INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 1, PP. 133–138
Manuscript received February 9, 2022; revised February, 2022. DOI: 10.24425/ijet.2023.144342

Blockchain System for Secure and Efficient UAV-to-Vehicle Communication in Smart Cities

Suganthi Evangeline, Ashmiya Lenin, and Vinoth Babu Kumaravelu

***Abstract*—In a smart city environment, Intelligent Transportation System (ITS) enables the vehicle to generate and communicate messages for safety applications. There exists a challenge where the integrity of the message needs to be verified before passing it on to other vehicles. There should be a provision to motivate the honest vehicles who are reporting the true event messages. To achieve this, traffic regulations and event detections can be linked with blockchain technology. Any vehicle violating traffic rules will be issued with a penalty by executing the smart contract. In case any accident occurs, the vehicle nearby to the spot can immediately send the event message to Unmanned Aerial Vehicle (UAV). It will check for its credibility and proceed with rewards. The authenticity of the vehicle inside the smart city area is verified by registering itself with UAVs deployed near the city entrance. This is enabled to reduce the participation of unauthorized vehicles inside the city zone. The Secure Hash Algorithm (SHA256) and Elliptic Curve Digital Signature Algorithm (ECDSA-192) are used for communication. The result of computation time for certificate generation and vehicles involvement rate is presented.**

***Keywords*—blockchain technology; elliptic curve digital signature algorithm (ECDSA-192); intelligent transportation system (ITS); smart contract; unmanned aerial vehicle (UAV); secure hash algorithm (SHA); vehicular ad hoc network (VANET)**

I. Introduction

VEHICULAR Ad hoc Network (VANET) is expanding to the decentralized technology called the Internet of Vehicles (IoV). IoV mainly emphasizes communication between nodes in a network by unifying various communication technologies. It offers types of assistance and arrangements that further develop fulfillment, security, and protection of vehicles and clients in the network. IoV faces challenges like, dealing with resource constraints of devices in terms of battery, computational power, which limits the algorithm implementation. The main test is to confront its security and protection to the common information like pictures, area, individual information. The smart city is a perception that aims at employing various types of communication technologies to improve the lives of the population in that city [1]. IoV is the derived class from the Internet of Things (IoT) which also involves UAV to increase the capacity and coverage of existing cellular networks [2]. In particular, UAVs can be deployed as Aerial Base Station (ABS) to support wireless communication in remote areas, emergency situations, medicine, structural inception, and traffic-monitoring applications. The quick development of UAV innovation attached with its adaptability of improvement and network is making possible revenue to cellular administrators [3]. In the smart city environment, the nodes (vehicles, mobile devices, infrastructure units) are connected to the cloud for delivering services to the residents in that city. The data should be securely disseminated in such environments. There is a need for decentralized and distributed ledger technology, which involves secure way of data transmission. Because of this nature, Blockchain technology has attracted high interest in many areas such as finance, health care, supply chain, transportation, and also in defense. It is mainly employed for maintaining transparency, integrity, identity management, and also to address some threats. There is no need for a centralized entity to control or govern all activities in Blockchain. It incorporates cryptographic techniques and double hashing approach; tampering of the message is not possible. With the smart contract feature of Blockchain, the event is executed automatically based on trigger values. Suppose, in the case of an auction, the user who bids high will get the ownership of the property. The process of auctioning, ownership changing and amount settlement is automatically done by the smart contract which is deployed in the blockchain network. Blockchain likewise gives the advantage of interoperability, since it is conveyed on top of the peer-to-peer organization. In this work, we propose a blockchain-based data transmission where the vehicle is connected with the UAV, and all transactions are stored in the blockchain network. We also execute the smart contract functionality in monitoring the vehicle's behavior in a smart city.

II. Related Works

In recent years, advances in UAV in research and industry have developed many applications like security, supply chain, surveillance, exploration, response during an emergency. UAVs can be deployed in smart cities and create positive impacts for society. Various applications of UAV network with blockchains such as security, decentralized storage, and the challenges in the integration of UAV and blockchain is presented [3]. In [4], the concepts of UAV-assisted smart city, solutions for UAV-assisted IoV in smart cities based on blockchain technology are discussed. The authors in [5]

Suganthi Evangeline is with Department of Electronics and Communication Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India (e-mail:evangelineme4@gmail.com).

Ashmiya Lenin is PG Scholar in Communication Systems, Karunya Institute of Technology and Sciences, Coimbatore, India (e-mail:ashmiyalenin21@gmail.com).

Vinoth Babu Kumaravelu is with School of Electronics Engineering, VIT University, Vellore, India (e-mail:vinothbab@gmail.com).

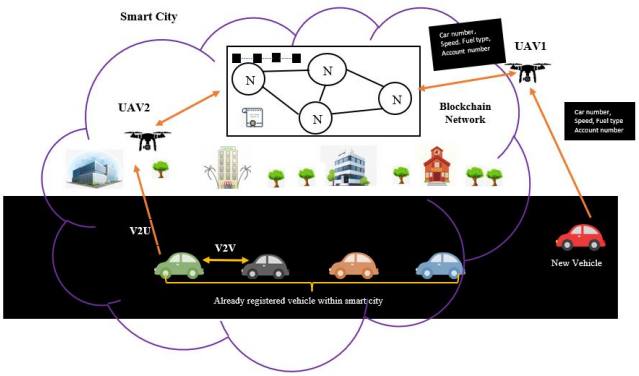

Fig. 1. System model of the proposed work

proposed a decentralized authentication scheme for IoV which uses the consensus mechanism of blockchain technology. It improves the quality of the authentication process and protects IoV against malicious attacks. The authors in [6] proposed blockchain-assisted UAVs to meet user demands in smart city scenarios. Drones are used for delivery within the smart city and each UAV is deployed with public and private blockchains. In [7], the deployment scenario of UAV within the smart system and its integration with blockchain technology and the challenges around it are discussed. Integration of UAV, blockchain, IoT is introduced, solutions based on blockchain for security issues in UAV is briefed in [8]. It mainly focuses on applying the principles of blockchain technology in the domain of UAV. The authors in [9] proposed an Internet of Drones system using blockchain technology. Proof of concept used illustrates that the system offers improved accuracy in detecting humans, transparency, increased operation time of drones, security, and traceability.

UAV-assisted data dissemination scheme is proposed in [10] for VANETs. To predict the vehicle mobility recursive least square (RLS) algorithm is used. This technique minimizes data dissemination delay and improves throughput. In [11] the authors proposed a decentralized architecture that brings in blockchain technology to secure the location and identity privacy in VANET. In [12], a multi-UAV surveillance scheme based on blockchain technology is proposed. It has two main functionalities; the first one is, the path of each UAV is coordinated using the game theory approach implemented into the smart contract and the second one is to grant financial transactions between the system users. In [13] the authors used a blockchain-based framework for delivering the goods in the COVID-19 scenario using drones. Smart contracts are deployed to enable trust and process the payment. This framework is evaluated based on transaction time, gas price, and mining time.

III. BLOCKCHAIN SYSTEM IN UAV-VANET

A new blockchain is proposed to solve the issues related to message transmission in VANET with UAV. The system model is presented in Figure.1. This approach uses an immutable distributed database for message transmission, where all nodes in the blockchain can able to access the information. Unlike cryptocurrency transactions that happen in traditional blockchain, in this scenario, the event and vehicle information are considered as transactions. The event information includes traffic jams, road accidents, environmental hazards and traffic rules violations. All vehicles are equipped with Global Positioning System (GPS) and also have a certificate of location based on Proof of Location (PoL).

- UAV: They are responsible for enlisting, confirming, and giving location certificates to the new vehicles coming into the smart city.
- Vehicles: There are two categories of vehicles, new and already registered. They generate event messages and communicate with UAVs and also with other vehicles.
- VANET messages: There are two types of messages generated from vehicles. They are safety and registration message. Registration messages are sent to UAV to inform about its status to join and access the services in the smart city. The safety messages are broadcasted to UAV and with other vehicles for informing about accidents, hazards, traffic status.
- Blocks: A block in a distributed database consists of a block header and a body. The header includes the previous block hash, nonce, difficulty target, timestamp, and Merkle root. The body consists of a list of events generated by vehicles.
- Certificate of location: Each vehicle needs a PoL to verify that the vehicle is located near the event spot. It is also used as proof in an event message that assists in the blockchain. The UAV acts as a validator to provide the certificate of location to the vehicles after successful registration.

The process of getting the certificate of location is given in Fig.2.

For our proposed work, issuing a location certificate for a vehicle that holds a specific private key. The private key remains masked and only public key is exposed to the UAV. For a given pair (K_{PV},k_{uv}) the location certificate attests that a vehicle containing the was near the UAV at the time of issuing. The certificate issue protocol involves the following steps.

1. The vehicle initiates the message with its registration details to UAV including its K_{PV}.

2. The UAV sends a random session ID S_{ID} to the vehicle.

3. The vehicle directs back the S_{ID} signed with k_{uv}.

4. The UAV checks the time elapses between step 2 and step 3 process and verifies the genuineness of the signature using and sends the location certificate to the requested vehicle signed by the private key of UAV K_{PU}.

The vehicle is unable to create a certificate without a UAV because a valid certificate requires the signature of the UAV. The S_{ID} can only be signed after the beginning of the session because it is not revealed before the session. The vehicle that can sign the S_{ID} with k_{uv} must be near to UAV, to respond in a reduced latency.

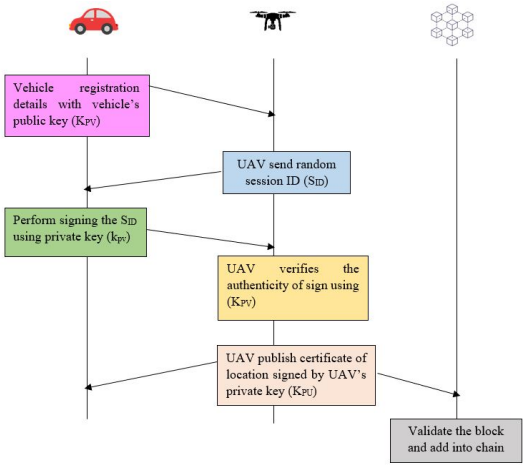

Fig. 2. Steps involved in getting certificate

IV. PROPOSED BLOCKCHAIN SYSTEM

In this section, we propose a blockchain-based data transmission in the smart city environment. In smart city scenario, a new vehicle needs to get the certificate of location to attest its location at a given time. The certificate is provided by the UAV. In the traditional blockchain, a block is sent wide to all other nodes in the blockchain network for validation process called mining. Here, in our proposed work, the block is only transmitted locally. Any vehicle can query the details about other vehicles in the blockchain. The new block is generated and accumulated in the pool of unconfirmed transactions. Once a new block is generated it is broadcasted to the network and updated in the blockchain.

The vehicle which is coming first time to the smart city set up, it should be registered in the database. To support in registration, UAVs are deployed near the city entrance. Because of this, no vehicle can join the network without being checked [14]. The vehicle will register basic details such as registration number, distance covered, account number and its public key (K_{PV}). The UAV validates the authenticity by sending S_{ID} . To do the process of mining, the blockchain network has few nodes called miners, they will be rewarded in terms of cryptocurrencies or crypto tokens as incentives. Once the block is mined, it is added to the blockchain. The registered vehicle will have a unique identity (U_{ID}) and virtual identity (V_{ID}) . When a registered vehicle encounters an event such as accident, it will broadcast to neighboring vehicles or UAVs. On receiving an event message, the neighboring vehicle or UAV verifies the certificate of location and also other parameters. Any vehicle wishes to access any services in smart city, the vendors will get the details about the new vehicle and provide the necessary services. Similarly, when a vehicle is intervening in some traffic regulations, the smart contract will be automatically executed and it will withdraw the penalty from the respective vehicle's accounts.

Algorithm 1 Speed violation algorithm

Assume: A vehicle exceeds the speed limit
$Vehicle(U_{ID}, V_{ID}, I_{ID}, loc, D_t, PoL, speed, T_s)$→UAV
If $V_{ID} \in U_{ID}$ && $speed > nomial\ speed$,
Execute penalty function
  function penalty (VehicleAddress, VehicleBalance, PenaltyAmount)
    Get input: VehicleBalance
    VehicleBalance = VehicleBalance-PenaltyAmount
    emit VehicleAddress, VehicleBalance
  end function
else
  discard the event message
end if

Fig. 3. Speed violation algorithm

V. SECURE MESSAGE DISSEMINATION IN UAV-VANET

In smart city environment, any registered vehicle can transmit an incident message E_i, to UAVs. When a UAV receives an E_i, it checks for location certificate embedded along with the incident message. The incident message includes details such as V_{ID}, incident-ID (I_{ID}), incident location (loc), direction of travel (D_t), PoL, speed, timestamp (T_s) etc. The UAV sends the incident message to the blockchain network, where each mining nodes will validate the incident and verify the parameters. The mining nodes will verify the following details such as, PoL and timestamp. The smart contract is executed based on the incident parameters. In this, we have considered three case scenarios,

Case 1: where a vehicle is exceeding the speed limit, which is considered as an incident. The same vehicle will send E_i to UAVs, the node in the blockchain will execute the smart contract by which the penalty is deduced from the vehicle account. During the registration phase by UAV, the details related to account number are registered and included as a new user in smart contract entry. Hence, without any human intervention, the contract is executed and data is transmitted into the blockchain network. Blockchain enables the UAV organizations to encode the information and store them in the blockchain consequently making it out of reach to anybody without the authentic decoding key. The speed violation algorithm is given in Fig. 3.

Case 2: When a vehicle identifies some accident or traffic collision it initiates an event message E_i, if it is a true incident, an incentive is added to the vehicle's account. This is encouraging each vehicle in the smart city environment to act honestly and help other vehicles. It will increase the vehicle's renown value. The true event dissemination is given in Fig. 4.

Case 3: Consider an intruder vehicle, which finishes its registration and started to misbehave by sending an incident message E_k which indicates some accident. Along with the event message, it will send its vehicle location and randomly send some accident location. When the UAV identifies that it is a false incident, the vehicle's renown value is decreased and also its registration is canceled by removing it from the network. In our proposed model, all of the verified events are stored in Interplanetary File System (IPFS) in a decentralized manner. UAVs are responsible to send event information to IPFS. Since it is a hash-based storage system, the information

Algorithm 2 True/false event handling algorithm

$Vehicle(V_{ID}, I_{ID}, loc, D_t, PoL, speed, T_s)$→UAV
If ($V_{ID} \in U_{ID}$ && $speed > nomial\ speed$ && $loc = PoL$ && $T_s = valid$)
  Execute renown function
    function renown (VehicleAddress, VehicleBalance, VehicleRenown, CreditAmount)
      Get input: VehicleBalance, VehicleRenown
      VehicleBalance = VehicleBalance + CreditAmount
      VehicleRenown= VehicleRenown + 10
      emit VehicleAddress, VehicleBalance, VehicleRenown
    end function
else if ($loc \neq PoL$ && $T_s = invalid$)
  Execute disown function
    function disown (VehicleAddress, VehicleBalance, VehicleRenown, PenaltyAmount)
      Get input: VehicleBalance, VehicleRenown
      VehicleBalance = VehicleBalance – PenaltyAmount
      VehicleRenown= VehicleRenown - 10
      emit VehicleAddress, VehicleBalance, VehicleRenown
    end function
    discard the event message
end if

Fig. 4. Event handling algorithm

Fig. 5. Smart contract Set and Get functions

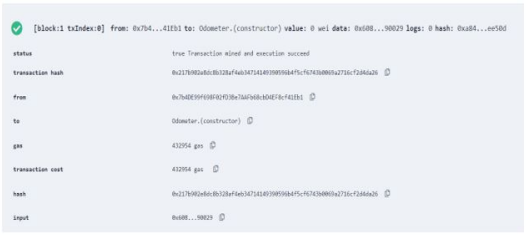

Fig. 6. The transaction and execution cost for the proposed smart contract

can be accessed by any vehicle in the environment using the hash value. All transactions are executed via smart contracts.

1) Involvement rate of vehicles: The vehicle's participation can be improved by providing incentives to their account and by its renown value. By doing this way, the selfish behavior is reduced and involvement rate is increased. The involvement rate (I_r) at time t is calculated by:(1).

$$I_r = \frac{N_t}{N_T} * 100 \tag{1}$$

Where N_t is the number of vehicle acts as true event reporter and N_T is the total number of vehicles located at the event place.

2) Security analysis: The proposed work aims in reducing following attacks and also satisfies the security requirements.

A. Replay attack: The replay attack is performed by the vehicle to inform a true incident again and again to improve its renown value. Since the proposed system uses IPFS as a data storage element, it stores all event information along with time which reduces the redundancy.

B. Anonymity conserving: Each vehicle gets its V_{ID}. Using this identity, the vehicles can initiate and verify events. The V_{ID} is changed on every request to avoid traceability. UAV maintains the connection between U_{ID} and V_{ID}. The intruder vehicle is unable to find the U_{ID}.

C. Smart contract security: The smart contract sometimes leads to reentrancy attack and it results in losing of cryptocurrencies. To avoid such bugs, the following security parameters are checked during compiling the smart contract in remix IDE.

VI. EXPERIMENT RESULTS

The exhibition of the proposed event validation scheme is assessed based on transaction cost and computation time. The proposed framework is executed in Python and the smart agreement is written in the Solidity language that is utilized for the execution of smart contract on the Ethereum blockchain. The smart contract is tried on Remix IDE, which is an online testing device. During testing, Ganache and Metamask are likewise utilized. The experiments are conducted on AMD Ryzen 3 3250U with Radeon Graphics 2.60 GHz, 4 GB RAM.

The vehicle registration is done by providing car number, account details, kilometre covered. The details are presented in Fig. 5. The status of the smart contract, its hash value with transaction and execution gas value are summarized and presented in Fig. 6. Two kinds of expenses are seen in the blockchain network. One is the transaction cost and another is the execution cost. The transaction cost is the aggregate sum of gas that is needed to send the information to the blockchain network; though, the execution cost is the measure of gas needed for the execution of any capacity [15]. The execution cost relies upon the tasks performed inside the capacity. The authors in [16] discuss the utilization of gas for various kinds of activities. It tends to be seen from Fig. 6 that the transaction cost is more prominent than the execution cost for conveying the smart contract in the Ethereum organization. The transaction cost is consistently higher because it incorporates the execution cost.

In Remix IDE, the deployment of smart contract is done by selecting Web3 provider. The ganache CLI provides 10 addresses with 100.00 ETH each. It is given in Fig. 7. Any one address is linked with Remix IDE then the deployment process is executed. The private key of any one account is copied and pasted in Metamask for further transactions. It is presented in Fig. 8 respectively. The deployment of smart contract with address extracted from Ganache. is presented in Fig. 9. After this process, transaction hash is created and it is given in Fig. 10. The hash value is same in both Figs. 6 and 10. After each transaction, it is aggregated into a block and it is validated by the process of mining and each block details are given in Fig. 11 respectively. This address is nothing but the vehicle's account number through which the penalty and credit amount are transacted after the smart contract execution.

Fig. 12 shows the computational time taken for generating certificate of location for each vehicle. This is done using

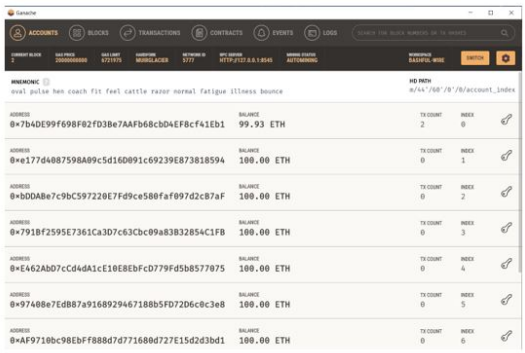

Fig. 7. Ganache CLI having address, ether balance and private key

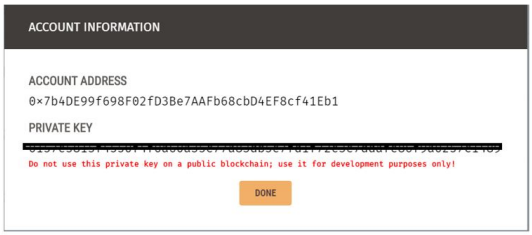

Fig. 8. Getting private key from Ganache CLI

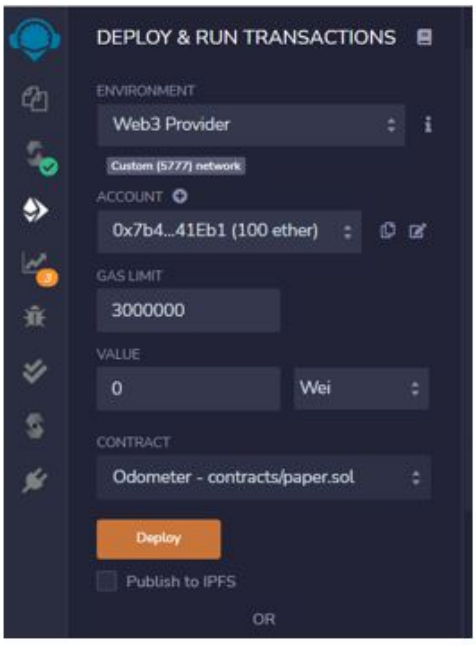

Fig. 9. Smart contract is executed with same address (0x7b4DE99f698F02fD3Be7AAFb68cbD4EF8cf41Eb1)

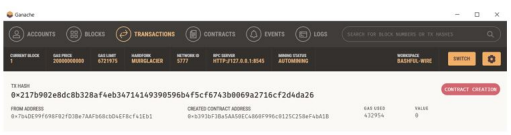

Fig. 10. Ethers spent from the account when deploying the contract

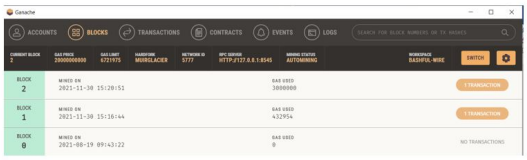

Fig. 11. Blocks in Ganache

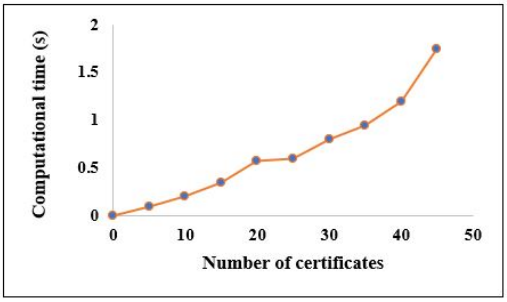

Fig. 12. Computational time for certificate generation

ECDSA-192. The result shows that an increase in computational time with an increase in the number of certificates.

Fig. 13 shows the involvement rate with respect to the number of vehicles. The proposed system involves an incentive mechanism for true event information, the vehicles are voluntarily sharing the event messages.

VII. Conclusion

In this work, a blockchain based secure transmission between UAV-vehicle is proposed for smart city environment. IPFS is used for off-chain data storage and access. The authenticity of the vehicle is done by getting location certificate and they were allowed to report events in the environment. All the credits and transactions are stored in blockchain, so that to avoid non-repudiation by the vehicles. In smart city environment, we need to have efficient monitoring of vehicles. This will highly help the drivers to follow the rules and regulations. Once they violate the rules, immediately the smart contract will execute and penalty is issued. The event detection and validation are also encouraged by providing credits to

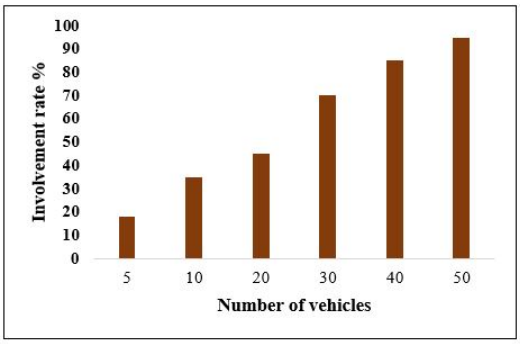

Fig. 13. Involvement rate vs Number of vehicles

their account. The proposed work is implemented on Ethereum platform and smart contracts are executed using Remix IDE.

ACKNOWLEDGMENT

The authors would like to thank the inventor of Ethereum blockchain.

REFERENCES

[1] Yu, Sungjin, et al. "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment." *IEEE Access* 8 (2020): 167875-167886. https://doi.org/10.1109/WPNC.2007.353643.

[2] Sharma, Sachin, and Seshadri Mohan. "Cloud-based secured VANET with advanced resource management and IoV applications." *Connected vehicles in the internet of things*. Springer, Cham, 2020. 309-325. https://doi.org/10.1007/978-3-030-36167-9$_1$1.

[3] Alladi, Tejasvi, et al. "Applications of blockchain in unmanned aerial vehicles: A review." *Vehicular Communications* 23 (2020): 100249. https://doi.org/10.1016/j.vehcom.2020.100249.

[4] Álvares, Paulo, Lion Silva, and Naercio Magaia. "Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives." *Telecom*. Vol. 2. No. 1. MDPI, 2021. https://doi.org/10.3390/telecom2010008.

[5] Wang, Xiaoliang, et al. "An improved authentication scheme for internet of vehicles based on blockchain technology." *IEEE access* 7 (2019): 45061-45072. https://doi.org/10.1109/ACCESS.2019.2909004.

[6] Aloqaily, Moayad, et al. "Design guidelines for blockchain-assisted 5G-UAV networks." *IEEE network* 35.1 (2021): 64-71. https://doi.org/10.1109/MNET.011.2000170.

[7] Fourati, Mohamed, Bilel Najeh, and Aicha Idriss. "Blockchain towards secure uav-based systems." Enabling Blockchain Technology for Secure Networking and Communications. *IGI Global*, 2021. 149-174. https://doi.org/10.4018/978-1-7998-5839-3.ch007.

[8] Wakode, Madhuri S., and Rajesh B. Ingle. "Blockchain-Based Solutions for Various Security Issues in UAV-Enabled IoT." *Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications* (2021): 143-158. https://doi.org/10.1002/9781119769170.ch8.

[9] Nguyen, Tri, Risto Katila, and Tuan Nguyen Gia. "A Novel Internet-of-Drones and Blockchain-based System Architecture for Search and Rescue." *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2021. https://doi.org/10.1109/MASS52906.2021.00044.

[10] Zeng, Fanhui, et al. "UAV-assisted data dissemination scheduling in VANETs." *2018 IEEE international conference on communications (ICC)*. IEEE, 2018. https://doi.org/10.1109/ICC.2018.8422219.

[11] Li, Hui, et al. "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET." *Peer-to-Peer Networking and Applications* 12.5 (2019): 1178-1193. https://doi.org/https://doi.org/10.1007/s12083-019-00786-4.

[12] Santos de Campos, Mário Gabriel, et al. "Towards a blockchain-based multi-uav surveillance system." *Frontiers in Robotics and AI* (2021): 90. https://doi.org/10.3389/frobt.2021.557692.

[13] Singh, Maninderpal, et al. "Blockchain-enabled secure communication for drone delivery: A case study in COVID-like scenarios." *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and beyond*. 2020. https://doi.org/10.1145/3414045.3415937.

[14] Lu, Zhaojun, et al. "A blockchain-based privacy-preserving authentication scheme for vanets." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 27.12 (2019): 2792-2801. https://doi.org/10.1109/TVLSI.2019.2929420.

[15] Naz, Muqaddas, et al. "A secure data sharing platform using blockchain and interplanetary file system." *Sustainability* 11.24 (2019): 7054. https://doi.org/10.3390/su11247054.

[16] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.