electronics

MDPI

Article

Lightweight-BIoV: Blockchain Distributed Ledger Technology (BDLT) for Internet of Vehicles (IoVs)

Asif Ali Laghari [1], Abdullah Ayub Khan [1,2], Reem Alkanhel [3,*], Hela Elmannai [3] and Sami Bourouis [4]

[1] Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Pakistan
[2] Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi 75660, Pakistan
[3] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[4] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
* Correspondence: rialkanhal@pnu.edu.sa

Abstract: The vast enhancement in the development of the Internet of Vehicles (IoV) is due to the impact of the distributed emerging technology and topology of the industrial IoV. It has created a new paradigm, such as the security-related resource constraints of Industry 5.0. A new revolution and dimension in the IoV popup raise various critical challenges in the existing information preservation, especially in node transactions and communication, transmission, trust and privacy, and security-protection-related problems, which have been analyzed. These aspects pose serious problems for the industry to provide vehicular-related data integrity, availability, information exchange reliability, provenance, and trustworthiness for the overall activities and service delivery prospects against the increasing number of multiple transactions. In addition, there has been a lot of research interest that intersects with blockchain and Internet of Vehicles association. In this regard, the inadequate performance of the Internet of Vehicles and connected nodes and the high resource requirements of the consortium blockchain ledger have not yet been tackled with a complete solution. The introduction of the NuCypher Re-encryption infrastructure, hashing tree and allocation, and blockchain proof-of-work require more computational power as well. This paper contributes in two different folds. First, it proposes a blockchain sawtooth-enabled modular architecture for protected, secure, and trusted execution, service delivery, and acknowledgment with immutable ledger storage and security and peer-to-peer (P2P) network on-chain and off-chain inter-communication for vehicular activities. Secondly, we design and create a smart contract-enabled data structure in order to provide smooth industrial node streamlined transactions and broadcast content. Substantially, we develop and deploy a hyperledger sawtooth-aware customized consensus for multiple proof-of-work investigations. For validation purposes, we simulate the exchange of information and related details between connected devices on the IoV. The simulation results show that the proposed architecture of BIoV reduces the cost of computational power down to 37.21% and the robust node generation and exchange up to 56.33%. Therefore, only 41.93% and 47.31% of the Internet of Vehicles-related resources and network constraints are kept and used, respectively.

Keywords: smart contracts; blockchain; hyperledger sawtooth; internet of vehicles (IoVs); lightweight PoW consensus; consortium network channels

check for updates

Citation: Laghari, A.A.; Khan, A.A.; Alkanhel, R.; Elmannai, H.; Bourouis, S. Lightweight-BIoV: Blockchain Distributed Ledger Technology (BDLT) for Internet of Vehicles (IoVs). *Electronics* **2023**, *12*, 677. https://doi.org/10.3390/electronics12030677

Academic Editors: Nikolay Hinov, Darius Andriukaitis and Jožef Ritonja

Received: 3 January 2023
Revised: 21 January 2023
Accepted: 23 January 2023
Published: 29 January 2023

1. Introduction

The Internet of Vehicles (IoV) has gained popularity because of its unique prospects, which are adopted globally for distinct purposes. There are various implementational bottlenecks involved, including the IoV systems generally containing a large number of scattered devices and their complex connectivity [1]. It is highly vulnerable when facing cyberattacks, such as DDoS (distributed denial of service). Substantially, the client-server-based architecture for data management and responses is not self-certified [2]. The list of challenges and limitations includes personal privacy leaking, unprotected ledger delivery, transmission inefficiency, and preserved information security. As shown in Figure 1, continuous evaluation in an open wireless network, as well as topology differences, complicate the processing and computation of Internet of Things (IoT)-enabled vehicular applications [3]. However, the number of IoV devices and applications is growing quickly, which leads to higher costs for running central client-server-enabled services. This will make them more expensive to pay for in the future.

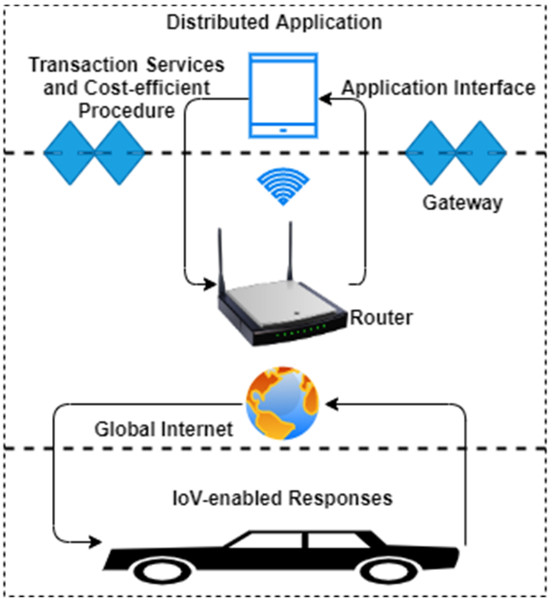

Figure 1. Current working Applicational Interface for IoV.

Several small-medium enterprises (SMEs) are adopting blockchain technology and alleviating its benefits, such as its distributed nature with the collaboration of NuCypher. It protects transactions over the consortium network and maintains ledger integrity, transparency, preservation, privacy, and security [4]. Because of blockchain's decentralized infrastructure, which appends only digital ledgers in chronological order in a chain-like structure, using this technology, consensus operation, immutable storage, and the ability to non-repudiate and ledger untempering, with no forgery, are possible. With these helpful tools, IoV-related applicational information can be shared in a peer-to-peer (P2P) distributed network with consortium capability. It allows for maintaining data traceability in a distributed manner and facilitates flow control in a non-trustable infrastructure [5]. A distributed, decentralized domain name service is also provided, where experts activate the capability of blockchain to mitigate existing vulnerabilities involved in domain name services as well as malicious attacks such as spoofing and phishing. However, the following mechanisms have been successfully implemented and deployed: (i) ride-hailing for autonomous vehicles [6,7], (ii) EPS-Ledger [8,9], and (iii) blockchain for IoV communication protocols [10]. It entails creating a stable blockchain-enabled distributed environment for the industrial intent of vehicles.

However, blockchain distributed ledger technology eliminates the dependency on a third-party authority and relies on certificate authorities. By the act of this, decentralized and mathematically enabled automated mechanisms are applied to ensure information security and privacy from malicious attacks [11]. However, in this case, the IoV-enabled devices required more computational resources to maintain efficient performance. To optimize blockchain resource constraints, a variety of research proposals have been presented since 2019. For instance, Li et al. presented a lightweight blockchain consensus mechanism for the computational constraints of Internet of Things (IoT) devices [12]. For energy efficiency, Yang et al. [13] described a procedure to allocate and manage the efficient energy resources of blockchain-enabled Industrial Internet of Things (IIoT) devices with machine-learning-based reinforcement techniques. In addition, Lu et al. [14] proposed a distributed communication architecture with a federated learning mechanism for a permissioned blockchain to handle the digital twin infrastructure of an edge environment. This technique handles the computational offloading and contents of node transactions and smoothly reduces network traffic, while the mentioned systems do not lighten all the resource constraints of the blockchain hyperledger, especially sawtooth-enabling systems.

Motivation, Objectives, and Contributions

In this paper, several key implementation challenges related to blockchain in the IoV environment are studied. First, it examines and analyzes the benefits of used nodes, including proof-of-work, to continually improve the computational power, while participating stakeholders are unable to maintain the speed of transactional updates. As the size of the node increases, which directly impacts the transactions and deliverance, it leads to centralization in terms of using more computational power in the distributed network. Secondly, to achieve consistency of distribution in peer-to-peer (P2P) networks, which is the most concerning issue involving them in the past few years, all the nodes in the chain require data preservation in immutable storage and maintain a network to exchange transactions between stakeholders without a recycling mechanism. Furthermore, the IoV-enabled devices conflict with different permissioned private network resources. It is difficult for a few resources to support blockchain-related operations in the IoV environment because there are large changes to throughput, response time, and duty cycle.

To provide a solution to these highlighted challenges, we proposed a blockchain hyperledger sawtooth-enabled Lightweight-BIoV. The design of this proposed distributed architecture helps to minimize the resource occupations throughout the deliverance, for example, the blockchain hyperledger sawtooth to the node. Thus, it ensures the real-time performance of the IoV. Thus, the blockchain engineer can monitor all the events of node transactions and access the ledger directly in accordance with the defined consensus policies. However, the resource occupations are categorized into three sub-parts, such as (i) computational power, (ii) network constraints, and (iii) information preservation. In this manner, we design, develop, and deploy a Lightweight-BIoV infrastructure to lighten the blockchain with the use of the hyperledger sawtooth. The major objectives and contributions of this paper are discussed as follows:

- In this paper, a consortium network infrastructure (meaning both public and private channels) is designed. It maintains the implicit and explicit IoV communication and related information exchange between nodes in the chain. During transmission, the Lightweight-BIoV consumption mechanism is presented, which consumes fewer resources in terms of limited network constraints with a fixed size of blocks, which provides efficient service delivery communications.
- A secure blockchain sawtooth-enabled distributed modular architecture for the IoV is proposed. It provides robust performance in terms of events of IoV nodes' transaction deliveries with privacy and ledger security that uses reduced resource constraints of network bandwidth throughout.
- For IoV transactions and deliverable log storage, we choose InterPlanetary File Storage (IPFS) with a blockchain-unrelated node offloading filter mechanism. It examines and optimizes the IoV-related transactions before they are preserved in the immutable ledger and shares acknowledgment among participating stakeholders.
- A consensus mechanism of the hyperledger sawtooth is tuned for multiple proof-of-transactions (a customized proof-of-work called BIoV consensus). It promotes connectivity between Internet-of-Vehicles-enabled devices. In addition, while mining, we also set the range of parameters that analyze the node workload capability to

effectively handle the reduced consumption of computational power and save energy better than the blockchain proof-of-work.

- The smart contracts/chaincodes are implemented and deployed to automate verification and validation of IoV-enabled transactions from initial acquisition to the deliverance process. Thus, details of delivery are exchanged with participating stakeholders in accordance with the protocols of the hyperledger sawtooth. To protect the execution of the transaction, we use the NuCypher Re-Encryption mechanism, which efficiently maintains the hashing tree.
- Finally, we evaluate and analyze the policies of lightweight-BIoV, and open research challenges involved in the future blockchain-IoV environment.

The rest of this paper is structured and organized as follows: In Section 2, several blockchain-chaincodes-related distributed vehicular architectures and hyperledger technologies are studied. The traditional security mechanism and existing topology of privacy preservation in the IoV are discussed in Section 3. Section 4 proposes a blockchain sawtooth-aware protected and secure distributed architecture for IoV privacy, security, dynamic resource management, and lightweight authentication. The simulation results are presented in Section 5. We also compare the proposed distributed architecture with other state-of-the-art methods and models, along with open research issues. Finally, Section 6 concludes this paper.

2. Related Work

The new research proposals in the IoT and the development of industrial systems provide a variety of opportunities to control machine-to-machine communication and connect different devices without any physical intervention [15]. Resource constraints, such as delay tolerance, are considered one of the challenging aspects that need concern. Li et al. [15] presented the mechanism to reduce and handle efficient communication and connectivity between IoT devices, respectively. For this purpose, it puts more emphasis on the other constraints, including caching powerful data, processing and computations, privacy, security, and stability in scaling node transactions over the distributed network. In intelligent transportation systems and privacy, Jiang et al. [16] described the benefits of blockchain distributed technology to improve the performance of the internet of vehicles' data integrity and transparency in an edge environment. In this case, it improves the intelligent transportation network node connectivity and transaction delivery. It also manages the collaboration of blockchain technology with AI.

Feng et al. [17] presented a joint optimization solution for blockchain-enabled IoT-edge devices. The main objective of this work is to limit computational resources and increase performance. Several works are presented in order to achieve the best trade-off in a distributed environment, to effectively reduce energy consumption in terms of delay, duty cycle, response, and so on, while maintaining robust performance. For more efficient analytics in this domain, we need to consider the additional matrices such as data rate and allocation, scheduling and managing node producers, computational resource allocation and investigation, and quality of service and experience. On the IoV nodes, transactions via permissioned networks require variable optimization for evaluating transactional data blocks individually, which aims to design an efficient infrastructure and protocols. Therefore, a decoupled strategy with artificial intelligence is proposed. As shown in Table 1, there are a few different types of literature on blockchain-enabled IoV technology that are discussed.

Table 1. Literature on Blockchain Smart Contracts and Hyperledger-Technology-Enabled Architecture for IoV Security and Privacy.

Research Methods	Detailed Working Procedure of the Proposed Work	Current Issues/ Challenges/Limitations	Similarities and Differences with the Proposed Work
A Blockchain-enabled distributed architecture for empowered asynchronous federated learning is proposed to secure the IoV ledger and provide data-exchanging facilities among participating stakeholders [18].	Lu et al. presented a modular architecture based on a federated learning strategy that releases a load over network transmission and privacy-related concerns using blockchain distributed ledger technology with deep learning.	• Consume more computational power while authenticating stakeholders. • To keep transmission resources, a local directed acyclic graph (LDAG) is used. • Cross-chaining issues.	• Two-stage verification. • A Blockchain-based permissioned network. • Deep reinforcement learning. • Asynchronous federation. • Hybrid blockchain.
A collaborative approach of blockchain and deep-neural-network-enabled cooperative positioning is defined for IoV [19].	The authors of this paper defined the fundamental procedure of cooperative positioning and the current implementation issues, along with security features discussed, as follows: • Lane-level positioning constraints. • The issue of a degree variation. • Energy consumption.	• A multi-intelligent vehicle positioning error. • Common vehicle GPS • The scope of data. preservation and protection issues.	• The permissionless blockchain network is defined. • An artificial neural network is used to optimize multi-channel transactions.
A roadside unit that helps with ledger authentication and digital signatures for IoV devices that use blockchain technology [20].	Xu et al. described the capability of blockchain technology to handle multi-trusted authorities in a permissioned network. This paper also highlighted the concept of multi-authentication and key agreement protocols concurrently.	• Cross trusted authority. • Layered hierarchy for road-side units. • Centralized authentication protocols affect trusted authority communication and computing resources.	• The simulation platform ProVerif is used. • A blockchain permissioned network. • Pre-defined consensus mechanism;
Blockchain for IoV security and privacy along with proof-of-work protocols defined [21]	A comprehensive blockchain-enabled solution was proposed for IoV security and privacy protocols. The highlights of this paper are discussed as follows: • Overcome the blockchain scalability issue. • Authentication and network resource limitations • Thus, the computational analysis matrices are defined.	• Platform interoperability issues. • Cross-chain blockchain limitation. • Privacy preservation challenge. • High-level resource consumption.	• No hyperledger technology is used. • Hash-encryption SHA-256. • Third-party distributed storage is used. • Blockchain public network. • Predefined consensus mechanism.
Blockchain multi-channel mechanism for managing resource constraints of IoV [22]	This paper diverted the path of simple blockchain toward the multiple blockchain scheme for IoV to optimize vehicle density. It also managed the node's transactional throughput and latency throughout the execution of the event.	• Scope of data exchange and communication. • Streamline automation. • Centralized blockchain service architecture issues (interoperability).	• Trusted third party. • Vehicle density level. • Multi-level blockchain protocol. • Hash encryption.
Hierarchical blockchain federation learning reduces the computational resource consumption framework for knowledge sharing in IoV environment [23].	The authors of this paper proposed a hierarchical blockchain-enabled framework for IoV devices and elaborated on the feasibility of the adaptation of a hierarchical model for managing large-scale vehicles over the network. Furthermore, it calculated the data sharing behavior while transmitting the data from source to destination and recorded all the details in immutable storage.	• Distributed patterns and privacy requirements. • Tuned consensus policies defined. • Nodes of transaction execution resource limitation. • Participating stakeholder's authentication problem.	• Federated learning. • Blockchain permissionless network. • Machine learning method. • Cryptographic encryption algorithm used.

3. The Internet of Vehicles Security and Blockchain Technology

The paradigm of the Internet of Things (IoT) has changed conventional IoVs from small-scale ad hoc-based networks to the higher scale of manageable IoVs with a distributed ledger architecture [24,25]. The IoV-enabled devices consist of several connected sensors, each of which has an individual task, such as details of movement, speed, directions, collisions, and receiving and transmitting records/logs. Some sensors collect distinct types of data and transmit them to computational nodes for examination and analysis based on which direction the data are moving in order to be delivered to an individual vehicle. The path of deliverance, computational nodes, and vehicle-to-vehicle communication and connectivity consume higher levels of resources with privacy and security loopholes. For this reason, we identified the problem in the IoV environment and proposed a blockchain hyperledger sawtooth-enabled modular architecture called Lightweight-BIoV that provides a consortium infrastructure to reduce the IoV-related cost of resource constraints down to 37.21%. The details of the Lightweight-BIoV are discussed as follows.

3.1. The Proposed Lightweight-BIoV Architecture

The proposed Lightweight-BIoV presents the blockchain-enabling secure modular infrastructure for IoV security, resource management, efficient information preservation facility, and dynamic monitoring for further ledger investigation. In the proposed architecture, the blockchain serverless network environment is designed to manage the complete procedure of vehicle data collection to deliverance with the use of wireless network sensors (radio-frequency identification sensors), as shown in Figure 2. This process starts with individual IoV devices, which are moved to workshops and then moved toward the warehouse in order to maintain the protocols of service delivery.

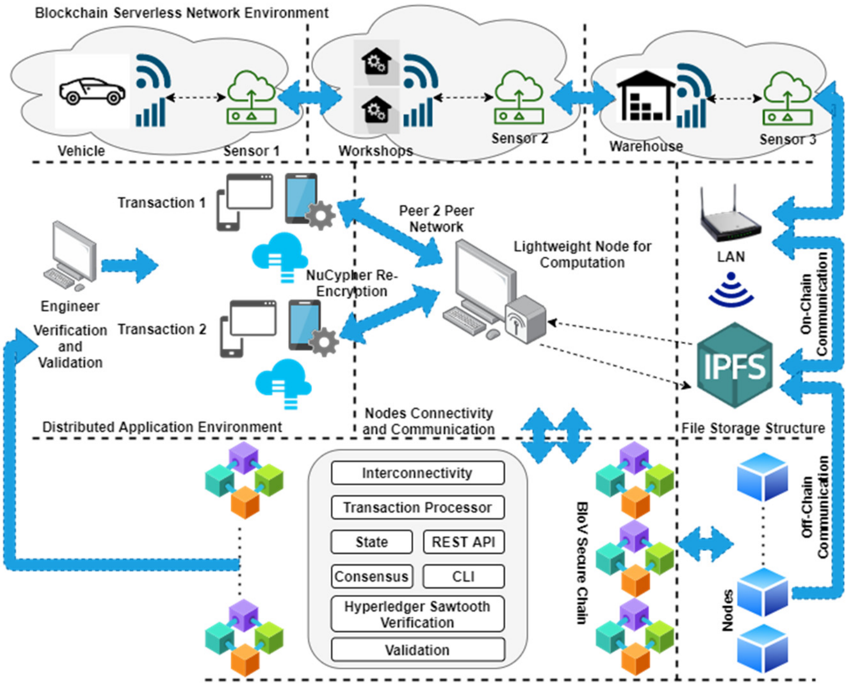

Figure 2. The Proposed Lightweight-BIoV Architecture.

In this scenario, the generated data related to IoV devices can be examined and analyzed by the workshops, which detect problems and propose amendments as well. Records of individual devices are submitted to the warehouse. As shown in Figure 2, all these transactions are successfully received and delivered because of the local area network (LAN) in order to maintain ledger security. The LAN is used to transmit to the duty node, whose applicational layer allows the sending of the action types, for example, transmit and write, and send ledger details to the Lightweight-BIoV-defined layer. After this complete process execution, all the transactional details and addresses are preserved in the InterPlanetary File Storage (IPFS). However, the IPFS is the third-party immutable file storage structure that provides a distributed ledger preservation environment to record

IoV-related information, logs, access details, actions, and errors at a lower cost. On-chain and off-chain communication protocols are designed in such a way that the off-chain can handle the IoV nodes' related transactions outside the network, while the on-chain handles all the related transactions implicitly.

The distributed applicational environment is designed and created to handle large-scale dynamic IoV transactions. In this, the blockchain hyperledger performs the key objectives to verify and validate each device and node connectivity before transaction occurrence. The P2P distributed network is designed that act as a bridge between the events of IoV-related truncations transmission and computational nodes. This procedure reduces the communication and network-based resource constraints and cost of connectivity in the distributed environment. However, we designed a hyperledger sawtooth-enabled multiple-validation mechanism to verify the integrity, transparency, and validity of pending validation of the digital signature, as shown in Figure 2. This former execution enabled the consortium-based NuCypher Re-Encryption [26,27], to protect against two-way attacks known as spending attacks and ensure the transaction request is not forged throughout the propagation. Every IoV transaction collaborates with two attachments, which are digital signature validation and privacy, which aim to verify the type and transaction format. These attachments are standardized. In this regard, the Lightweight-BIoV provides data traceability, IoV-related workshops, warehouse manufacturing records, and other performed details stored concurrently among all the connected distributed devices.

The large-node size and blockchain scalability have an impact on ledger preservation and, thus, the distributed nodes' limited storage capacity controls. In this paper, we divide the file storage mechanism into two different parts, where it performs concurrently and substantially. Dynamic storage (serverless storage, as shown in Figure 2) is the only cache memory whose objective is to filter transactional data. whereas a copy of the IoV distributed ledger containing the complete list of operations, controls, and actions is registered and stored in IPFS storage, which will aid in future investigations.

3.2. Problem Formulation and Notations

In the proposed Lightweight-BIoV, we designed a layer hierarchy that converts IoV actions according to the defined types (transmit/write) and sends these flows by applicational layer into predefined types. The BIoV procedure extracts the inputs, T1, outputs, T2, and constraints object $\mathrm{T}\hat{}'$, when a transaction request T' is received. It is highlighted that the procedure of transaction execution is the same as the blockchain-bitcoin-based coin incentives. Thus, the transactions are executed as normal transactions with a collaborative procedure, such as cross-validation. For IoV transactions' integrity and transparency, we designed and created a security component using a cryptographic hash encryption mechanism, where T' encrypts it using the NuCypher Re-Encryption algorithm. Flowing through the two-attachment mechanism, this blockchain hyperledger sawtooth-based digital signature is complete. The chain execution can now move on with its work, thanks to this process.

The execution of consensus and their calculation is based on the hyperledger sawtooth-enabled transaction processor, which is predefined in nature. These consensus protocols are responsible for handling and maintaining a list of peers and creating transmission control protocols (TCP) or internet protocols (IP), which connect devices. Every block-based transaction in the local host environment generates a verification request. The blockchain hyperledger sawtooth engineer is responsible for handling all these applicational requests and sending the message commands, such as *msg.file[type]*, after verification and validation of nodes with IoV devices.

However, the distributed consensus operations, executions, and pr*msg.file[type]*eservation with presentation are designed using a consortium distributed mechanism. It is open to all the industrial IoV nodes for secure transactions in a trusted hybrid environment. Thus, it belongs to both private and public chains. In this case, the Lightweight-BIoV concurrently uses proof-of-work for parallel execution in the hyperledger sawtooth-enabled modular infrastructure. It sets the load-of-work according to the size of the node transaction in the consortium environment to avoid collisions unless its results are decreased to its finalized predefined target. With this act, we achieve a reduction in the computational power in the distributed IoV transactional environment.

$$NuCypher\ \left(Re - Encryption\ \left(IoV_{devices_{nodes}} + size\ of\ data\right)\right) < t \tag{1}$$

where 't' is the predefined target and '+' is performed as a concatenation symbol between the IoV nodes and the data size that will transact, as shown in Equation (1).

Observing the working operations of the hyperledger sawtooth and limited size of the transaction because of computational nodes restricts the industrial IoV devices capability; for this reason, we proposed a Lightweight-BIoV consensus that is different from the proof-of-stake. In the load-of-work distribution, the proposed consensus handles the competition because of the defined degree of collaboration, as mentioned in Smart Contracts.

$$\text{Collaborative degree} = [(\text{average throughput}/\text{predefined throughput threshold} \times \text{total number of transactions})\ \text{collaborative index}/\text{node size (KB)}] \tag{2}$$

Thus, this procedure reduces the network resources in the distributed environment, as mentioned in Equation (2), whereas the blockchain hyperledger sawtooth engineer owns the permission to add new devices, access the control, authentication, and node filtration, and offload the local ledger. The transactions on the blockchain are mainly based on the bitcoin-based coin incentive-enabled mechanism. The input transactions are subsequently referred to as a list of outputs that belong to the previous transactions with the index value. Through the rollback, the genesis IoV devices (blocks) trackback with the full nodes because of the graph structure. This makes for complete and proper blockchain storage for ledger preservation. However, the pending transaction that causes a two-way spending problem cannot be looked at right away, because it needs to be proven that other transactions are legitimate.

4. Working Operations of the Proposed Blockchain Hyperledger Sawtooth-Aware IoV

In this context, we present the working operations of the proposed Lightweight-BIoV for the IoV events of node transactions and ledger privacy and preservation through smart contracts and control mechanisms. They are discussed as follows:

Smart Contracts

As shown in Appendix A (Smart Contracts), the BIoV initializes the IoVTransaction() function, which receives data from various IoV devices according to the criteria of the system, such as collecting all the receive and response data of an individual IoV, capturing all the transmission details, node connectivity (active and passive), and logs of stored records. After that, initial registration of new devices is required with IoV-device authentication. It is a two-way process but consumes less cost and allows easy management to access the digital ledger environment, in order to perform IoV-related transactions according to the assigned task and to preserve all the logs in the distributed storage. The blockchain hyperledger sawtooth engineer initiates contract functionality with the design consensus policies and creates a ledger preservation contract (IoVLedgerPres()) to store IoV processed data immutability. The proposed BIoV contracts also record the additional information, such as ioVDR(), ioVLGN(), ioVAT(), ioVIP(), soB(), ioVTD(), ioVT(), ioVD(), ioVR(), blockchain hyperledger sawtooth-enabled current timestamp() [execute], and other related activities performed. Thus, it automatically registers in the IPFS distributed storage with the help of the designed IoVTransManage() contract, as shown in Table 2. These three contract functions are designed, implemented, and deployed to investigate individual IoV-related transactions and to record all these logs in immutable storage for future processing.

Table 2. Comparison of The Proposed Lightweight-BIoV with Other Methods.

Purpose of Work	Research Features	Performance Matrix	Compared with Our Proposed Lightweight-BIoV
An anonymous authentication approach was proposed for lightweight cross-regional mutual verification and validation with the help of blockchain distributed ledger technology in the IoV environment [28].	Meng et al. presented the main features of a lightweight anonymous authentication system, such as automated validation, formal proof of BAN logic, security protocol, and key agreement strategy, using the blockchain Ethereum architecture.	The evaluation criteria of the proposed scheme are discussed as follows: • Blockchain network: Permissioned network. • Hyperledger: No hyperledger used. • Encryption: Hash-encryption. • Consensus: Predefined. • Reduce resource constraints: computational cost and network load. • Accuracy: Not applicable. • Optimization: Not defined. • Node size: Fixed. • Storage: Cloud-based.	Our proposed Lightweight-BIoV reduces the consumption of blockchain-IoV-enabled resources into three different categories, such as computational power, network, and storage. The defined matrix presents the importance of system adaptation in an industrial IoV environment. • Blockchain network: Consortium. • Hyperledger: Hyperledger Sawtooth. • Encryption: NuCypher Re-Encryption. • Consensus: Proposed new consensus for reducing the load of work and PoW transactions. • Reduce resource constraints: Network, computing energy, and preservation. • Accuracy: Computational cost down to 37.21%. • Optimization: Not applicable. • Node size: Fixed size 4 MB. • Storage: IPFS distributed storage.
A blockchain consensus mechanism was presented for IoV security and privacy [29].	A consensus mechanism was presented that prevents user control over the 5G network. The main features of the proposed system are as follows: • Hoarding huge-scale coins. • Reduce the cost of messages. • Automated verification of the IoV ledger. • Secure preservation.	The examination and analysis matrix of the proposed system are as follows: • Blockchain network: permissionless public network. • Hyperledger: no hyperledger used. • Encryption: Hash-encryption. • Consensus: Proof-of-stake (PoS). • Reduce resource constraints: Communication and Connectivity. • Accuracy: Not applicable. • Optimization: Not defined. • Node size: Fixed. • Storage: Cloud-based.	
A secure data preservation solution was demonstrated for distributed vehicular permissioned networks [30].	A secure data sharing, exchange, and preservation mechanism is defined in this research. The highlights of this paper are as follows: • IoV-related ledger integrity and transparency. • Analysis and optimization of gas consumption. • A new caching system was implemented. • Vehicular network defined.	The criteria of the proposed system investigation are discussed as follows: • Blockchain network: public network. • Hyperledger: No hyperledger used. • Encryption: Hash-encryption. • Consensus: Proof-of-Authority (PoA). • Reduce resource constraints: network and communication. • Accuracy: Not defined. • Optimization: Gas consumption. • Node size: Customize. • Storage: IPFS.	

5. Simulations, Results, and Discussion

In this section, we define the complete procedure of the proposed lightweight-BIoV, in which a consortium P2P network provides connectivity with different computing nodes to initiate the data processing and related procedure, as shown in Figure 3. Each node is equipped with an Intel i7 v pro CPU (2.3 GHz) and executes Windows 10 with Hyperledger Docker and the generic kernel. Every node is designed with static and dynamic memory to hold data during parallel processing. We simulated the practical conditions of the

IoV (prototype of land-enabled general IoV associated with WSN) while designing and implementing the consortium architecture. The main assumptions behind these simulated results are discussed as follows:

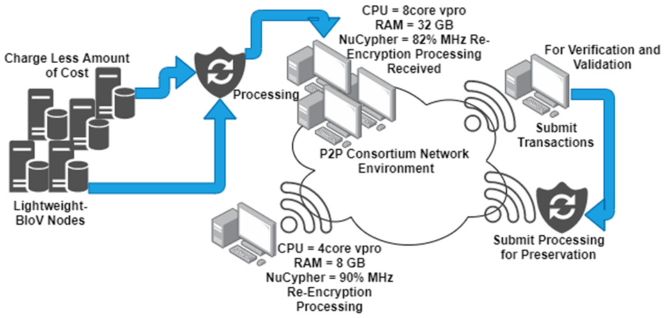
CPU = 8core vpro
RAM = 32 GB
NuCypher = 82% MHz Re-Encryption Processing Received
Charge Less Amount of Cost
For Verification and Validation
Processing
Submit Transactions
P2P Consortium Network Environment
Lightweight-BIoV Nodes
Submit Processing for Preservation
CPU = 4core vpro
RAM = 8 GB
NuCypher = 90% MHz Re-Encryption Processing

Figure 3. Criteria for IoV Node Evaluation.

Resource constraints: To reduce the computational cost and increase the performance of a distributed node structure, a fixed block size/storage is allocated to individual nodes, which is up to 4 MB/transaction.

Consortium network topology: In this prospect, the individual node processing is dedicated to a public internet protocol with a limited bandwidth of up to 1 Mb per second. At the same time, the designed local area network allocates 1 GB per second.

Node heterogeneity: For scheduling distribution, we contract a heterogeneous consortium P2P network, whose task is to configure node connectivity and memory management, as shown in Figure 3.

In this paper, we highlight the monitoring perspective and deploy blockchain hyperledger engineers to monitor the usage of the CPU and consumption of computational power. We also compare the current proof-of-work with the proposed Lightweight-BIoV consensus. The contrast between Figure 4(1),(2) shows that the proposed consensus reduces the workload and achieves the percentage of 37.21% (−60 to −30, and −40 to −10), which shows that the computational cost decreases drastically. By the adaptation of the consensus, we alleviate the utilization of computing resources and increase performance.

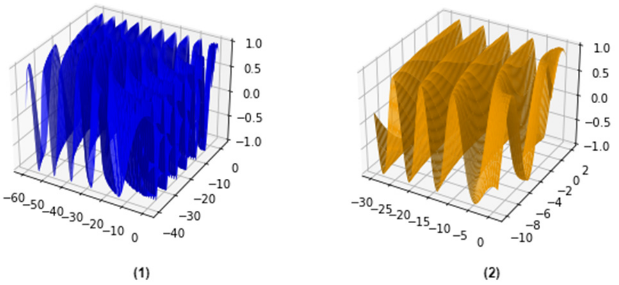

Figure 4. CPU Usage and the Rate of Computational Power Utilization. (**1**) The current Hyperledger PoW and (**2**) the Proposed Lightweight-BIoV Consensus.

Figure 5 shows the consumption of the computational power of all the connected nodes, whose metric is elaborated as the total number of nodes analyzed (in dynamic time) and the operations of NuCypher Re-Encryption operations that a Lightweight-BIoV signal measure tried during the ten (10) iterations. In addition to this, we also tune the configuration of different analyzing nodes and reduce difficulties for node examiners to further enhance the heterogeneity of the consortium network. Through the management of such difficulties, we increase the rate of data generation and management in the node by up to 56.33%, whereas the high quality of proof-of-work is defined to measure the efficiency of the proposed BIoV for energy utilization.

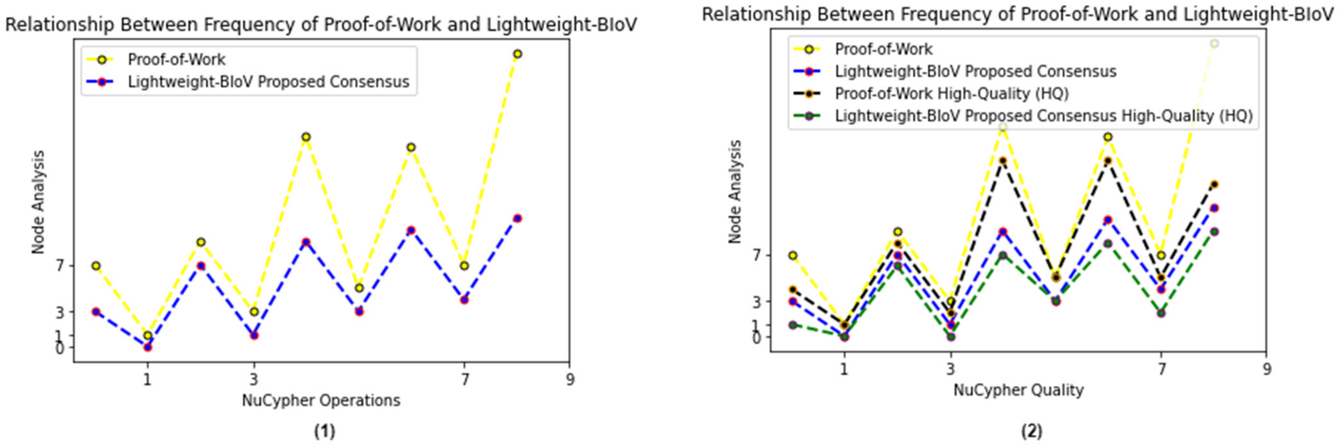

Figure 5. The Computational Cost Utilization: (**1**) Demonstrates the Relationship between the Proof-of-Work and BIoV Consensus Using NuCypher Operations and Node Capability. (**2**) Demonstrates the Large Scale of High-Quality Measurement.

As the results of the simulation, Figure 6 shows the distributed computation over the consortium public/private distributed network between the hyperledger proof-of-work (PoW) (utilized 350 cycles) and the proposed Lightweight-BIoV consensus (utilized 200 cycles, which are customized in nature), whose metric is the total number of IoV devices generating data and the number of process executions. It is clear that the BIoV reduces the cost of computations in the distributed network environment by 41.93% and increases the performance of node transactions and examinations by 47.31%.

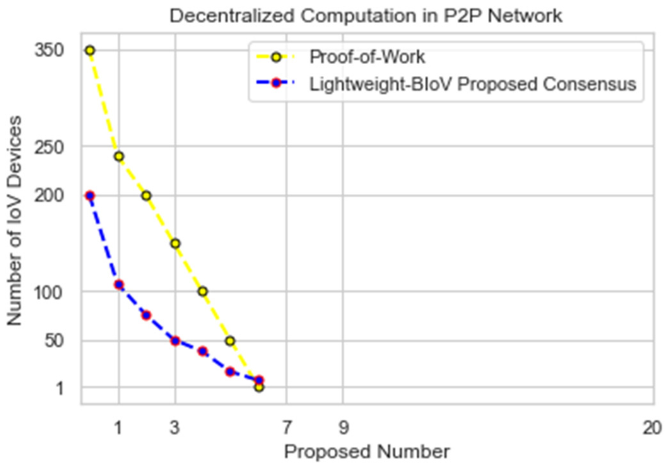

Figure 6. P2P Consortium Network Simulation Result of Decentralized Distributed Computation.

Figure 7 illustrates the total amount of IoV-enabled device data (such as details of movement, speed, directions, and collisions) that are filtrated under different nodes, and the throughput is evaluated, whereas 7(a) shows the comparison of IoV ledger preservation, whose metrics are the total number of throughput and the local node analysis; in this case, the blue bar represents the hyperledger of PoW and the orange bar shows the performance of the Lightweight-BIoV. Meanwhile, Figure 7(2) illustrates the duty cycle during the IoV data preservation in the distributed immutable storage (IPFS). It clearly highlights that the proposed BIoV performs better compared to the previously proposed blockchain methods.

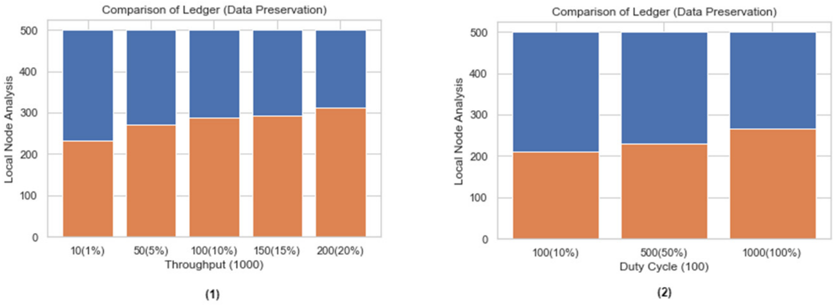

Figure 7. Comparison of Ledger Preservation or Data Storage: (**1**) the calculation of Throughput, and (**2**) the calculation of Duty Cycle.

In the IoV, the trust authority is designed and used to manage the node of the vehicle to realize strong interaction between different vehicles for the purpose of sending and receiving data and records and to promote both the developing details and experience of IoV safety and privacy. The node of the vehicle consists of integrated data acquisition devices, computing nodes, storage, and communication devices. These nodes are used to collect the day-to-day dynamic time of data, actions, and impact on the environment and quality of service and experience. In this regard, Bonadio et al. [31] presented an integrated system architecture for the full context of a vehicle network to react to the traffic anomalous condition. This procedure provides a secure manner of data transmission and preservation but consumes an additional cost of storage with a complex infrastructure of data storage in the fog environment. On the other hand, Xiao et al. [32] proposed BS-IoV, a blockchain-enabled distributed architecture for IoV security. This work is mainly focused on the roadside units, which are designed for mobile edge computing to maintain secure communication and data preservation, and guarantee high-quality transaction delivery. As compared to this, the research method provides efficient IoV node transactions facilities but uses blockchain-enabled resource constraints such as network, storage, and computational power with no additional consensus mechanism and data encryption protocols. However, we look at some of the related research work in terms of the matrix that was set-up. This is shown in Table A1.

5.1. *Open Research Environments*

In this context, the paper evaluates, examines, and presents the proposed serverless hyperledger sawtooth-enabled secure IoV architecture. It provides a novel and protected platform where vehicular-related information transactions and management procedures and protocols are presented. Thus, there are a few challenges and limitations reported with detailed descriptions. In this manner, this paper explains such emerging open research issues and future directions and provides a few solutions to the current issues for the futuristic development of secure distributed applications in the Industrial IoV.

5.1.1. Interoperability Issues and the Role of Hyperledger Cross Chaining

Scheduling, processing, managing, organizing, and preserving high-scale generated records in the domain of a blockchain-enabled distributed environment are challenging problems. There are numerous research proposals and solutions available today, but we have yet to find a specific platform that achieves the mentioned problem exclusivity [33]. This causes an interoperable issue that requires a proper ecosystem where blockchain-enabling systems can interact directly without any interventions. Moreover, the ecosystem also requires novel design and development to maintain integrity and transparency between different blockchains. One of the reasons for building a distributed architecture is to have blockchain capabilities. It handles scalability-related issues that do not affect the transactional protocols and delivery. This act makes systems more reliable in terms of privacy, security, protection, and managing node time availabilities. However, hyperledger technology plays a vital role in building an interoperable architecture to reduce operational costs and increase performance in the distributed environment. The lack of a direct interoperable solution impacts the prevention of the IoV of node transactions execution. It involves third-party connectivity, which also creates a huddle in the communication over the network. The industrial IoV must focus on the stateless environment, SPVs, atomic swaps, relays, and response because of merged consensus and federated learning for synchronized systems' safety and efficiency in terms of interoperable connectivity.

5.1.2. Information Management and Prevention in Distributed Environments

These days, the adaptation of blockchain distributed technology makes most of the concept easier as compared to the centralized server-based architecture. The main objective is to maintain the distributed ledger infrastructure because it is needed to protect information from malicious attacks. The list of attacks that impact information integrity and transparency includes spoofing, tampering, information disclosure, distributed denial of service, and elevation of privileges [33–35]. It can be attacked through different techniques, either used for jamming the network or eavesdropping and intrusions. However, these malicious activities compromise the IoV devices, which cause several negative prospects, for example, accidents. In a real-time scenario, it can affect stability, performance, and robustness, which leads to halted IoV devices in running conditions. User authentication attacks are one of the challenging aspects; a Sybil attack may claim multiple identities from a single source node in a network. Withholding multiple identities affects the control procedure of the system. This poses a serious issue while logging into the environment. However, the blockchain hyperledger sawtooth-enabled modular architecture provides consortium network connectivity that allows two-way lightweight authentication that requires engineer verification and validation, but it requires 24/7 availability. In this case, experts need to pay attention to the blockchain-based authentication verification protocols and the lightweight validation strategy.

5.1.3. IoV Ledger Preservation and Privacy Concerns

Managing, organizing, and preserving large-scale IoV information and records in distributed immutable file storage systems is a critical task. In dynamic times, dealing with log duplication and IoV ledger redundancy issues is difficult [5,33]. While the IoV distributes transactions, node scalability is the key task for maintaining an efficient storage structure. For this purpose, experts should focus on the sharding mechanism along with the meta storage concept. The transparency and consistency of B-IoV applications during the process of sharding are more complex in the distributed environment. Not only that, maintaining elastic scaling is also not an easy task either. Until we transform the distributed applicational storage concept into static data sharding, with this advancement, it is difficult to handle elasticity statistically. Another thing that can be difficult in a distributed storage environment is how to distribute the keys and make the shards random.

5.1.4. Node Transactions and Connectivity Events

The complete process of IoV node installment and designing connectivity takes a significant amount of time and needs expert management to deploy protocols [34,35]. The hyperledger sawtooth engineer is the only manager and is responsible for designing nodes that preserve information reliably and correctly in a distributed environment. In this case, all the preserved ledgers in the nodes should keep an image of individual files in their distributed storage infrastructure [33,35]. Through this act, the inter-nodes can directly connect and communicate. However, it consumes more storage resources as compared to the centralized structure. It also increases the capability of engineering; deploying intercommunication nodes privacy with two different blockchains and effective information exchange among participating stakeholders are still the most challenging prospects in the domain of blockchain streamlined node transactions and monitoring environment.

6. Conclusions

The main purpose of this research is to highlight the existing security and privacy mechanisms and protocols, and the gaps between the connected IoV devices during communication over the network are discussed. In this paper, we propose a lightweight-BIoV blockchain hyperledger sawtooth-enabled IoV architecture to alleviate the resource adaptation of blockchain DLT and make the system more suitable. This lightweight-BIoV presents the design/infrastructure as resource-efficient without affecting the system's provenance and maintain efficient information traceability and reliability with no repudiation of the hyperledger sawtooth. However, we design, create, and deploy smart contracts and multiple PoW consensus mechanisms to investigate in terms of verification and validation of vehicular node transactions with a reduced consumption of computational power. During transmission to delivery, the vehicular information is optimized and preserved in the distributed immutable storage in accordance with the designed smart contracts-enabled data structure to streamline transactions and broadcast content. Furthermore, we present two different communication channels for accessing ledgers, filtering identities, and helping to mitigate the load of storage-related costs and optimization purposes, such as on-chain and off-chain communication, respectively. In the end, the simulation results show that adopting this proposal and using it in the real world is a good candidate.

Author Contributions: A.A.K. wrote, prepared, structured, and organized the original draft. A.A.L., A.A.K., R.A., H.E. and S.B. reviewed, rewrote, and performed part of the literature survey; edited, investigated, and designed the hyperledger architecture; explored distributed applicational tools. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by both Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. This work was also supported by the Taif University Researchers Supporting through Taif University, Taif, Saudi Arabia, under Project (TURSP-2020/26).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like also to acknowledge Taif University Researchers Supporting Project number (TURSP-2020/26), Taif University, Taif, Saudi Arabia.

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

Appendix A

Table A1. Pseudo-Implementation of the Proposed Lightweight-BIoV Smart Contracts.

Input Data: Blockchain Hyperledger Engineer Responsible for Managing Secure Each IoV Transaction and Ledger Preservation
Capture Data from IoV devices
Collect Transmission records
Collect details from Storage Structure
Node Connectivity and Communication Details
Resources Constraints Declaration and Assumptions: Analysis Blockchain Resource Constraints before Executing IoV-Transactions
Variables Declaration and Initialization:
int main().file[type][main]:
IoV device registration
(ioVDR());

Table A1. *Cont.*

IoV logs generation number
(ioVLGN());
IoV assign task
(ioVAT());
IoV information preservation
(ioVIP());
size of block
(soB());
IoV transmission details
(ioVTD());
throughput
(ioVT());
delay
(ioVD());
response
(ioVR());
Blockchain Hyperledger Sawtooth-enabled current timestamp()
[execute];
Steps/Process: Blockchain Hyperledger Sawtooth Engineer responsible to manage all the IoV transaction and log preservation and store addresses
IoVTransaction() contract;
if int main().file[type][main]: = Blockchain Hyperledger Sawtooth Engineer = true
then,
if IoVIP == false
then,
preserve new node transactions and exchange information
counter + 1;
add additional information and addresses,
ioVDR(), ioVLGN(), ioVAT(), ioVIP(), soB(), ioVTD(), ioVT(), ioVD(), ioVR(), Blockchain Hyperledger Sawtooth-enabled current timestamp() [execute];
preserve individual records along with addresses in the IoVLedgerPres() contract;
and manage each ledger in the horizontally IoVTransManage() contract in the IPFS;
else
change state analysis, records detail, check other details, and trackback;
else
change state analysis, records detail, check other details, and trackback;
Output: IoVTransaction(), IoVLedgerPres(), and IoVTransManage()
Consensus Policies:
Proof-of-work (PoW) = Lightweight-BIoV PoW:
Order individual transaction in chronological structure;
NuCypher Encrypted (each ledger transmission);
Add data on IoVLedgerPres() and exchange; 51% vote (digital signature) is required to update ledger() and exchange;

References

1. Benalia, E.; Bitam, S.; Mellouk, A. Data dissemination for Internet of vehicle based on 5G communications: A survey. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3881. [CrossRef]
2. Zhang, T.; Zhang, D.-G.; Yan, H.-R.; Qiu, J.-N.; Gao, J.-X. A new method of data missing estimation with FNN-based tensor heterogeneous ensemble learning for internet of vehicle. *Neurocomputing* **2021**, *420*, 98–110. [CrossRef]

3. Chen, C.; Quan, S. A Summary of Security Techniques-Based Blockchain in IoV. *Secur. Commun. Netw.* **2022**, *2022*, 8689651. [CrossRef]
4. Bourouis, S.; Laalaoui, Y.; Bouguila, N. Bayesian frameworks for traffic scenes monitoring via view-based 3D cars models recognition. *Multimed. Tools Appl.* **2019**, *78*, 18813–18833. [CrossRef]
5. 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]
6. Khan, A.A.; Laghari, A.A.; Shaikh, A.A.; Bourouis, S.; Mamlouk, A.M.; Alshazly, H. Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission. *Appl. Sci.* **2021**, *11*, 10917. [CrossRef]
7. Khan, A.A.; Laghari, A.A.; Shaikh, Z.A.; Dacko-Pikiewicz, Z.; Kot, S. Internet of Things (IoT) Security with Blockchain Technology: A State-of-the-Art Review. *IEEE Access* **2022**, *10*, 122679–122695. [CrossRef]
8. Shubhani, A.; Kumar, M. Hyperledger. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 323–343.
9. Nishi, F.K.; Khan, M.M.; Alsufyani, A.; Bourouis, S.; Gupta, P.; Saini, D.K. Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. *J. Sens.* **2022**. [CrossRef]
10. Ramesh, T.R.; Vijayaragavan, M.; Poongodi, M.; Hamdi, M.; Wang, H.; Bourouis, S. Peer-to-peer trust management in intelligent transportation system: An Aumann's agreement theorem based approach. *ICT Express* **2022**, *8*, 340–346.
11. 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*, 3813841. [CrossRef]
12. Li, C.; Zhang, J.; Yang, X.; Youlong, L. Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices. *Inf. Process. Manag.* **2021**, *58*, 102602. [CrossRef]
13. Yang, L.; Li, M.; Si, P.; Yang, R.; Sun, E.; Zhang, Y. Energy-efficient resource allocation for blockchain-enabled industrial internet of things with deep reinforcement learning. *IEEE Internet Things J.* **2020**, *8*, 2318–2329. [CrossRef]
14. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet Things J.* **2020**, *8*, 2276–2288. [CrossRef]
15. Li, M.; Yu, F.R.; Si, P.; Wu, W.; Zhang, Y. Resource optimization for delay-tolerant data in blockchain-enabled IoT with edge computing: A deep reinforcement learning approach. *IEEE Internet Things J.* **2020**, *7*, 9399–9412. [CrossRef]
16. Jiang, X.; Yu, F.R.; Song, T.; Leung, V.C. Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing. *IEEE Internet Things J.* **2020**, *9*, 14260–14272. [CrossRef]
17. Feng, J.; Yu, F.R.; Pei, Q.; Du, J.; Zhu, L. Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4321–4334. [CrossRef]
18. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. [CrossRef]
19. Song, Y.; Fu, Y.; Yu, F.R.; Zhou, L. Blockchain-enabled Internet of Vehicles with cooperative positioning: A deep neural network approach. *IEEE Internet Things J.* **2020**, *7*, 3485–3498. [CrossRef]
20. Xu, Z.; Liang, W.; Li, K.-C.; Xu, J.; Jin, H. A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. *J. Parallel Distrib. Comput.* **2021**, *149*, 29–39. [CrossRef]
21. Herbadji, A.; Goumidi, H.; Harbi, Y.; Medani, K.; Aliouat, Z. Blockchain for Internet of Vehicles Security. In *Blockchain for Cybersecurity and Privacy*; CRC Press: Boca Raton, FL, USA, 2020; pp. 159–197.
22. Gao, L.; Wu, C.; Yoshinaga, T.; Chen, X.; Ji, Y. Multi-channel Blockchain Scheme for Internet of Vehicles. *IEEE Open J. Comput. Soc.* **2021**, *2*, 192–203. [CrossRef]
23. Chai, H.; Supeng, L.; Yijin, C.; Ke, Z. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3975–3986. [CrossRef]
24. Hammoud, A.; Hani, S.; Azzam, M.; Hadi, O.; Rabeb, M.; Jamal, B. AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions. *IEEE Internet Things Mag.* **2020**, *3*, 68–73. [CrossRef]
25. 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. *Multimed. Tools Appl.* **2022**, *81*, 23533–23549. [CrossRef]
26. Averin, A.; Samartsev, A.; Sachenko, N. Review of Methods for Ensuring Anonymity and De-Anonymization in Blockchain. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; pp. 82–87.
27. Bruschi, F.; Paulon, T.; Rana, V.; Sciuto, D. A privacy preserving identification protocol for smart contracts. In Proceedings of the 2021 IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 5–8 September 2021; pp. 1–6.
28. Meng, X.; Xu, J.; Liang, W.; Xu, Z.; Li, K.C. A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles. *Comput. Electr. Eng.* **2021**, *95*, 107431. [CrossRef]
29. Han, Q.; Yang, Y.; Ma, Z.; Li, J.; Shi, Y.; Zhang, J.; Yang, S. CMBIoV: Consensus Mechanism for Blockchain on Internet of Vehicles. In *International Conference on Blockchain and Trustworthy Systems*; Springer: Singapore, 2020; pp. 347–352.
30. Javed, M.U.; Rehman, M.; Javaid, N.; Aldegheishem, A.; Alrajeh, N.; Tahir, M. Blockchain-based secure data storage for distributed vehicular networks. *Appl. Sci.* **2020**, *10*, 2011. [CrossRef]

31. Bonadio, A.; Chiti, F.; Fantacci, R.; Vespri, V. An integrated framework for blockchain inspired fog communications and computing in internet of vehicles. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 755–762. [CrossRef]
32. Xiao, H.; Qiu, C.; Yang, Q.; Huang, H.; Wang, J.; Su, C. Deep Reinforcement Learning for Optimal Resource Allocation in Blockchain-based IoV Secure Systems. In Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 17–19 December 2020; pp. 137–144.
33. Khan, A.A.; Laghari, A.A.; Shafiq, M.; Cheikhrouhou, O.; Alhakami, W.; Hamam, H.; Shaikh, Z.A. Healthcare Ledger Management: A Blockchain and Machine Learning-Enabled Novel and Secure Architecture for Medical Industry. *Hum. Cent. Comput. Inf. Sci.* **2022**, *12*, 55.
34. Khan, A.A.; Asif, A.L.; Thippa, R.G.; Zaffar, A.S.; Abdul, R.J.; Mamoon, R.; Vania, V.E.; Alexey, M. 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]
35. Khan, A.A.; Asif, A.L.; Muhammad, S.; Shafique, A.A.; Zhaoquan, G. Vehicle to Everything (V2X) and Edge Computing: A Secure Lifecycle for UAV-Assisted Vehicle Network and Offloading with Blockchain. *Drones* **2022**, *6*, 377. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.