Xiao and H. Jin, "LDV: A Lightweight DAG based Blockchain for Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5749-5759, June 2020, doi: 10.1109/TVT.2020.2963906.

[5] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum and D. N. K. Jayakody, "A Blockchain based Framework for Lightweight Data Sharing and Energy Trading in V2G Network," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5799-5812, June 2020, doi: 10.1109/TVT.2020.2967052.

[6] Lei, Ao, Yue Cao, Shihan Bao, Dasen Li, Philip Asuquo, Haitham Cruickshank, and Zhili Sun. "A blockchain based certificate revocation scheme for vehicular communication systems." Future Generation Computer Systems 110 (2020): 892-903.

[7] Pu, Yuwen, Tao Xiang, Chunqiang Hu, Arwa Alrawais, and Hongyang Yan. "An efficient blockchain-based privacy preserving scheme for vehicular social networks." Information Sciences 540 (2020): 308-324.

[8] Lu, Zhaojun, Qian Wang, Gang Qu, Haichun Zhang, and Zhenglin Liu. "A blockchain-based privacy-preserving authentication scheme for vanets." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 27, no. 12 (2019): 2792-2801.

[9] Benarous, Leila, Benamar Kadri, and Ahmed Bouridane. "Blockchain based Privacy-Aware Pseudonym Management Framework for Vehicular Networks." Arabian Journal for Science and Engineering (2020): 1-17.

[10] Khalid, Adia, Muhammad Sohaib Iftikhar, Ahmad Almogren, Rabiya Khalid, Muhammad Khalil Afzal, and Nadeem Javaid. "A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs." Information Processing & Management 58, no. 2 (2021): 102464.

[11] Li, Lun, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles." IEEE Transactions on Intelligent Transportation Systems 19, no. 7 (2018): 2204-2220.

[12] Wang, Eric Ke, Zuodong Liang, Chien-Ming Chen, Saru Kumari, and Muhammad Khurram Khan. "PoRX: A reputation incentive scheme for blockchain consensus of IIoT." Future Generation Computer Systems 102 (2020): 140-151.

[13] Sun, Lijun, Qian Yang, Xiao Chen, and Zhenxiang Chen. "RC-chain: Reputation-based crowdsourcing blockchain for vehicular networks." Journal of Network and Computer Applications 176 (2021): 102956..

[14] Zhang, Xiaohong, and Di Wang. "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain." IEEE Access 7 (2019): 97281-97295.

[15] Malik, Nisha, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu. "Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology." Wireless Networks 26, no. 6 (2020): 4207-4226.

[16] Sadiq, Ayesha, Muhammad Umar Javed, Rabiya Khalid, Ahmad Almogren, Muhammad Shafiq, and Nadeem Javaid. "Blockchain based Data and Energy Trading in Internet of Electric Vehicles." IEEE Access (2020).

[17] Shahid, Affaf, Ahmad Almogren, Nadeem Javaid, Fahad Ahmad Al-Zahrani, Mansour Zuair, and Masoom Alam. "Blockchain-based agri-food supply chain: A complete solution." IEEE Access 8 (2020): 69230-69243.

[18] Zhao, Ning, Hao Wu, and Xiaonan Zhao. "Consortium Blockchain based secure software defined vehicular network." Mobile Networks and Applications 25.1 (2020): 314-327.

[19] Sutrala, Anil Kumar, Palak Bagga, Ashok Kumar Das, Neeraj Kumar, Joel JPC Rodrigues, and Pascal Lorenz. "On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of vehicles deployment." IEEE Transactions on Vehicular Technology 69, no. 5 (2020): 5535-5548.

[20] Zhang, Can, Liehuang Zhu, Chang Xu, Chuan Zhang, Kashif Sharif, Huishu Wu, and Hannes Westermann. "BSFP: Blockchain-Enabled Smart Parking with Fairness, Reliability and Privacy Protection." IEEE Transactions on Vehicular Technology 69, no. 6 (2020): 6578-6591.

[21] Firdaus, Muhammad, and Kyung-Hyune Rhee. "On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks." Applied Sciences 11.1 (2021): 414.

[22] Rahman, Md Abdur, Md Mamunur Rashid, M. Shamim Hossain, Elham Hassanain, Mohammed F. Alhamid, and Mohsen Guizani. "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city." IEEE Access 7 (2019): 18611-18621.

[23] Li, Kang, Wang Fat Lau, Man Ho Au, Ivan Wang-Hei Ho, and Yilei Wang. "Efficient message authentication with revocation transparency using blockchain for vehicular networks." Computers & Electrical Engineering 86 (2020): 106721. .

[24] Ma, Jianfeng, Tao Li, Jie Cui, Zuobin Ying, and Jiujun Cheng. "Attribute-Based Secure Announcement Sharing among Vehicles Using Blockchain." IEEE Internet of Things Journal (2021).

[25] X. Liu, H. Huang, F. Xiao and Z. Ma, "A Blockchain based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4101-4112, May 2020, doi: 10.1109/JIOT.2019.2957421.

[26] Q. Feng, D. He, S. Zeadally and K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4146-4155, June 2020, doi: 10.1109/TII.2019.2948053

[27] Fan, Bin, Dave G. Andersen, Michael Kaminsky, and Michael D. Mitzenmacher. "Cuckoo filter: Practically better than bloom." In Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies, pp. 75-88. 2014.