drones

MDPI

Article

Vehicle to Everything (V2X) and Edge Computing: A Secure Lifecycle for UAV-Assisted Vehicle Network and Offloading with Blockchain

Abdullah Ayub Khan [1,2], Asif Ali Laghari [3], Muhammad Shafiq [4,*], Shafique Ahmed Awan [2] and Zhaoquan Gu [5]

1 Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Pakistan
2 Department of Computing Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi 75660, Pakistan
3 School of Software Engineering, Shenyang Normal University, Shenyang 110034, China
4 Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China
5 School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China
* Correspondence: srsshafiq@gmail.com

Abstract: Due to globalization and advances in network technology, the Internet of Vehicles (IoV) with edge computing has gained increasingly more attention over the last few years. The technology provides a new paradigm to design interconnected distributed nodes in Unmanned Aerial Vehicle (UAV)-assisted vehicle networks for communications between vehicles in smart cities. The process hierarchy of the current UAV-assisted networks is also becoming more multifaceted as more vehicles are connected, requiring accessing and exchanging information, performing tasks, and updating information securely. This poses serious issues and limitations to centralized UAV-assisted vehicle networks, directly affecting computing-intensive tasks and data offloading. This paper bridges these gaps by providing a novel, transparent, and secure lifecycle for UAV-assisted distributed vehicle communication using blockchain hyperledger technology. A modular infrastructure for Vehicle-to-Everything (V2X) is designed and 'B-UV2X', a blockchain hyperledger fabric-enabled distributed permissioned network-based consortium structure, is proposed. The participating nodes of the vehicle are interconnected with others in the chain of smart cities and exchange different information such as movement, etc., preserving operational logs on the blockchain-enabled immutable ledger. This automates IoV transactions over the proposed UAV-assisted vehicle-enabled consortium network with doppler spread. Thus, for this purpose, there are four different chain codes that are designed and deployed for IoV registration, adding new transactions, updating the ledger, monitoring resource management, and customized multi-consensus of proof-of-work. For lightweight IoV authentication, B-UV2X uses a two-way verification method with the defined hyperledger fabric consensus mechanism. Transaction protection from acquisition to deliverance and storage uses the NuCypher threshold proxy re-encryption mechanism. Simulation results for the proposed B-UV2X show a reduction in network consumption by 12.17% compared to a centralized network system, an increase in security features of up to 9.76%, and a reduction of 7.93% in the computational load for computed log storage.

Keywords: Vehicle-to-Everything (V2X); edge computing; UAV-assisted vehicle network; blockchain; smart contract; cost-effective scheduling

Citation: Khan, A.A.; Laghari, A.A.; Shafiq, M.; Awan, S.A.; Gu, Z. Vehicle to Everything (V2X) and Edge Computing: A Secure Lifecycle for UAV-Assisted Vehicle Network and Offloading with Blockchain. *Drones* **2022**, *6*, 377. https://doi.org/10.3390/drones6120377

Academic Editors: Dawei Wang and Ruonan Zhang

Received: 1 November 2022
Accepted: 20 November 2022
Published: 25 November 2022

1. Introduction

The future development of the Internet of Vehicles (IoV) depends on Vehicle to Everything (V2X) applicational maturity [1,2]. However, applications include intent sharing, distributed environment design, bi-directional intercommunication, interactive gaming, and wireless network-based coordinated driving. These developments are anticipated

to make the system more efficient, reliable, secure, and diverse, allowing execution of vehicular transactions autonomously [3]. However, in recent advances, the success of these vehicular applications relies on a large amount of generated data, a fusion of data handling, and processing from wireless sensor-based distributed networks that are associated with the vehicles. Therefore, deployed on-road infrastructure guarantees data management in real time while precisely perceiving the environment. Perception and related computation for each vehicle increases the continuity of learning in the smart environment. In fact, it leads to low resource consumption in terms of computing energy, network bandwidth, and storage, due to the high price of precision sensors and the powerful computational processing units (CPUs) used [4]. The usage of low-priced equipment in the IoV domain impacts the performance ratio of systems. Furthermore, it limits local perception capabilities, which directly affects centralized network-based V2X applications. Resource usage, especially energy consumption for computation and high-precision sensor management, substantially reduces the efficiency of vehicular systems in terms of battery life, reducing mileage. In order to improve the use of computational resources, different applications of the IoV have adopted different artificial intelligence (AI)-based methods for dynamic monitoring. This has led to various significant challenges that pose resource-management-related problems in IoV terminals [5].

Beyond these limitations, each IoV node is able to directly interconnect with other nodes in the chain of smart cities, as shown in Figure 1. This is possible because the centralized network-enabled infrastructure provides intercommunication facilities with no repudiation [6]. However, the technology is more robust with vehicular edge computing, fifth-generation networks (5G), and fog/cloud-based system integration. These developments aim to provide a vigorous computational environment, high storage, sensor connectivity, smart sharing and exchanging, and service orientation by leveraging distributed IoV energy usage with low-cost distributed communication [7]. This differs from cloud/fog-enabled technologies, which use an old paradigm where physical proximity between information systems and computing services promised distinct advantages. These advantages include low throughput and latency, high power efficiency, security and privacy protection reliability, reduced network bandwidth usage, and storage-related context awareness. On the other hand, vehicular edge computing integration depends on distributed wireless networks to divide a large number of computing tasks and sensor-based corresponding records/details over the IoV and the edge network. This leads to a quick response by enabling smart vehicles to perform all applications for a distributed IoV network.

The current standard of V2X (UAV-assisted network) is categorized into two different parts: short-range dedicated communication and a cellular V2X. Dedicated short-range communication is used as a standard protocol of IEEE 802.11p, while cellular communication follows 5G protocols [8,9], as shown in Figure 1. The combination of short-range and cellular V2X on the existing system is used to gain broader coverage for pilot-distributed applicational facilities with distance transmission, steadier channels, and UAV network-related deployment. The recent of UAV-assisted infrastructure system uses 5G cellular V2X to offload a large amount of data to IoV edge nodes with new frequencies, such as millimeter-wave frequency bands.

However, the offloading problem in a UAV-assisted network creates different challenges in the V2X environment. These include problem segmentation, IoV edge selection and offloading, problem mitigation, and privacy protection, which are becoming widely researched concerns [10]. For instance, edge computing offloading strongly depends on a large-scale ubiquitous base station to handle data and coverage for transmission. It assumes that the current communication resources of the UAV-assisted network are not sufficient for vehicular edge offloading [11]. Therefore, deploying a dense-base station reduces the load of vehicular edge computing-enabled traffic by providing a simple structure to manage all the transactions. However, it is considered a cost-inefficient method for IoV services and locations. To manage these complexities, a middle base station/middle infrastructure with the

standard process hierarchy is required to evaluate the requests of IoV devices concurrently. Only a valid service request can pass; otherwise, it is discarded at an initial level.

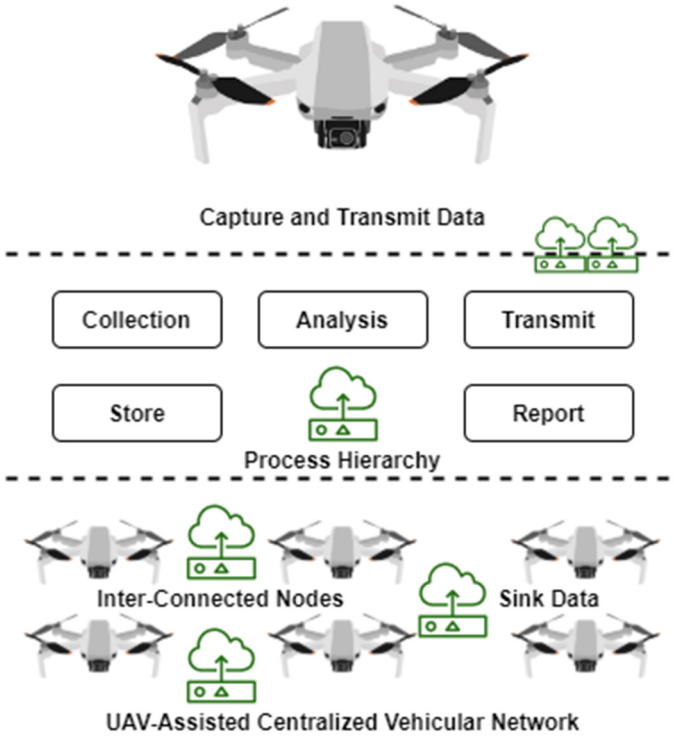

Figure 1. The current Vehicle to Everything (V2X) environment.

Major actors are analyzing distributed UAV-assisted vehicular network solutions related to connectivity and offloading for futuristic transportation. One of the main reasons for adopting blockchain hyperledger-enabled distributed architecture in a UAV-assisted vehicular network is to eliminate the dependency on certificate authority [12–16]. The decentralized nature of blockchain ledger technology integrates with different domains of computing to allow new designs in IoV transaction processing, privacy, and security. The modular infrastructure of blockchain technology provides automated transaction execution facilities via distributed applications (DApp). Thus, it ensures information security against malicious attacks during inter/outer-communication between nodes. However, the current system of UAV-assisted vehicle network consumes significant computing resources because no standard protocol for request management has been proposed [17]. For this reason, hyperledger technology is used to provide a customized design for consensus, chaincode execution, privacy and security procedures, and network communication-related facilities, directly reducing resource consumption. In addition, another advantage of this technology is that it provides ledger (log records) preservation and protection in a serverless environment through the proxy threshold re-encryption mechanism.

1.1. Objectives and Contributions

This paper addresses the current issues, challenges, and limitations involved in centralized UAV-assisted vehicle networks. It highlights the changes in the evolution of Vehicle to Everything (V2X) and presents the role of V2X in futuristic transportation development. A number of enhancements/improvements when deploying a UAV-assisted vehicular network with blockchain, including in record scheduling, managing, organizing, optimizing, and offloading in a secure and protected manner in a decentralized environment. By enabling the current design of UAV-assisted V2X to be integrated with a consortium channel's blockchain structure, the load on vehicular network resources is reduced drastically compared to previous infrastructures. The major contributions of this research paper are as follows:

- This paper proposes B-UV2X, a novel and secure distributed UAV-assisted vehicular network infrastructure for IoV interconnectivity. The designed system realizes interoperable communication between devices in the V2X environment with blockchain;
- A blockchain-enabled standardized lifecycle is designed. The main objective is to maintain the process hierarchy throughout transactions acquisition towards deliverance in a secure manner;
- A consortium network with doppler spread is deployed for edge-enabled IoV systems to handle requests related to permissioned or permissionless environments;
- To protect individual transactions of the IoV, B-UV2X uses a proxy re-encryption threshold mechanism. Furthermore, a multi-consensus protocol is created with the predefined method of the digital signature of the hyperledger to schedule the list of node transaction executions, which helps in the management of resources;
- In this paper, three different types (IoV connectivity and data management, record updates, and exchanging) of smart contracts are created and deployed;
- Finally, this paper highlights the implementation challenges faced in the process of B-UV2X deployment, with future open research questions. Possible solutions are discussed.

1.2. Section Distribution

The remainder of this paper is structured and organized as follows. In Section 2, various related works are studied and investigated to find the current gaps in vehicle-to-everything, UAV-assisted vehicle networks, the IoV, and seamless edge computing services for centralized networks. The problem description, formulations, and related working objectives of the proposed B-UV2X are discussed in Section 3. The experimental results of B-UV2X and related comparisons with other state-of-the-art methods are presented in Section 4. In Section 5, the paper describes different implementation challenges, issues, and limitations, and highlights futuristic objectives as well. Finally, the conclusion of this research is discussed in Section 6.

2. Related Work

2.1. Vehicle-to-Everything (V2X) and UAV-Assisted Vehicle Network

Recently, drone-enabled technology has been widely adopted in different industrial, manufacturing, and production units to smartly enhance working objectives in terms of scheduling, managing, and monitoring. The open nature of centralized vehicular networks threatens privacy of information [18]. This may also lead to privacy leakage of personal information, posing various tampering- and forgery-related issues. In this regard, several artificial intelligence, machine learning, deep learning, federated learning, and blockchain-enabled distributed modular architectures of UAV-assisted vehicular networks with doppler spread have been presented [19]. These address different kinds of dependent centralized aggregative servers, which are designed to maintain system objectives and a crash-less environment. In addition, unauthorized participation also drives positioning attack, reducing the usability of the system and creating communication barriers that hinder integration in the large number of cross-domain IoVs. The research gaps in previously published state-of-the-art methods are discussed as follows (as shown in Table 1).

Table 1. Related literature on blockchain, UAV-assisted vehicular networks, and vehicle to everything.

Title of the Article	Proposed Method/Procedure	Research Gaps in the Study	Similarities and Differences with the Proposed B-UV2X
Internet of Drones (IoD) applications with blockchain [20]	The authors of this paper discussed the role of blockchain and its integration in the improvement of IoD connectivity and security, as well as the importance of distributed applications for drone-based data management and monitoring in a protected manner, especially in smart-city environments.	• Scope of data privacy security issues • Explored commercial applicational problems • Derived blockchain mechanism proposed • Data optimization and offloading issues	• Internet-of-Vehicles (IoV) connectivity • Blockchain permissionless network • Platform interoperability limitation • Security and privacy concerns
A decentralized machine learning framework for intrusion detection in UAV using blockchain distributed ledger modular infrastructure [21]	This paper presents a distributed framework for intrusion detection using integrated machine learning and blockchain technologies. In this design, the system is potentially able to significantly enhance the integrity, transparency, and storage of information for smart decision-making among multiple UAVs.	• Conventional UAVs • Complex machine learning algorithm used • Predictive analysis • Multi-UAV intercommunication	• Cross chain platform-based challenges • Intercommunication node integrity • Permissionless network structure
Drone-based delivery scheme for industrial healthcare using blockchain technology [22]	This paper highlights the list of current blockchain-based drone-enabled industrial healthcare applicational challenges and limitations. These include harsh environmental conditions, rough terrain, war-prone areas, congested traffic, remote location, etc.	• Integrated IoD delivery scheme • Data driven analytics • Two-way verification and validation process • Cross-chaining platform	• Blockchain distributed ledger technology • Permissioned architecture • Hash-encryption • Cloud-enabled storage
Internet of Drones (IoD): communication leveraging with blockchain [23]	The authors of this paper presented a security approach for drone-to-everything communication, in which the locations of drones are traced by segment divisions of the areas in which they are deployed.	• Fifth generation network (5G) connectivity • Deployed across remote sides • Remote cloud for storage	• Cryptographic hash-encryption mechanism used • Advanced sensors and GPS used • Segment division by areas
Internet of Vehicles (IoV) security [24]	In this paper, the authors defined the taxonomy of IoD security and privacy along with access to the controlled airspace to provide an inter-location navigation service using AI, machine learning, blockchain, and federated learning.	• Federated learning architecture used • Proposed IoD paradigm (standardized) • Level-of-security category	• Blockchain integrates with AI • Permissionless architecture • On-chain and off-chain intercommunication channels designed • Distributed interconnected node hierarchy
A lightweight assisted secure routing scheme for the IoV using blockchain Ethereum [25]	A secure routing algorithm for IoT-enabled drone management swarm UAS networking is proposed in this research. The benefits are as follows: • Swarm UAS orientation; • Customized consensus using blockchain; • Estimate traffic status/dynamic monitoring; • Lookup table and scheduling.	• Customized protocols and policies • Improved predefined consensus • Blockchain permissionless network • Distributed ledger preservation and digital signature	• Monitoring resource usage • Reduce network bandwidth consumption • Data security and preservation • Interoperability issues between inner and outer chain connectivity

2.2. Internet of Vehicles and Mobile Edge Computing with Blockchain

By virtue of intelligence in UAV-assisted vehicular networks, the IoV performs a primary role for transport systems in dynamic-time information exchange, which improves data processing and traffic management, especially in smart cities. In addition, to ease the computational energy and preservation load, which is increased by a large number of IoV nodes requesting to connect, edge-enabled computing resources are introduced to reduce the load of computing tasks, offload data and management, and optimize the local vehicular network with low latency [26–30]. Data integrity and privacy are still challenging prospects in these proposed systems. To address these problems, various researchers apply different methods in their proposed architectures, along with conditional privacy-preservation authentication protocols to enable the IoV with edge computing using blockchain distributed ledger technology.

The use of mobile edge computing provides enormous storage resources with a powerful computing network infrastructure. The IoV with mobile edge computing ensures that the paradigm can handle a large amount of data storage, sharing and exchanging, and processing capabilities close to the devices. However, the system is unable to share data when the architectural approach is based on a centralized server. With these potential risks of data leakage, an IoV node faces difficulty when evaluating the credibility of a message; this is also because it receives requests for transactions from an untrusted centralized environment [2–30]. To enhance security, blockchain hyperledger technology with a consortium network structure with doppler spread is proposed.

3. Preliminary Knowledge of the Proposed B-UV2X

This section discusses the fundamentals and critical assumptions of blockchain-enabled distributed technologies in UAV-assisted vehicular networks to create a new paradigm in the IoV. Related problem formulations are discussed as follows:

3.1. Notation, Problem Formulation, and Description

First, to design a UAV-assisted distributed vehicular network lifecycle, the state of the data item is requested by the IoV nodes in a transactional manner; then, the IoV builds encoded data point broadcasts based on the high clique (priority) of the transactional request. Second, these transactional requests must be secure and protected while being transmitted. To ensure this, we present a standardized process hierarchy: (i) data generation (transaction request sent from the IoV devices/nodes), (ii) capturing, (iii) examining, (iv) analyzing, (v) preserving, (vi) sharing/exchanging, and (vii) reporting (details of log recordings), as shown in Figure 2. Finally, the IoV receives encoded data points via the process hierarchy of the proposed B-UV2X lifecycle. In the decoding procedure, the broadcasted logs of UAV-assisted vehicular data points are accepted by the IoV itself. In the design and development, the main objective is to reduce resource usage in terms of IoV-enabled computational energy, network bandwidth consumption, and memory, which directly affect battery life. For the sake of standardization and simplification, we use IoV_1, IoV_2, IoV_3, ..., IoV_n to denote Internet of Vehicles (IoV) devices; the position coordinates of IoVs in smart cities are as follows: (a_x, b_x) of IoV_n. d_1, d_2, d_3, . . . , d_n represent the transactional requests and related data broadcasted over the UAV-assisted vehicular network. 'r' represents the radius of interconnected IoV nodes for communication (or sharing information) in the designed distributed vehicular network.

In order to check that the IoV nodes in the proposed B-UV2X-enabled distributed vehicular network are receiving or sending data points/transactional requests at the same time, the interoperable platform provides a distanced measurement structure that calculates the distance between devices before transmitting requests. The distance between IoV devices is represents as '2r', 'r', and 'r_0', showing the coverage radius of two nodes in the UAV-assisted distributed network. The maximum radius of the distributed IoV network is equal to the distance between locations, which must be less than or equal to the coverage area ('r').

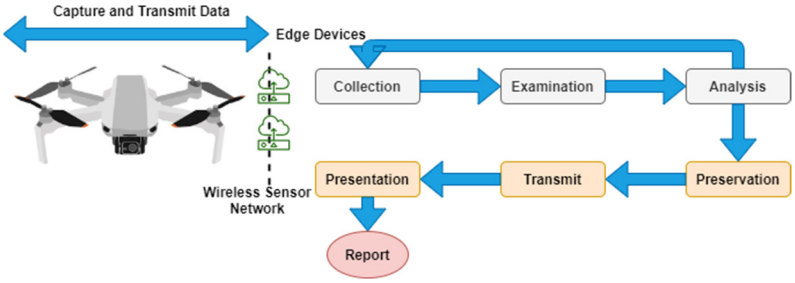

Figure 2. Block diagram of the proposed lifecycle of B-UV2X.

With the goal of reducing network bandwidth usage in the distributed environment, we tune the maximum radius of multiple IoVs (maximum in the four interconnected pairs of shared information/transactional requests). Given the maximum area ('r') of the distributed network circle, we can obtain the coverage area of a circle of the inscribed graphical domain (such as an equilateral triangle). The length of the sides of the equilateral triangle (which means the area of IoVs/drones) is $\sqrt{}$four-sides ($\sqrt{}$4s).

If the size of the IoVs is = $\sqrt{}$4s or >= $\sqrt{}$4s, the maximum distance between IoVs is 'r', which is directly proportional to $\sqrt{}$4s. The exterior radius of the designed UAV-assisted distributed vehicular network is 2r. In another case, the exterior is >= 2r.

The vehicle IoV_n sends or receives transactional requests for data points d_n; then, the UAV-assisted distributed vehicular network schedules transactions t_n. In this way, the system can identify from which IoV devices the requested and scheduled transactions originate, as well as where they are shared. In addition, the integration of edge-enabled computation with the proposed B-UV2X lifecycle reduces the load of data offloading. With request/transaction scheduling, the computational processing of the IoVs is reduced by increasing the rate of execution and transmission. In this manner, the cost of information preservation is also reduced.

However, duplicate and redundant scheduled transactions can be discarded before execution. This is because the system verifies and validates request automatically by the use of deployed chain codes (and functions such as IoVReg(), UAVAVLC(), AddNTD(), update() and InfoPre()). The role of a hyperledger expert, the person responsible for initiating the proposed B-UV2X chain and handling the request for participating IoV registrations, is also highlighted in this scenario.

3.2. Proposed Architecture

The operation of the proposed B-UV2X is divided into four phases. First, B-UV2X registers the IoV node in the designed consortium chain after proper verification and validation while obtaining the enrollment request from the nodes and related device stakeholders. For a complete analysis of the registered request, the role of a blockchain hyperledger expert is crucial; this person is responsible for initiating chain transactions, handling a number of requests and related executions, and managing information preservation (records logs), as shown in Figure 3. The data movement hierarchy of this phase is bi-directional in nature. Second, in the distributed vehicular environment, the IoV-enabled captured data is received via a wireless sensor network (which is placed between the first and second phases); the captured data points are processed through the proposed B-UV2X standardized lifecycle, as shown in Figure 3. Initially, data points are collected and data are preprocessed and filtered for different types of noises, such as duplication, shallow data, etc. After that, the system examines and analyzes the data (schedules to execute); if the data have necessary details that require further investigation, then the system preserves the data, transmits them towards execution, and presents a report (category of information of further investigation).

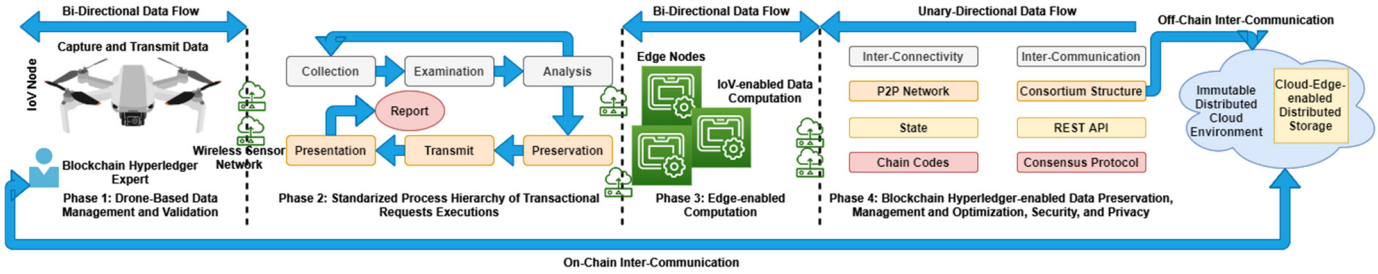

Figure 3. Proposed B-UV2X.

In the third phase, the computational node is placed between the lifecycle and blockchain hyperledger-enabled distributed ledger technology. There, it receives scheduled transactions/data points for execution. Therefore, the performance of B-UV2X is robust while reducing usage of computational energy. This is because edge nodes consume fewer computing resources compared to the fog, cloud, and other customized computational units. The data movement hierarchy of this phase is bidirectional. The fourth phase includes security and privacy operations of the proposed B-UV2X, as shown in Figures 3 and 4. A blockchain hyperledger-enabled consortium modular infrastructure is proposed; the main purpose of this design is to protect data from malicious attackers, provide data integrity, transparency, provenance. organization, and management, and to prevent forgery of and tampering with data, thereby maintaining privacy and security.

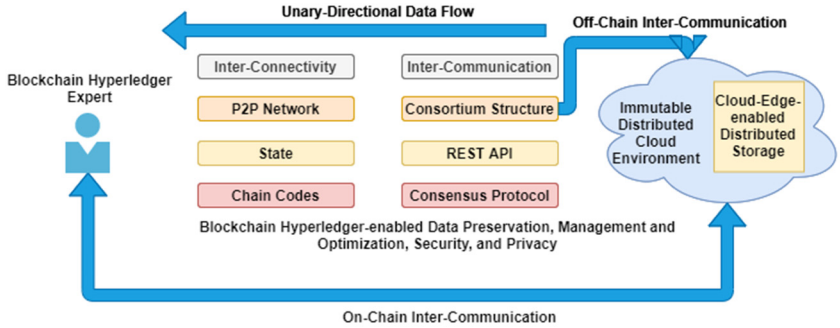

Figure 4. Working operation of the proposed B-UV2X security and privacy hierarchy.

In order to maintain privacy and security, we design two channels of inter-communication between inter-connected nodes of the IoV over the distributed UAV-assisted vehicular network, as shown in Figure 4. In this process, a transaction processor is placed, the main objective of which is to handle requests for transactions in the deployed B-UV2X consortium Peer-to-Peer network (P2P). For instance, to reset the stack of transactional requests and schedule transactions and exchanges, we use the REST API and state facilities of hyperledger technology. Multi-proof-of-stack (MPoS), along with chain code (with different functions ()), is designed, created, and deployed to automate verification, validation, transaction execution, and preservation. For storage of IoV-based logs (transactional requests), cloud-edge-enabled distributed immutable storage is utilized, which is considered one of the most customizable and cost-efficient distributed information preservation methods in the domain of blockchain-enabled ledger technology.

3.3. Smart Contracts Implementation

In this section, we discuss the procedure to automate transactional requests of IoVs and process each request through the designed lifecycle of a UAV-assisted vehicular network, responding to these transactions via DApp and records (in the cloud–edge-enabled immutable storage, as mentioned in Table 2 (InfoPre())). For execution (request verification and validation) automation, we designed, created, and deployed chain code with five different functions, multi-consensus protocols, and digital signature, as shown in Table 2.

The main objectives of these codes/functions are to provide operations automation in terms of IoV registration (IoVReg()), monitoring stakeholder registration in accordance with the designed lifecycle (UAVAVLC()), schedule the number of transactions, perform related requests executions (AddNTD()), conduct record management (UpdTr()), and preserve (InfoPre()) and exchange information.

Table 2. Chain codes, consensus, and digital signature implementation.

Input Variables: The engineer of the blockchain hyperledger is the person to initiate chain/transactional requests. Manages events of node (IoV) transactions executions and preservation. Stakeholder registration (verification and validation). Exchange information between the participating nodes. Updates logs/records and sharing.
Assumptions and Declaration: int main().File[x].X: IoV node/device registration, IoVReg(); Stakeholder registration (smart cities), StkReg(); UAV-assisted vehicular lifecycle, UAVAVLC(); Add new transaction/request details, AddNTD(); Resource management and monitoring, ResMM(); Consortium channels, Ccha(); Update transactions, UpdTr(); Exchange information, ExInfo(); Data/information preservation, InfoPre(); Blockchain fabric timestamp [run]; Blockchain hyperledger expert schedule list of requests and executions, Counter + 1; Count(request/executed);
Executions: **if** IoV is not in IoVReg(), **then,** AddNTD() and exchange; **if** transactions initiated/requested passes through UAVAALC(), **then,** AddNTD(), ResMM(), Ccha(), and ExInfo(); Multi-Proof-of-Stack (MPoS()), Digital signature (after receiving 51% consensus votes), Consensus(); Counter + 1, updTr(), and InfoPre(); **else** check error, change state, share, exchange, and preserve, terminate; **else** check error, change state, share, exchange, and preserve, terminate;
Outputs: IoVReg(); UAVAVLC(); AddNTD(); UpdTr(); and InfoPre();

4. Simulations, Results, and Discussion

This section discusses the simulation of the proposed B-UV2X. The results are based on a blockchain hyperledger-enabled consortium modular infrastructure designed for connected nodes of IoVs for a UAV-assisted distributed vehicular network. The proposed B-UV2X was tested on a Core i7 VPro CPU (2.8 base clock speed—3.4 Turbo Boost) with

16 GB RAM, 8 GB shared Iris Xe Graphics, and 1 TB storage/internal SSD. The network connectivity between IoVs and the proposed architecture was 24 MB/s with dedicated channels of distribution. With some assumptions (discussed as follows), the docker of the blockchain hyperledger included:

- Heterogeneous node connectivity;
- 4MB size of transactional nodes;
- Single network bandwidth used
- Cloud-edge enabled customized distributed storage deployed;
- Blockchain hyperledger expert initiates a chain of the transactional requests of IoVs, as shown in Figure 5 (the test code of smart contract/chain codes with MPoS consensus is presented, along with the parameters of simulations executions).

```
package abac

import (
    "encoding/base64"
    "encoding/json"
    "fmt"

    "github.com/hyperledger/fabric-contract-api-go/contractapi"
)

// SmartContract provides functions for managing an Asset
type SmartContract struct {
    contractapi.Contract
}

// Asset describes basic details of what makes up a simple asset
type Asset struct {
    ID             string `json:"ID"`
    Color          string `json:"color"`
    Size           int    `json:"size"`
    Owner          string `json:"owner"`
    AppraisedValue int    `json:"appraisedValue"`
}
```

Figure 5. Chain code with MPoS. Test code for simulation of the proposed B-UV2X.

In Figure 6(1–3), the simulation results of the proposed B-UV2X show that it decreases the cost of computing resources by 7.93%, which allows edge-enabled computation (as shown in Figure 3). After evaluation of the computation of B-UAV2X, it is considered to be a good candidates for real-time industrial implementation and scheduling. The operation of this simulation shows that the process initiates when the request management of the proposed lifecycle executes (as shown in Figure 6(3)), the matrices of which are the number of data requests received and the data examined for further executions.

However, the IoV-enabled self-data-capturing capability was enhanced after the tuning of lifecycle hierarchy, as shown in Figure 4(1–3) and Figure 6(1–3), which is most importantly used for the sake of heuristic reconciliation in smart cities. This capability is also needed because the process hierarchy sends a request to preserve captured records for heuristic investigation. To do this, we manipulate the design of the lifecycle to examine and analyze the collected details in terms of binary color transformation, entropy, extracted critical features, and preserve optimized records, as shown in Figures 7 and 8 (also discussed in the proposed architecture section and highlighted in Figure 3).

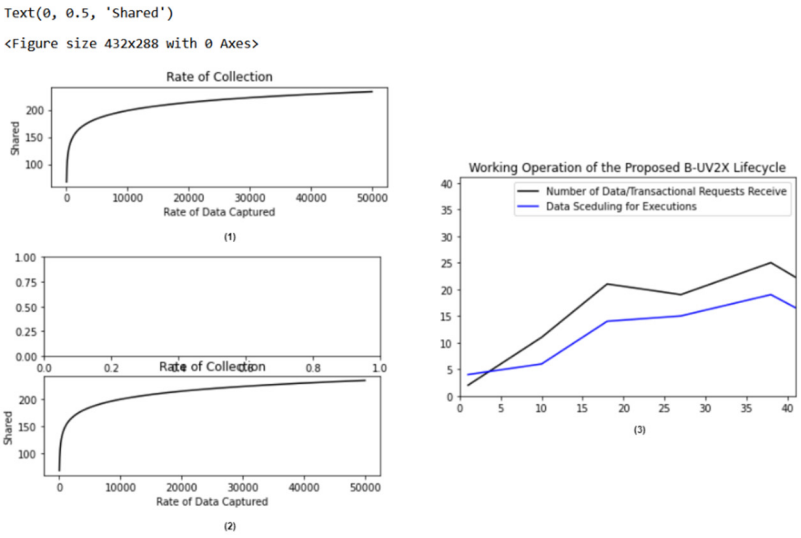

Figure 6. The working operation of the proposed B-UV2X lifecycle: (**1**) shows the rate of data captured by the IoVs, (**2**) shows the rate of data collected, and (**3**) shows that the fluctuation between the data received and the data scheduled for execution.

Figure 7. IoV-enabled data capture: (**1**) shows the original image, (**2**) shows the transformation in the binary color format, (**3**) shows the extracted features for heuristic purposes, and (**4**) shows the optimized record preservation.

Figure 8. IoV-enabled data capture: (**1**) shows the original image, (**2**) shows the transformation in the binary color format, (**3**) shows the extracted features for heuristic purposes, and (**4**) shows the optimized record preservation.

In the entire process of B-UV2X simulations, the blockchain hyperledger expert and registered participating stakeholders can observe the resources utilized in the complete process execution. The consumption of network bandwidth is reduced by 12.17% throughout the execution of each transaction, and security capability is increased by up to 9.76% by protecting individual ledger transactions of UAV-assisted vehicles using the NuCypher threshold proxy re-encryption mechanism (as shown in Figure 9).

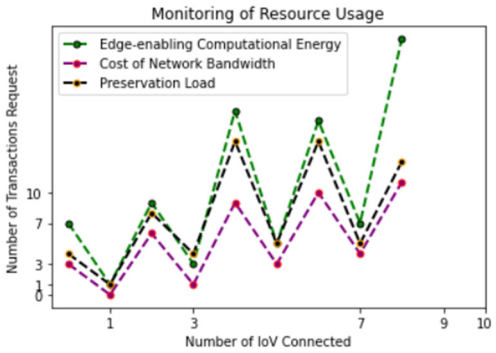

Figure 9. Monitoring of resource usage: shows the consumption fluctuation in number of IoVs connected and number of requested transactions.

Observe that the deployment of the chaincodes and related functions (such as IoVReg(), UAVAVLC(), AddNTD(), UpdTr(), and InfoPre()) with MPoS customized consensus policy and edge computing technology decreases the cost of IoV-enabled data scheduling, organization, management, optimization, and preservation. Figure 10 illustrates the fluctuations between the predefined hyperledger consensus and the proposed B-UV2X over the UAV-assisted consortium distributed vehicular network in terms of the number of transactional requests and the number of connected IoVs' for data verification and validation.

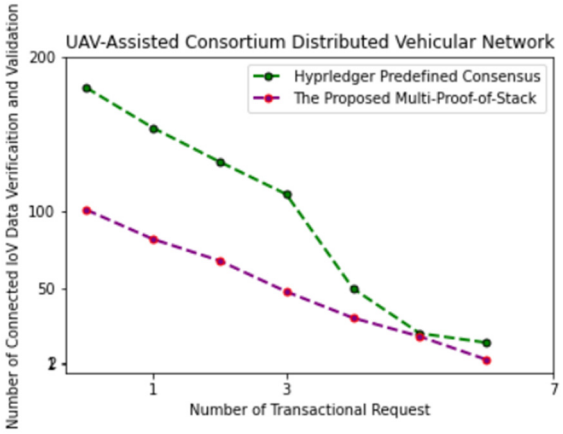

Figure 10. UAV-assisted consortium distributed vehicular network shows the fluctuation between the predefined hyperledger consensus and the proposed B-UV2X.

The evaluation matrices of the proposed B-UV2X are compared with newly published methods (previous state-of-the-art methods) such as "edge intelligence for IoV" [31] and "blockchain-based conditional privacy preservation" [32]. The metrics for this analytical procedure are based on the usage of resources, preservation, protection efficiency (proxy threshold re-encryption level), reliability, privacy, and security. In Table 3, a few more analytical comparisons are discussed, indicating the superiority of the proposed work compared to other state-of-the-art methods. A comparative parameter of the evaluation is presented (as mentioned in Table 3, attribute 3), which helps to measure the fluctuation/improvement of the proposed B-UAV2X compared to other methods.

Table 3. Comparison table: state-of-the-art methods.

Methodology of Other State-of-the-Art Methods	Main Contributions	Analytical Matrices of Other State-of-the-Art Methods	Proposed B-UV2X
A resource trading, computational offloading, and management approach for enhanced drone-to-drone assisted environment using blockchain distributed ledger [33]	• Decentralized resource sharing system • One ledger multi follower strategy • KKT-based algorithm	• Blockchain: yes • Hyperledger: no • Network type: permissionless • Encryption mechanism: hash-encryption • Block size: variable • Intercommunication channels: two • Consensus: predefined • Digital signature: predefined • Efficiency: not applicable • Accuracy: not applicable	The analytical matrices of the proposed B-UV2X are as follows: • Blockchain: yes; • Hyperledger: yes; • Network type: consortium; • Encryption mechanism: NuCypher proxy threshold re-encryption; • Block size: 4 MB–6 MB; • Intercommunication channels: on and off-chain; • Consensus: multi-proof-of-stack (MPoS); • Digital signature: customized (51% vote based); • Efficiency: 12.17%, 7.93%; • Accuracy: not applicable.
Edge-enabled mobile server deployment scheme for IoVs with blockchain [34]	• Edge server deployment • Roadside node management • Distributed application uses for resource monitoring	• Blockchain: yes • Hyperledger: no • Network type: permissionless • Encryption mechanism: defined hash encryption • Block size: variable • Intercommunication channels: not defined • Consensus: predefined • Digital signature: [redefined • Efficiency: not applicable • Accuracy: not applicable	

Table 3. *Cont.*

Methodology of Other State-of-the-Art Methods	Main Contributions	Analytical Matrices of Other State-of-the-Art Methods	Proposed B-UV2X
A multi-access edge computing for vehicular network using a deep neural approach [35]	• Multiple multi-access edge is designed • VANET ecosystem deployment • Distributed permissionless structure is proposed for IoV interconnectivity	• Blockchain: yes • Hyperledger: no • Network type: permissioned • Encryption mechanism: hash encryption SHA-256 • Block size: variable • Intercommunication channels: not applicable • Consensus: predefined • Digital signature: predefined • Efficiency: not defined • Accuracy: not defined	
A resource efficient framework for IoVs using blockchain, AI, and edge computing [36]	• Proof-of-lottery consensus mechanism is proposed • ETCZ: the edge terminal consensus zone • Resource efficient distributed modular framework is presented	• Blockchain: yes • Hyperledger: no • Network type: permissioned • Encryption mechanism: hash SHA-256 • Block size: variable • Intercommunication channels: two • Consensus: predefined • Digital signature: predefined • Efficiency: not applicable • Accuracy: not applicable	

5. Current Status of Edge Computing and Related Implementation Issues

The use of edge-enabled computing integrated with UAV-assisted vehicular network technology to design a secure intercommunication channel for IoV interconnectivity and related advantages are discussed. With blockchain distributed technologies, edge networks provide a cost-efficient manner to share and exchange information in a distributed environment. However, there are various implementation challenges that impact resource usage, such as computing power, storage, and network bandwidth.

5.1. Edge Computing Integrated with Outsourced Computation

The edge computing-enabled Internet of Things (IoT) plays a significant role in outsourcing computation and related management, such as providing participating node proximity [37]. In the UAV-assisted vehicular network environment, nodes receive a reward for computational task executions. For instance, the technology uses with a blockchain hyperledger to verify the integrity of arbitrary deterministic functions and restricts illegal authentications of false negative contractors that try to maximize their activities in the distributed environment [38,39]. The verification mechanisms of blockchain-enabled technology with IoV creates a challenging problem when the pre-trained models are designed for validation purpose. However, all the nodes consume less than 1 milli-second (ms) computational overhead with minimum network bandwidth (almost 80 bytes/frame). This may lead to another limitation regarding resource management and parallel usage.

5.2. Vehicle to Everything-Enabled Distributed Node Interconnectivity

In the V2X environment, one of the biggest issues to design and develop an efficient and secure distributed node architecture. For instance, when applying a blockchain distributed consortium mechanism over a Peer-to-Peer (P2P) network, there are different node scaling challenges that arise, while the lack of cost-efficiency requirements is also considerable [37,38]. However, with the introduction of a hyperledger-enabled modular framework, we can meet various integrity, transparency, provenance, and trustworthiness requirements [39]. By constantly stimulating the ledger, every request for IoV transactions is incorporated, with the details of information acquisition towards deliverance and exchange. However, the participating stakeholders can see the movement of individual IoVs

through the dynamic monitoring capability/traceability using the blockchain hyperledger, regardless of the particular stakeholder that initiates activities.

5.3. Role of Blockchain Hyperledger Technology in Edge Computing Environment

Edge-enabled technology brings computational resources close to end devices (IoT-enabled devices), allowing edge computing, preservation, operation and control, and analysis of related data [38,39]. Blockchain distributed ledger technology has the potential to provide a platform to solve privacy-, protection-, and security-related problems associated with edge computing, including access control, authentication, verification, and validation. In a blockchain-enabled edge network, the system provides UAV-assisted vehicular intercommunication channel facilities, from which on-chain and off-chain channels are derived. These interconnected node channels are designed to handle the list of implicitly and explicitly transactional requests more efficiently and reliably.

5.4. Drone-Based Data Management and Monitoring

In the domain of data management and monitoring, there are major limitations to providing data integrity and transparency, most importantly in the distributed ledger environment [37,38]. At present, most hyperledger technology cannot provide a customized data integrity policy and consensus management, only allowing moderate predefined validator processors for distributed verification of consensus, such as PoET, PoW, PoS, etc. [39]. However, a robust structure of privacy protection has been proposed by the Linux community to allow construction of an infrastructure to preserve information and chain-of-records with data traceability. This modular improvement of the hyperledger effectively tracks information management at every step of the transactional request schedule. In addition, it enhances the dynamic monitoring facilities by providing a better transaction/drone registration (IoV registry) hierarchy, with more efficient control compared to previously state-of-the-art methods [38,39].

6. Conclusions

This paper addresses current problems involving centralized UAV-assisted vehicular networks such as scheduling, offloading, management, optimization, privacy, and security. The key objective of this paper is to address gaps in the design, development, and deployment of distributed vehicular networks for the IoV in smart cities using the blockchain hyperledger. The existing protocol/process hierarchy of IoV-enabled request execution via distributed applications (DApp) is also highlighted. This paper proposes B-UV2X, a secure and novel lifecycle of UAV-assisted vehicular data processing for the IoV, using blockchain consortium architecture. It includes a customized consensus mechanism for multi-proof-of-stack (MPoS), where data offloading can be managed, directly impacting the management of resources as well. Transactional executions of the proposed B-UV2X are fully protected by the NuCypher threshold proxy re-encryption algorithm. The individual ledger/records of the node's transactions are preserved in immutable storage, such as edge network-enabled cloud storage. The participating stakeholders of the proposed B-UV2X receive details of ledger traceability for the sake of dynamic monitoring of resource management and related IoV node activities in smart city environments. The simulation results of B-UV2X show that it reduces network consumption by 17%, reduces the computing load with preservation by 7.93%, and increases security by 9.76% compared to other state-of-the-art methods.

Author Contributions: A.A.K. wrote the original draft and was responsible for organization, preparation, and analysis. A.A.K., A.A.L., S.A.A., M.S. and Z.G. reviewed and rewrote the draft, performed part of the literature survey, investigated and designed the architecture/framework, were responsible for lifecycle design, code, and presentation, and explored software tools. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (grant nos. 62250410365, 61902082), and the Guangzhou Science and Technology Planning Project (no. 202102010507).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors of this paper declare that there are no conflict of interest.

References

1. Lv, Z.; Qiao, L.; Hossain, M.S.; Choi, B.J. Analysis of Using Blockchain to Protect the Privacy of Drone Big Data. *IEEE Netw.* **2021**, *35*, 44–49. [CrossRef]
2. Gumaei, A.; Al-Rakhami, M.; Hassan, M.M.; Pace, P.; Alai, G.; Lin, K.; Fortino, G. Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection. *IEEE Netw.* **2021**, *35*, 94–100. [CrossRef]
3. Cheema, M.A.; Ansari, R.I.; Ashraf, N.; Hassan, S.A.; Qureshi, H.K.; Bashir, A.K.; Politis, C. Blockchain-based secure delivery of medical supplies using drones. *Comput. Netw.* **2022**, *204*, 108706. [CrossRef]
4. Hasan, M.K.; Islam, S.; Shafiq, M.; Ahmed, F.R.A.; Ataelmanan, S.K.M.; Babiker, N.B.M.; Abu Bakar, K.A. Communication Delay Modeling for Wide Area Measurement System in Smart Grid Internet of Things Networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9958003. [CrossRef]
5. Khan, A.A.; Laghari, A.A.; Awan, S.; Jumani, A.K. Fourth Industrial Revolution Application: Network Forensics Cloud Security Issues. In *Security Issues and Privacy Concerns in Industry 4.0 Applications*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2021; pp. 15–33. [CrossRef]
6. Feng, C.; Yu, K.; Bashir, A.K.; Al-Otaibi, Y.D.; Lu, Y.; Chen, S.; Zhang, D. Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach. *IEEE Netw.* **2021**, *35*, 130–137. [CrossRef]
7. Li, T.; Liu, W.; Liu, A.; Dong, M.; Ota, K.; Xiong, N.N.; Li, Q. BTS: A Blockchain-Based Trust System to Deter Malicious Data Reporting in Intelligent Internet of Things. *IEEE Internet Things J.* **2021**, *9*, 22327–22342. [CrossRef]
8. Khan, A.A.; Laghari, A.A.; Shaikh, A.A.; Dootio, M.A.; Estrela, V.V.; Lopes, R.T. A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF). *Neurosci. Inform.* **2021**, *2*, 100030. [CrossRef]
9. Alsamhi, S.H.; Almalki, F.A.; Afghah, F.; Hawbani, A.; Shvetsov, A.V.; Lee, B.; Song, H. Drones' Edge Intelligence Over Smart Environments in B5G: Blockchain and Federated Learning Synergy. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 295–312. [CrossRef]
10. Aloqaily, M.; Bouachir, O.; Boukerche, A.; Al Ridhawi, I. Design Guidelines for Blockchain-Assisted 5G-UAV Networks. *IEEE Netw.* **2021**, *35*, 64–71. [CrossRef]
11. Shafiq, M.; Tian, Z.; Bashir, A.K.; Cengiz, K.; Tahir, A. SoftSystem: Smart Edge Computing Device Selection Method for IoT Based on Soft Set Technique. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8864301. [CrossRef]
12. Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. *IEEE Access* **2022**, *10*, 78887–78898. [CrossRef]
13. Luo, S.; Li, H.; Wen, Z.; Qian, B.; Morgan, G.; Longo, A.; Rana, O.; Ranjan, R. Blockchain-Based Task Offloading in Drone-Aided Mobile Edge Computing. *IEEE Netw.* **2021**, *35*, 124–129. [CrossRef]
14. Khan, A.A.; Shaikh, A.A.; Shaikh, Z.A.; Laghari, A.A.; Karim, S. IPM-Model: AI and metaheuristic-enabled face recognition using image partial matching for multimedia forensics investigation with genetic algorithm. *Multimedia Tools Appl.* **2022**, *81*, 23533–23549. [CrossRef]
15. Abualigah, L.; Diabat, A.; Sumari, P.; Gandomi, A.H. Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. *IEEE Sens. J.* **2021**, *21*, 25532–25546. [CrossRef]
16. Khan, A.A.; Shaikh, Z.A.; Belinskaja, L.; Baitenova, L.; Vlasova, Y.; Gerzelieva, Z.; Laghari, A.A.; Abro, A.A.; Barykin, S. A Blockchain and Metaheuristic-Enabled Distributed Architecture for Smart Agricultural Analysis and Ledger Preservation Solution: A Collaborative Approach. *Appl. Sci.* **2022**, *12*, 1487. [CrossRef]
17. Shaikh, Z.A.; Khan, A.A.; Teng, L.; Wagan, A.A.; Laghari, A.A. BIoMT Modular Infrastructure: The Recent Challenges, Issues, and Limitations in Blockchain Hyperledger-Enabled E-Healthcare Application. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 813841. [CrossRef]
18. Wang, D.; Wu, M.; He, Y.; Pang, L.; Xu, Q.; Zhang, R. An HAP and UAVs Collaboration Framework for Uplink Secure Rate Maximization in NOMA-Enabled IoT Networks. *Remote Sens.* **2022**, *14*, 4501. [CrossRef]
19. Wang, D.; Zhou, F.; Lin, W.; Ding, Z.; Al-Dhahir, N. Cooperative Hybrid Non-Orthogonal Multiple Access Based Mobile-Edge Computing in Cognitive Radio Networks. *IEEE Trans. Cogn. Commun. Netw.* **2022**, *8*, 1104–1117. [CrossRef]
20. Singh, M.P.; Aujla, G.S.; Bali, R.S. Blockchain for the Internet of Drones: Applications, Challenges, and Future Directions. *IEEE Internet Things Mag.* **2021**, *4*, 47–53. [CrossRef]
21. Khan, A.A.; Khan, M.M.; Khan, K.M.; Arshad, J.; Ahmad, F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Comput. Netw.* **2021**, *196*, 108217. [CrossRef]

22. Gupta, R.; Bhattacharya, P.; Tanwar, S.; Kumar, N.; Zeadally, S. GaRuDa: A Blockchain-Based Delivery Scheme Using Drones for Healthcare 5.0 Applications. *IEEE Internet Things Mag.* **2021**, *4*, 60–66. [CrossRef]
23. Aujla, G.S.; Vashisht, S.; Garg, S.; Kumar, N.; Kaddoum, G. Leveraging Blockchain for Secure Drone-to-Everything Communications. *IEEE Commun. Stand. Mag.* **2021**, *5*, 80–87. [CrossRef]
24. Yahuza, M.; Idris, M.Y.I.; Bin Ahmedy, I.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
25. Wang, J.; Liu, Y.; Niu, S.; Song, H. Lightweight blockchain assisted secure routing of swarm UAS networking. *Comput. Commun.* **2021**, *165*, 131–140. [CrossRef]
26. Mei, Q.; Xiong, H.; Zhao, Y.; Yeh, K.-H. Toward Blockchain-Enabled IoV with Edge Computing: Efficient and Privacy-Preserving Vehicular Communication and Dynamic Updating. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Japan, 30 January–2 February 2021; pp. 1–8. [CrossRef]
27. Wang, D.; He, T.; Zhou, F.; Cheng, J.; Zhang, R.; Wu, Q. Outage-driven link selection for secure buffer-aided networks. *Sci. China Inf. Sci.* **2022**, *65*, 182303. [CrossRef]
28. Al-Hourani, A.; Kandeepan, S.; Lardner, S. Optimal LAP Altitude for Maximum Coverage. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 569–572. [CrossRef]
29. He, Y.; Wang, D.; Huang, F.; Zhang, R.; Pan, J. Trajectory Optimization and Channel Allocation for Delay Sensitive Secure Transmission in UAV-Relayed VANETs. *IEEE Trans. Veh. Technol.* **2022**, *71*, 4512–4517. [CrossRef]
30. Islam, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. Blockchain-Enabled Intelligent Vehicular Edge Computing. *IEEE Netw.* **2021**, *35*, 125–131. [CrossRef]
31. Jiang, X.; Yu, F.R.; Song, T.; Leung, V.C. Edge Intelligence for Object Detection in Blockchain-Based Internet of Vehicles: Convergence of Symbolic and Connectionist AI. *IEEE Wirel. Commun.* **2021**, *28*, 49–55. [CrossRef]
32. Yang, J.; Liu, J.; Song, H.; Liu, J.; Lei, X. Blockchain-based Conditional Privacy-Preserving Authentication Protocol with Implicit Certificates for Vehicular Edge Computing. In Proceedings of the 2022 7th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA) 2022, Chengdu, China, 22–24 April 2022; pp. 210–216. [CrossRef]
33. Jing, W.; Fu, X.; Liu, P.; Song, H. Joint resource trading and computation offloading in blockchain enhanced D2D-assisted mobile edge computing. *Clust. Comput.* **2022**, 1–15. [CrossRef]
34. Xu, L.; Ge, M.; Wu, W. Edge Server Deployment Scheme of Blockchain in IoVs. *IEEE Trans. Reliab.* **2022**, *71*, 500–509. [CrossRef]
35. Zhang, D.; Yu, F.R.; Yang, R. Blockchain-Based Multi-Access Edge Computing for Future Vehicular Networks: A Deep Compressed Neural Network Approach. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 12161–12175. [CrossRef]
36. Wang, K.; Tu, Z.; Ji, Z.; He, S. Faster Service with Less Resource: A Resource Efficient Blockchain Framework for Edge Computing. 2022. Available online: https://assets.researchsquare.com/files/rs-1719287/v1_covered.pdf?c=1654894162 (accessed on 31 October 2022).
37. Shaikh, Z.A.; Khan, A.A.; Baitenova, L.; Zambinova, G.; Yegina, N.; Ivolgina, N.; Laghari, A.A.; Barykin, S.E. Blockchain Hyperledger with Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture. *Appl. Sci.* **2022**, *12*, 2534. [CrossRef]
38. Ahmed, M.M.; Hasan, M.K.; Shafiq, M.; Qays, O.; Gadekallu, T.R.; Nebhen, J.; Islam, S. A peer-to-peer blockchain based interconnected power system. *Energy Rep.* **2021**, *7*, 7890–7905. [CrossRef]
39. Khan, A.A.; Laghari, A.A.; Gadekallu, T.R.; Shaikh, Z.A.; Javed, A.R.; Rashid, M.; Estrela, V.V.; Mikhaylov, A. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. *Comput. Electr. Eng.* **2022**, *102*, 108234. [CrossRef]