future internet

Review

Advances in Blockchain-Based Internet of Vehicles Application: Prospect for Machine Learning Integration

Emmanuel Ekene Okere * and Vipin Balyan

Department of Electrical, Electronics and Computer Engineering, Faculty of Engineering & the Built Environment, Cape Peninsula University of Technology, Bellville, Cape Town 7535, South Africa; balyanv@cput.ac.za
* Correspondence: okeree@cput.ac.za; Tel.: +27-743454760

Abstract: Blockchain-based technology has completely revolutionized the development of the Internet of Vehicles (IoV) framework. This has led to increasing blockchain-based Internet of Vehicles application over the last decade. However, challenges persist, including scalability, interoperability, and security issues. This paper first presents the state-of-the-art overview on IoV systems along with their applications. Then, we explore novel technologies, including blockchain-based IoV and machine learning-based IoV and highlight how the blockchain technology could be integrated with machine learning for intelligent transportation systems in the IoV ecosystem. This paper has shown the potential of machine learning integration in addressing the technical challenges in individual blockchain-based Internet of Vehicles applications.

Keywords: autonomous vehicles; deep learning; intelligent transportation systems; interoperability; vehicle data management

check for updates

Citation: Okere, E.E.; Balyan, V. Advances in Blockchain-Based Internet of Vehicles Application: Prospect for Machine Learning Integration. *Future Internet* **2024**, *16*, 449. https://doi.org/10.3390/fi16120449

Academic Editor: Paolo Bellavista

Received: 30 October 2024
Revised: 21 November 2024
Accepted: 25 November 2024
Published: 2 December 2024

1. Introduction

The need for smart transport systems is growing rapidly. The existing transport system is ladened with recurrent accident issues, coupled with a growing opportunity cost in regard to traffic congestion in industrialized and developed cities [1] and safety concerns by users. The VANET system was ushered in to address these concerns and was able to improve the performance of vehicular networks and overcome their inherent limitations. Growing demand and technological breakthroughs over the years have now challenged the VANET system and have ushered in the blockchain-based Internet of Vehicles (IoV) [2]. The exponential advancement in the development and deployment of intelligent and connected vehicles has further necessitated and deepened the demand for IoV systems [3,4]. The IoV is a branch of IoT that is dedicated to vehicular communication and interaction with the internet. IoV is a growing innovation and researchers project that the number of IoT devices in use will reach 75 billion by 2025 [5,6]. This surge in usage signals challenges such as resource management, security etc.

The blockchain is a powerful technology that acts as a distributed ledger, integrated to provide a solution to the challenges in the IoV [2,7–9]. One of the main benefits of integrating blockchain technology (BC) with the IoV is that they could contribute to improving the vehicular network environment by providing credit support for intelligent transport systems (ITS) [8]. BC adoption globally is incremental, and experts project that its market value would reach USD 39.7 billion by 2025 [10]. This is largely owing to its capabilities in providing features such as interoperability, security, confidentiality, authentication, and overall better performance in the IoV domain [8].

Machine learning offered the most promising strategies to detect unauthorized attacks or access in IoV-based enterprise information systems due to its better accuracy and precision [11]. Its learning capacity makes it adaptable to new forms of security bridge. ML is a subbranch of artificial intelligence (AI) [10,12] that empowers computers to think, study, and act without any human intervention [13]. ML seeks to mimic the human neuron system in its operation. It learns from input data through a set of neural networks within the architecture and makes decisions based on feedback process [10,13]. The adoption and application of ML algorithms are usually on a use basis, and they are specific to the required outcome for each application [12].

The combination of BC and ML promises cutting-edge opportunity in many technological domains [12,14–17]. The concept of technological convergence birthed the Industrial 4.0 [16]. Modern vehicles are now beyond mere thermo-mechanical machines; they are sophisticated hardware and software systems due to combination of IoV connectivity [6]. These have opened innovative business opportunities for manufacturers like Tesla, GM, Ford, and many others to design autonomous/self-driving cars with increased precision and accuracy [18,19]. Today, vehicles in the IoV system generate a tremendous amount of real-time data, which has given rise to concerns such as decentralization, interoperability issues, and scalability issues [16]. Furthermore, big data demands have increased the required data processing time for ML applications [20]. For efficient system operations, ML and blockchain technology could be integrated to improve operational performance [10,20,21]. For instance, blockchain can be adapted for a secure and decentralized platform, where data collection and sharing are screened for privacy and security, which then enables machine learning models to be deployed and executed in a decentralized and distributed manner [20,21]. These challenges can be addressed through the convergence of BC and ML technologies, thus enabling communication between vehicles, humans, sensors, and road infrastructure [16]. Therefore, we conduct a detailed survey, exploring the prospect of the convergence of ML, BC, and IoV in addressing the emerging technological challenges posed by intelligent transport system (ITS).

1.1. Motivation and Paper Contributions

Although quite a substantial number of studies have been reported relating to the applications of blockchain-based IoV [22,23], nevertheless, none of these studies have focused on integrating blockchain-based IoV with machine learning for intelligent transportation systems (ITSs). The review is aimed at addressing this gap and providing readers with a state-of-the-art review on the convergence of blockchain, machine learning, and the Internet of Vehicles.

1.2. Contributions

This review focuses on the advances in the IOV ecosystem and highlights the incorporation of blockchain as well as machine learning to provide a more secured and intelligent IoV application. The study seeks to identify the merits in the applications of this convergence and the solutions they proffer. Also, the technical challenges are discussed and the ways to overcome these challenges are highlighted. This study also incorporates some critical future research needs for successful deployment of these new converging technologies in the transportation system. The review seeks to address the research question “Can ML-assisted approach integrated with blockchain techniques, improve the overall system performance in an IoV system?”. Table 1 provides all summaries of abbreviations used.

Table 1. Summary of acronyms.

Acronyms	Definitions
AC	Average Correlation
ADASs	Advanced Driver-Assistance Systems
ANFIS	Adaptive Neuro-Fuzzy Inference System
ANN	Artificial Neural Network

Table 1. *Cont.*

Acronyms	Definitions
AI	Artificial Intelligence
AIS	Artificial Immune System
AV	Autonomous Vehicles
BC	Blockchain
Bi-LSTM	Bi-directional Long-Short Term Memory
BPFL	Blockchain-based Privacy-preserving Federated Learning
BPNN	Back Propagated Neutral Networks
BSM	Basic Safety Messages
CAVs	Connected and Autonomous Vehicles
CIoV	Cognitive Internet of Vehicles
C-LSTM	Centralized Long-Short Term Memory
CNN	Convolutional Neural Networks
CPABE	Cipher text Policy Attribute Based Encryption
CRT	Classification and Regression Tree
DAG	Directed Acyclic Graph
DDL	Distributed Deep Learning
DDoS	Distributed Denial of Service
DL	Deep Learning
DLT	Distributed Ledger Technology
DRL	Deep Reinforcement Learning
DSRC	Dedicated Short Range Communications
ECUs	Electronic Control Units
ELM	Extreme Learning Machine
EKM	Efficient Key Management
FL	Federated Learning
GA	Genetic Algorithm
IoT	Internet of Things
IoV	Internet of Vehicles
IPFS	Inter Planetary File System
ITS	Intelligent Transportation Systems
IVN	Intelligent Vehicular Network
k-NN	k-Nearest Neighbors
LSTM	Long Short-Term Memory
LTE	Long Term Evolution
MAPE	Mean Absolute Percentage Error
MEC	Mobile Edge Computing
ML	Machine Learning
MLP	Multi-Layer Perceptron
MVAEE	Multi-Vehicle Average Error Evaluation
NFC	Near Field Communications
NN	Neural Networks

Table 1. *Cont.*

Acronyms	Definitions
OBUs	On Board Units
PDR	Packet Delivery Rate
P2P	Peer-to-Peer
QR	Quick Response
RAN	Radio Access Network
R-CNN	Regions with Convolutional Neural Networks
RNN	Recurrent Neural Networks
RSU	Roadside Unit
SA	Simulated Annealing
SDN	Software Defined Networking
SV	Support Vector
SVM	Support Vector Machine
SVR	Support Vector Regression
TA	Trusted Authority
TCNN	Temporal Convolutional Neural Network
TPS	Transactions Per Seconds
UAV	Unmanned Aerial Vehicle
UL	Unsupervised Learning
VANET	Vehicular Adhoc Network
VCS	Vehicular Communication Systems
V2P	Vehicle-to-Pedestrian
V2I	Vehicle-to Infrastructure
V2R	Vehicle-to-Roadside Unit
V2S	Vehicle-to-Sensor
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to Infrastructure
WAVE	Wireless Access in Vehicular Environments
YOLO	You Only Look Once

1.3. Methodology

The content analysis method was used for this review study. Relevant studies were sourced from the different scientific databases. Some of the searched databases includes Google Scholar, Science Direct, IEEE Explore, SpringerLink, and Web of Science. The following word combination or phrases were used to search for articles for this study: "blockchain-based internet of vehicles", "Machine learning in internet of vehicles", "Blockchain-based intelligent transportation system", "Blockchain and ML convergence in IoV", "Blockchain in vehicular transportation", "Blockchain and deep learning integration in IoV", and "Blockchain based smart transportation system". This was done to narrow our search to only studies on the applications of blockchain or deep/machine learning in the IoV systems. The resulting articles after sorting were analyzed and used for this review. The materials used were grouped into three categories:

- Studies on blockchain applications for IoV
- Studies on ML applications for IoV
- Studies on the integration BC and ML for IoV

1.4. Related Surveys

Several surveys have been written that focused on blockchain-based IoV. We have summarized existing related reviews in Table 2. The following information is provided to compare this current review with existing related reviews. It includes authors' name, year of publication, title of review/survey, area of focus, discussions on IoV, discussions on blockchain-based IoV, discussions on ML-based IoV, and discussions on the integration of ML, BC, and IoV. We have compared these surveys with this current survey and shown how our review differs from the already-published surveys. It can be observed that a significant number of studies have been published in the IoV domain, and the number is still on the increase over the past decade due to the growing attention given to new and emerging technology globally. Though these survey studies have focused on the integration of specific technologies in isolation, BC integration in the IoV domain has been extensively reviewed [6,24–33]. These studies cover different aspects of the IoV system. ML, on the other hand, has received substantial review from researchers [1,34–36]. Despite these elaborate overviews on the breakthrough in these integrations, these studies did not consider the potential in their integration. Several studies have attempted to investigate the prospect of integrating these technologies for intelligent transportation [10,16,20,37,38]. However, many of these studies only partially discussed the convergence and its application [21,38,39], but did not focus mainly on the IoV domain. Dibaei et al. [37] and Zamanirafe et al. [20] have focused reviews on the IoV domain; however, no discussions on convergence were reported. From Table 2, we can see that no author has attempted to provide detailed discussions on the integration of blockchain and machine learning in an IoV system.

1.5. Paper Organization

The organization of the paper is as illustrated in Figure 1. After the introduction section, it continues with an overview of IoV (Section 2), It presents some preliminary information related to the IoV domain and its development, architecture, and transition from VANET and the challenges for intelligent transportation systems. Then, blockchain technology is presented in Section 3, where advances in blockchain-based IoV systems are discussed. Section 4 (ML-Based IoV) focusses on machine learning application and its integration prospects for machine learning-based IoV systems. Section 5 (Convergence of ML and Blockchain in IoV) briefly highlights the prospects of technological convergence, then further elucidates recent trends and approaches in the application of the convergence of blockchain and machine learning and IoV/VANETs for intelligent transportation systems. Section 6 (Discussion and Future Directions) discusses emerging trends and suggests some future research challenges after which the paper is finally concluded in Section 7 (Conclusions).

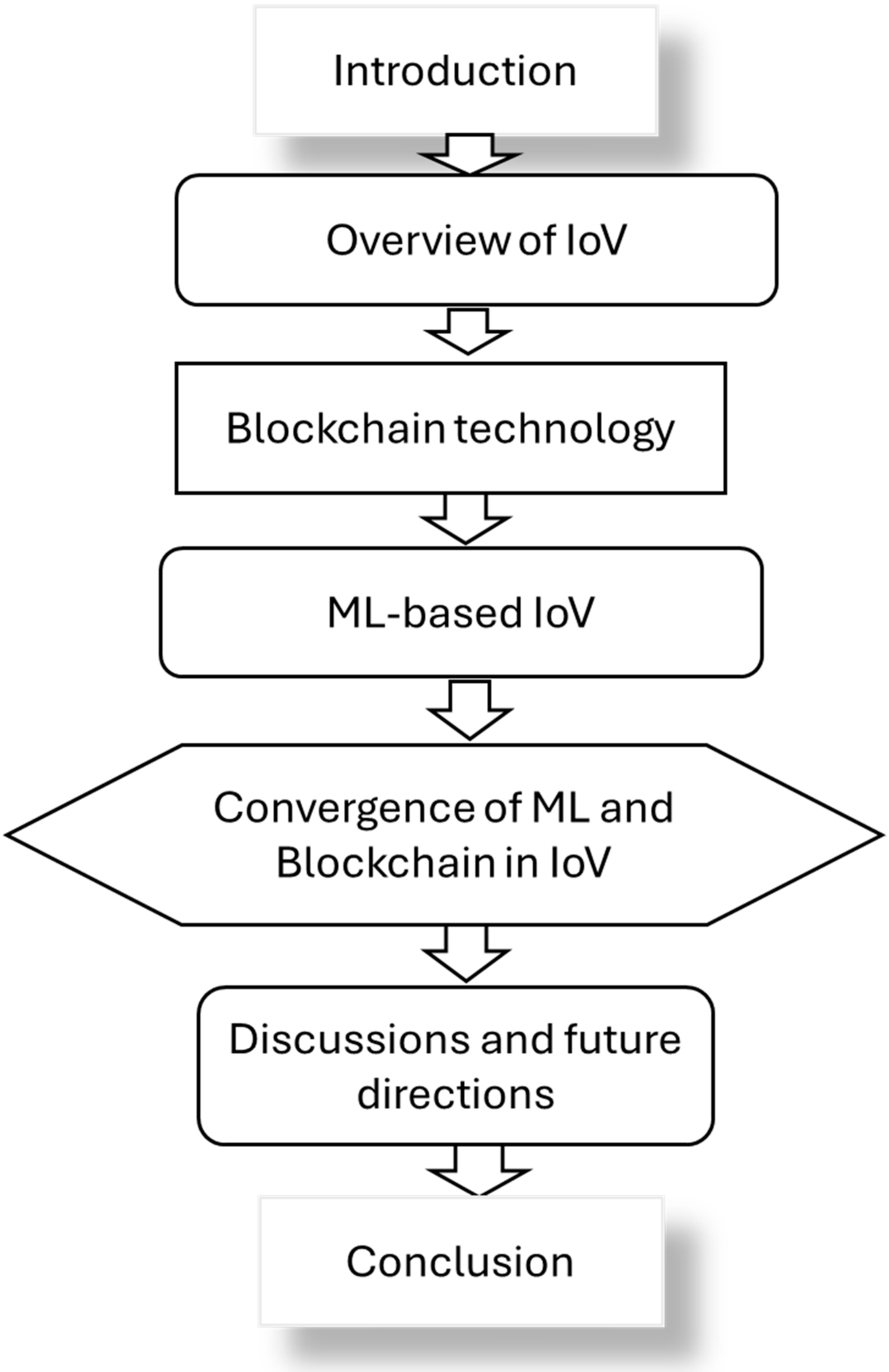

Figure 1. Review organization.

Table 2. Summary of related surveys and their area of focus as compared to ours.

References	Year	Title	Focal Area	Discusses IOV Overview	Discusses Blockchain-Based IOV	Discusses ML-Based IoV	Discusses ML Integrated with BC Based IoV	Dedicated to IoV
Abduljabbar et al. [1]	2019	Applications of Artificial Intelligence in Transport: An Overview	Addresses transportation problems mainly in traffic management, traffic safety, public transportation, and urban mobility.	No	No	Yes	No	Yes
Astarita et al. [40]	2019	Review of Blockchain-Based Systems in Transportation	Gives an overview of the application of blockchain-based systems in transportation.	No	Yes	No	No	Yes
Butt et al. [41]	2019	Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions	Identifies the challenges involved in managing privacy in SIoV	Partially	Yes	No	No	Yes
Mendiboure et al. [24]	2020	Survey on blockchain-based applications in internet of vehicles	Discusses blockchain-based applications in vehicular networks and the challenges related to the integration of the blockchain technology within vehicular networks	Partially	Yes	No	No	Yes
Ma et al. [34]	2020	Artificial Intelligence Applications in the Development of Autonomous Vehicles: A Survey	Focuses on the advancement of artificial intelligence (AI) and its deployment in autonomous vehicles (AVs) for the transportation industry	No	No	Yes	No	No
Mollah et al. [25]	2020	Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey	Highlighted the different application scenarios of blockchain-based IoV	Partially	Yes	No	No	Yes
Zhang et al. [17]	2020	Survey on Blockchain and Deep Learning	Discusses relevant studies on blockchain and deep learning on different domains including infrastructure, finance and trade, transportation and logistics, smart contract, and information security	No	No	No	Partially	No

Table 2. *Cont.*

References	Year	Title	Focal Area	Discusses IOV Overview	Discusses Blockchain-Based IOV	Discusses ML-Based IoV	Discusses ML Integrated with BC Based IoV	Dedicated to IoV
Karger et al. [26]	2021	Blockchain for Smart Mobility—Literature Review and Future Research Agenda	Focuses on blockchain's role in mobility and transportation in smart cities	Partially	Yes	No	No	Yes
Gangwani, & Gangwani [35]	2021	Applications of Machine Learning and Artificial Intelligence in Intelligent Transportation System: A Review	Reviewed various ML approaches for road anomalies detection and real-time traffic flow prediction in smart transportation system	No	No	Yes	No	Yes
Abbas et al. [27]	2021	Blockchain-Based Authentication in Internet of Vehicles: A Survey	Recent blockchain-based authentication schemes in IoV and VANETs	Yes	Yes	No	No	Yes
Kumar et al. [28]	2021	A survey on the blockchain techniques for the Internet of vehicles security	Blockchain techniques to secure IoV	No	Yes	No	No	Yes
Iyer [36]	2021	AI enabled applications towards intelligent transportation	Review focusses on discussions of AI solutions to technical issues in transport industry	No	No	Yes	No	Yes
Wang et al. [2]	2021	A survey: applications of blockchain in the Internet of Vehicles	Focusses on blockchain implementation in the IoV system	Partially	Yes	No	No	Yes
Sargolzaei et al. [29]	2021	Blockchain Applications to Improve Operation and Security of Transportation Systems: A Survey	Focusses on potential applications of blockchain in the future of transportation systems to be integrated with connected and autonomous vehicles (CAVs)	No	Yes	No	No	Yes
Mikavica et al. [30]	2021	Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey	Provides a survey on blockchain-based solutions for security services in vehicular networks	Yes	Yes	No	No	Yes

Table 2. *Cont.*

References	Year	Title	Focal Area	Discusses IOV Overview	Discusses Blockchain-Based IOV	Discusses ML-Based IoV	Discusses ML Integrated with BC Based IoV	Dedicated to IoV
Dibaei et al. [37]	2022	Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey	Focuses primarily on securing communication technologies in IoV, including using ML and blockchain defense mechanisms	Yes	Yes	Yes	No	Yes
Singh et al. [10]	2022	Blockchain and AI technology convergence: Applications in transportation systems	Investigates both technologies and their convergence in various domains of industry with a specific emphasis on transportation systems.	No	Yes	Yes	Partially	No
Saad et al. [31]	2022	Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review	Provides a comprehensive overview of blockchain applications for the Internet of Vehicles (IoV), with focus on advancements of blockchain and VANETs	No	Yes	No	No	No
Alladi et al. [6]	2022	A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks	Focuses on blockchain platforms, blockchain types, and consensus mechanisms used in blockchain implementation	Yes	Yes	No	No	Yes
Jabbar et al. [42]	2022	Blockchain Technology for Intelligent Transportation Systems: A systematic Literature Review	Reviewed blockchain technology opportunities, relative taxonomies, and applications in intelligent transport system	Yes	Yes	Yes	Partially	No
Grover et al. [33]	2022	Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review	Focus is on applications of blockchain in VANET security	Yes	Yes	No	No	Yes
Javed et al. [38]	2022	Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey	Focused on FL and blockchain applications in the Vehicular Ad Hoc Network (VANET) environment	No	No	No	Partially	No

Table 2. *Cont.*

References	Year	Title	Focal Area	Discusses IOV Overview	Discusses Blockchain-Based IOV	Discusses ML-Based IoV	Discusses ML Integrated with BC Based IoV	Dedicated to IoV
Zamanirafe et al. [20]	2023	Blockchain and machine learning in internet of vehicles: Applications, challenges, and opportunities	Provides an overview of IoV, block-chain, and ML	Partially	Yes	Yes	No	Yes
Yazici et al. [43]	2023	A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems	Focused on ML and AI applications for different use cases enabled by future mobile communication system	No	No	Yes	No	No
Hildebrand et al. [8]	2023	A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions	Focused on blockchain-based IoV applications such as crowdsourcing-based applications, energy trading, traffic congestion reduction, collision, accident avoidance, infotainment, and content caching	Yes	Yes	No	Partially	Yes
Fazel et al. [16]	2024	IoT Convergence with Machine Learning & Blockchain: A Review	Address the technical challenges of IoT, including architecture, hardware, privacy and security, scalability, interoperability, and heterogeneity issues	No	Partially	No	No	No
Ressi et al. [9]	2024	AI-enhanced blockchain technology: A review of advancements and opportunities	Overview of the methods that have been employed to improve blockchain technology	Partially	Partially	No	No	No
Sameera et al. [39]	2024	Privacy-preserving in Blockchain-based Federated Learning systems	Summarizes FL and blockchain and their integration for private security in different domains	No	No	Yes	Partially	No

Table 2. *Cont.*

References	Year	Title	Focal Area	Discusses IOV Overview	Discusses Blockchain-Based IOV	Discusses ML-Based IoV	Discusses ML Integrated with BC Based IoV	Dedicated to IoV
Alkashto and Elewi [21]	2024	Integration of blockchain and machine learning for safe and efficient autonomous car systems: A survey	Focused on the integration of blockchain with machine learning for autonomous cars and vehicles	Yes	Yes	Yes	Partially	No
This survey	-	-	Focusses on the integration of blockchain, machine learning, and IoV system for intelligent transportation system	Yes	Yes	Yes	Yes	Yes

2. Overview of IoV

Simply put, IoV is a form of IoT that is dedicated to vehicles solely. While IoV itself is a vehicular ad hoc network (VANET) that has now been advanced and linked to the Internet [8,44], IoV can be defined as an integrated network platform that enable vehicles and its environment to interact and exchange information towards an intelligent transportation system by means of a dedicated communication media. The need to transit into an intelligent transportation system (ITS) demanded that VANET infrastructures be upgraded to accommodate for the increasing vehicles added to the network [45–47]. Figure 2 illustrates how a typical IoV system is made up and how vehicles communicate in the network. In an IoV system, vehicles communicate with other vehicles by means of vehicle-to-vehicle (V2V) communication, and with RSUs aided by vehicle-to-RSU (V2R) communication [8,20]. The IoV system enables real-time information sharing relating to traffic or road condition; safety warnings can be relayed, and a better traffic management is achieved [44]. Other supporting applications that have emanated from IoV include autonomous driving, infotainment, smart payment services, and vehicle forensic investigations purposes [8,27,48]. It is projected that there will be over 2 billion vehicles in the network by 2035 [45]. The main goal of IoV is to lower the rate of accidents occurrence, drastically reduce traffic congestion, and provide secure and smart information exchange services [49,50].

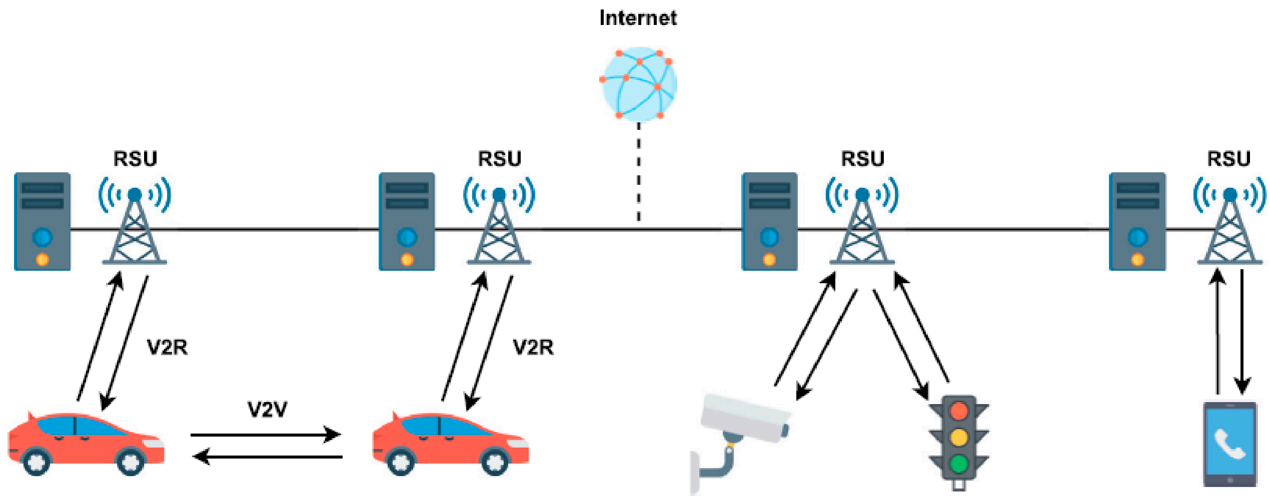

Figure 2. Typical infrastructure of IoV network. Adapted from [8].

The first step in formation of IoV is by integrating vehicles into wireless networks. Some of the existing wireless access technologies includes WLANs, WiMAX, Cellular Wireless, and satellite communications [46,47,51]. Vehicular communications in IoV are broadly divided into two main channels: intra-vehicle communication and inter-vehicle communication [44]. Intra-vehicle communication takes place within the vehicle. It is often referred to as vehicle-to-sensor communication (V2S) [44]. It is the interaction between the vehicle and the electronic control units (ECUs) inside the vehicle. The network protocols that facilitate intra-vehicle communication include CAN Bus, Local Interconnect Network (LIN), and Flex Ray communication networks [44]. Inter-vehicle communication, on the other hand, involves the interaction between the vehicles and other road entities connected in the IoV system [44,52]. Vehicular communications that fall under the inter-vehicle communication include vehicle-to-vehicle (V2V), vehicle-to-roadside-unit (V2R), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), vehicle-to-sensor (V2S), and vehicle-to-grid (V2G) [44]. The Dedicated Short-Range Communication (DSRC), the Long-Term Evolution Vehicular Network (LTE-V), and the 5th Generation mobile networks (5G) are among the network protocols dedicated to inter-vehicle communications [44,53,54].

2.1. VANETs to IoV Transition

Vehicular Ad hoc Networks (VANETs) consist of self-organized sets of vehicles in a mobile network [33]. VANET is a core component of an intelligent transportation system [33]. It was introduced to enhance vehicular communication using Dedicated Short-Range Communication (DSRC) for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [33,51]. This communication allows users to make timely, safe, and efficient smart decisions with regards to road safety, traffic flow, and overall improved travel experience. In the VANET system, vehicles are considered as a mobile node that connects to other vehicles to create a network [33,49]. During operations, vehicles are connected when they fall within the coverage and are disconnected as they fall outside of the coverage range [33,49]. These constraints, coupled with other shortfalls such as the increasing number of vehicles connected to the network, and several factors such as traffic jams, tall buildings, and poor driver behaviors, ultimately affect its performance and use [49]. Also, the VANETs' framework failed to support the global interconnectedness required of the smart vehicular system [27], thereby necessitating the transition of the VANET into IoV system [27,51].

The IoV system leverages on technological advancements such as ubiquitous connectivity, 5G and 6G wireless technologies, sensor devices, smart vehicles, and cloud computing to provide a more powerful vehicular network [27,37]. In IoV, vehicles are constantly connected to the internet, to form a network of vehicles to facilitate the provision of several smart vehicular services [45]. It is made of majorly three basic parts: (1) the intra-vehicular network, (2) the inter-vehicular network, and (3) the vehicular mobile Internet [27]. The intra-vehicular network is the communication of vehicles within the same network; inter-vehicular network enables communication between vehicles of different networks while vehicular mobile network is the connection that links vehicles and mobiles devices in the network. Vehicles in the IoV system are usually equipped with smart functionalities and devices that enable communication and data collection. Some of these devices include On Board Units (OBUs), sensors, event data records, cameras, electronic control units, GPS modules, and other wireless communication technologies (i.e., Bluetooth). The IoV system ensures that diverse communication dynamics (vehicle-to-vehicle (V2V), vehicle-to-roadside unit (V2R), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-sensor (V2S), are achieved [27,37]. Table 3 summarizes the different communication dynamics in the IoV system. Although IoV is often confused to mean something that can be used interchangeably with ITS, it differs in the sense that IoV focusses on information exchange among humans, vehicles, and the road infrastructures in place [45]. A detailed review on the different communication networks is highlighted by [37].

Table 3. Summary of the different communication dynamics of an IoV system.

Interaction	Description	Function	Communication Protocol
V2V	Vehicle-to-Vehicle	Supports the wireless communication across vehicles for sharing location data, and it consists of the speeds, coordinates, road condition, and traffic information	WAVE
V2R	Vehicle-to-Roadside Unit	Supports the wireless interaction between vehicle and RSUs	WAVE
V2I	Vehicle-to-Infrastructure	Supports the wireless interaction between vehicles and the supporting infrastructure (base stations, grid, networks, devices, etc.)	Wi-Fi, LTE, 5G, or 6G
V2H	Vehicle-to-Human	Supports mobility and awareness for the nearest users, such as pedestrians, cyclists, and drivers	NFC
V2S	Vehicle-to-Sensor	Support the bi-directional communication between different kinds of sensors and onboard terminals for real-time insights	Ethernet and Wi-Fi,

2.2. Architectural Framework for IoV

Different layered architectures for IoV frameworks have been proposed in the literature [27,45,51,55], which differ in their design and framework for optimum functionality. Achieving an optimized number of layers and enhancing the differentiability among layers are the keys towards efficient IoV framework [27]. Among the vital considerations for an IoV framework are a strong integration with the internet, a service-based focus, and a plug-and-play based interface [27,45,51,55]. Some of the major components in an IoV architectural framework include the perception layer, the coordination layer, the artificial intelligence (AI) layer, the application layer, and business, security, processing, service, and physical layers [27,51]. Abbas et al. [27] reports that the six-layer architecture is the most common design for IoV implementation. The components considered in the framework include the physical, communication, processing, services, business, and security layers. Figure 3 vividly depicts the six-layer architectural design of the IoV system.

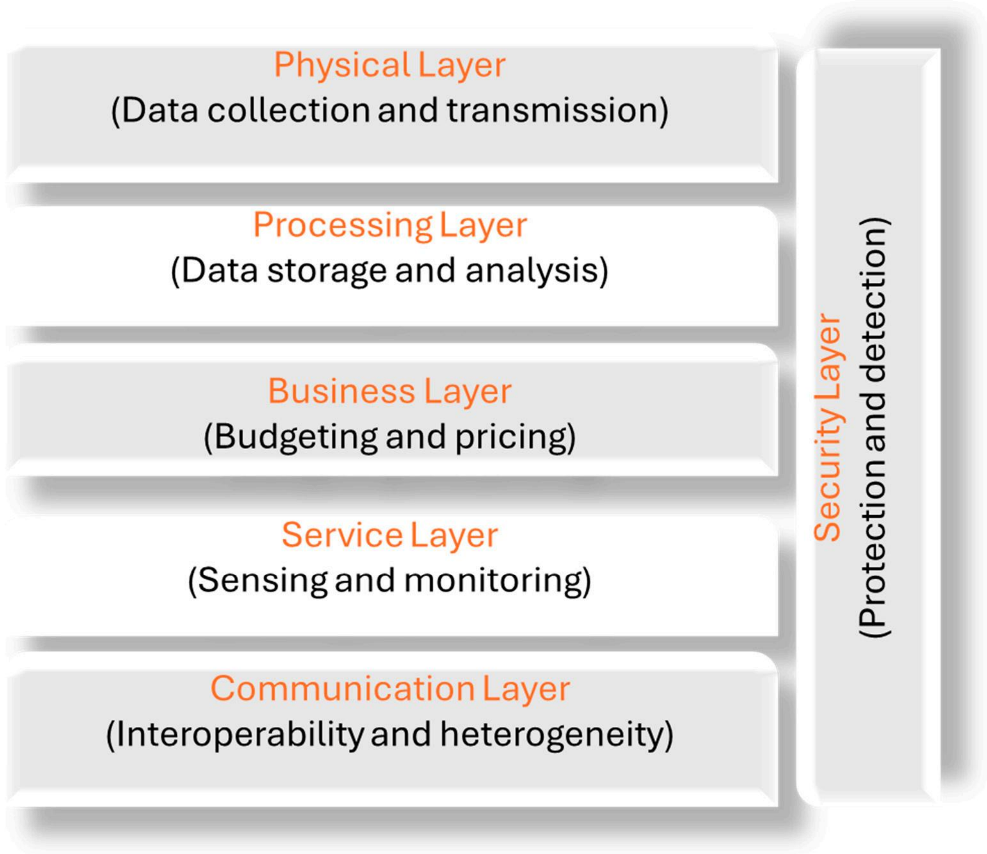

Figure 3. Six layered architectural frameworks of an IoV system.

2.3. Challenges in the IoV System

2.3.1. Authentication-Related Issues

A secure IoV network must be one that can authenticate the exchanged messages inside the network [8,27]. It must not be venerable to attacks [8]. Through authentication, the correct identity of both the sending and receiving nodes in the network are secured [27,28]. Some of the common attacks an IoV network is often susceptible to include sybil attacks, masquerading attacks, impersonation attacks, spoofing attacks, replay attacks, and wormhole attacks [27,28,48].

2.3.2. Privacy-Related Issues

Information exchanged in an IoV system can be personal, private, and sometimes confidential. Such data should not be leaked or accessed by unauthorized vehicles or participants in the network [27].

2.3.3. Integrity- or Trust-Related Issues

From an integrity perspective, the malicious nodes modify the routing information to misguide the genuine vehicles in the network. By integrity, we mean that data that have been transmitted from the source node are not modified when they are received at the sink node. In such types of attacks, the attacker somehow enters the IoV system and accesses the packets that are being sent in the IoV network, modifies them, and sends them to the sink node. Trust management is another crucial aspect that significantly impacts the utilization of IoV system. With the distributed nature of its architecture coupled with high volume of messages exchanged, the reliability of the system is often compromised [56].

2.3.4. Incentive-Related Issues

As the IoV system is improved, new technologies are integrated into the vehicular communication, aiming to provide more efficient functionality and adaptability to the technical challenges in the system [24]. Some of these technologies include SDN, NFV, mobile edge computing (MEC), AI, etc. These additional technologies bring about concerns around cooperation between vehicles, impeding the accessibility of data between vehicles for efficient data transmission and sharing. The need for an efficient incentive mechanism to encourage participating vehicles in the network to cooperate and initiate data transmission and sharing has now ensued.

2.3.5. Security-Related Issues

The IoV system is ladened with numerous security vulnerabilities; this is owing to its heterogeneous nature and in combination with the ever-increasing number to vehicles joining the network [45]. The traditional IoV was developed based on PKI technology [50]; this approach results in huge communication costs [50]. In this system, authentication nodes are centralized. These nodes have overworked, as they cannot be proxied, thereby making it easily compromised [27,50]. Aside from authentication concerns, other security requirements of a typical IoV system include data integrity, data confidentiality, access control, data nonrepudiation's, availability, and anti-jamming requirements [45]. Addressing the security and other concerns on IoV is critical as the threats are real. Any security breaches or mishap could compromise the entire system. This has forced researchers into finding different ways in tackling these problems. One such approach is incorporating the blockchain technology into the IoV system. The proposed blockchain technology boast promising features that should ensure authentication, data exchange and trading, transparency, and confidentiality to be guaranteed [56,57]. Participating nodes in the network can now utilize blockchain's decentralized, tamper-proof, secure, and traceable characteristics, to promote the overall system sustainability [57].

3. Blockchain Technology

Blockchain is a recent technology that is currently finding applications in different fields [6,58,59]. Blockchain is characterized by three unique attributes: decentralization, immutability, and distribution [8,20,27]. Other characteristics of BC include anonymity, autonomy, transparency, etc. [10]. The blockchain promises to adequately ensure data security and privacy for the IoV system [8,60]. It is defined as a group of connected blocks used to store large data and is maintained by all the participating users distributed over the network. BC eliminates the need of a central authority, by allowing all users in the network to generate and validate transactions directly in a peer-to-peer network [10,27]. The blocks in a blockchain are the simplest unit of a blockchain that keeps records of public transactions that are performed, authenticated, and then stored. The recorded transaction cannot be altered without the consent of the other participants [10]. Other components of the blockchain technology are cryptographic hash functions, asymmetric cryptography, transactions, and the ledgers [10]. Some of the core functionalities of a network peer in a blockchain system includes routing, storage, wallet, and mining [61].

The current blockchain technology was first popularized by Nakamoto [62]; though originally intended for cash systems behind Bitcoin or cryptocurrency, the blockchain technology has now found application in many domains, covering health, aviation, defense, and even transport. BC is based on distributed ledger technology, owing to it being hosted on many databases globally [63]. Earlier BC stored currency transactions of the parties involved on distributed computers that share a similar database. These computers are called nodes in a blockchain network [63]. BC stores information in a block-like structure that builds up in a linear chain as blocks are added to the network starting from the founding block [58,63]. BC technology eliminates the need for a central authority, as it enables participants in the network to generate and validate transactions directly in a peer-to-peer network that helps significantly lower the overall running cost and financial and time related costs associated with the intermediate party.

3.1. Building Blocks of a Blockchain

In a BC, records of network participants are hosted in blocks of a fixed size [64]. As blocks are added, every block provides a timestamp, and a hash of the previous block [64]. These continue and result in chains of blocks [64]. The reward could be paid by stakeholders in the system, which could find some agreement to split the running costs of the blockchain. The costs of running a blockchain can be extremely high, as shown in the next section. For this reason, the paying scheme of blockchain systems that has revealed that the greater success is the creation of new cryptocurrencies (digital currencies) [64]. Typically, a consensus process is performed before newly built blocks are added to the blockchain [57]. The efficiency of BC is achieved by two main approaches; one way is to increase the block size of the BC, while the other method is increasing the number of effective neighbors that each node can connect with [65].

3.2. Types of Blockchain

Typically, blockchains are categorized based on three different categories: based on data accessibility, based on mode of authentication, and based on core functionality [10,66]. Figure 4 summarizes the different types of blockchain depending on the three different categories.

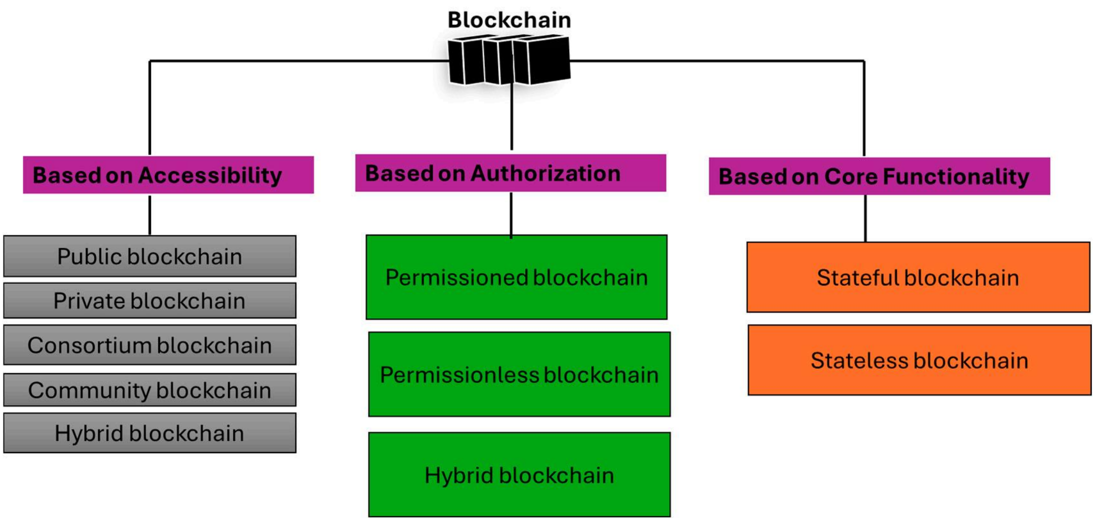

Figure 4. Classification of the different types of blockchain.

Based on Data Accessibility

Four types of blockchain exist under this category. They include public blockchain, private blockchain, consortium blockchain, and hybrid blockchain [10]. Public blockchains are like open-source platforms without user restrictions. Endless number of participants can submit and make transaction in the network [10,67]. They are usually permissionless during authentication, meaning clients can download the blockchain code into their own frameworks, change it, and use it as indicated by their own prerequisites [14,67]. Its decentralization and transparency while maintaining anonymousness makes it very desirable, though it can take longer to achieve exchange endorsement during transactions when compared to consortium and private blockchains [67]. Examples of a public BC includes Bitcoin, Ethereum, and Litecoin [27].

Unlike the public blockchain, the private blockchains are relatively quicker (usually less than 1 min), because of the known and limited participants in the blockchain. In this system, only the authorized group, whose participation has been validated, can access and submit transactions. Hence, it often requires less time to approve transactions. It operates under a permissioned framework, meaning that clients are authenticated and granted access before participation [10,67]. Private BCs are best suited for semi-closed systems like the banking sector and selected government agencies [27].

The consortium blockchains combine a group of participants and grant them access to submit and trade on the blockchain. The groups involved in consortium blockchain typically share common interest and work under a permissioned framework, although not all participants can access and submit transactions as in private blockchain. Its exchange endorsement time is somewhat quicker compared to the public blockchain [14,67]. Consortium BCs are seen in Stellar, R3CEV, Hyperledger, and Ripple blockchain [27]. The hybrid blockchain allows different blockchain types to be combined to achieve fast transactions in a blockchain [10,66].

3.3. Consensus Algorithms

Consensus algorithms play an important role in deciding how the nodes in a blockchain participate inside the blockchain network [8,9,67]. These algorithms ensure that there is no presence of faulty nodes in the network [67,68]. They bring about stability and trust in the overall blockchain by enhancing agreements between nodes inside the network [27,68,69] and are defined as the agreement on a common value among participating nodes in a blockchain system. Some of the most-used consensus protocols incude Proof of Work (PoW), Proof of Stake (PoS), Proof of Credit (PoC), Alternative to PoW (AltPoW), Proof of Authentication (PoAh), Proof of Elapsed Time (PoET), Proof of Space, Byzantine Fault Tolerance (BFT), Proof of Activity (PoAc), Practical Byzantine Fault Tolerance (PBFT), etc. [8,14,33,42]. Table 4 gives a summary of the different consensus algorithms and their applications in different blockchain scenarios.

Table 4. Some of the most common consensus algorithms and their application.

Consensus Algorithm	Abbreviation
Alternative to PoW	AltPoW
Byzantine Fault Tolerance	BFT
Byzantine Fault Tolerant Delegated Proof of Stake	BFT-DPoS
Delegated Proof of Stake	DPoS
Delegated BFT	dBFT
enhanced PoW	ePoW
Federated Byzantine Agreement	FBA
Leased Proof of Stack	LPoS

Table 4. *Cont.*

Consensus Algorithm	Abbreviation
Practical Byzantine Fault Tolerance	PBFT
Proof of Activity	PoAc
Proof of Acyclic Graph	PoAG
Proof of Authentication	PoAh
Proof of Authority	PoA
Proof of Burn	PoB
Proof of Capacity	PoC
Proof of Coin Age	PoCA
Proof of Credit	PoC
Proof of Deep Learning with Hyperparameter Optimization	PoDLwHO
Proof of Deposit	PoDe
Proof of Driving	PoD
Proof of Elapsed Time	PoET
Proof of Event	PoE
Proof of Importance	PoI
Proof of Knowledge	PoK
Proof of Learning	PoL
Proof of Lock	PoL
Proof of Work	PoW
Proof of Stake	PoSt
Proof-of-Stake Deposit	PoSD
Proof of Time	PoT
Proof of Useful Work	PoUW
Proof of Utility	PoU
Proof of Vote	PoV
Proof of X	PoX
Reliable Replicated Redundant and Fault Tolerant	RAFT
Redundant BFT	RBFT
Ripple	R

3.4. Smart Contract

A smart contract is a type of BC that act as predefined program that facilitates automatic transaction in a trading system [14,70]. As a computer code, its conditions are defined, and once met, it automatically executes the function defined in the contract or transaction. Smart contracts enable blockchain's ability to govern interactions among participants independent of a trusted third party [14].

3.5. Blockchain-Based Internet of Vehicles (BIoV)

Due to the inherent limitations of the IoV system to manage security and transparency, IoV platforms are now starting to adopt blockchain for various services. Merging BC with IoV offers solutions such as transparency, immutability, and high efficiency [8,21]. These properties of BC provide security, preserves privacy, and guarantee confidentiality of the IoV system [8,52]. Some of the areas where blockchain have found application in IoV platforms include data protection and management, data and resource trading; resource sharing, vehicle management, ride sharing, traffic control, and forensics applications [25,27]. Integrating BC and IoV promises to address the challenges posed by the decentralized and heterogeneous nature of IoV [16,21]. BC helps to validate the trustworthiness of transactions by means of consensus algorithms [16]. It acts as a distributed decentralized database by using properties such as digital signatures, cryptographic techniques, hash function, Merkle tree root, and timestamps [52].

In a BC based IoV, blockchain data can be classified into five categories: vehicle driving data monitored by the RSU, where dynamics monitored could include driver behavior, speeding, etc.; (2) vehicle sensory data obtained from the internal machinery, where dynamics could include electronics, air pressure, temperature, etc.; (3) D3 or vehicle user-generated data, which could include voice audio recording or video recordings inside the car; (4) vehicle insurance-related data; and (5) vehicle transactional data for users, such as car refueling, parking, charging, car washing, etc. [71]. Most research on BC-based IoV has been for authentication [27], although, other application areas have been identified.

3.6. Applications of Blockchain-Based IoV for Intelligent Transportation System

Though the adoption of BC for IoV-based application is still recent [10], its application for transport management is gaining rapid attention. The application of BC in the transport domain has been extensively reviewed by researchers [10,40,63]. In the aviation domain, BC-based solutions have been deployed for operations and information management [72–74], to improve trust [75]. There are considerations that have been made for its adoption [76,77], though, others consider it is too early and that it still needs extensive research [10,78]. Another transportation domain where BC is gaining attention is the railway transport domain [10,79], where is has provided solutions for the efficient management of the railway system [80,81], as well as in the maritime transportation domain [82].

BC-based IoV approaches have been investigated for different IoV applications [8,27]. Some of the major application areas include vehicle management [83], vehicle platooning [84,85], forensic investigations [86,87], traffic control [88,89], resource trading and sharing [83,90], data management [91], ride sharing [92–94], intelligent parking [95], and infotainment [96]. Table 5 gives a summary of the different BIoV applications together with the type of BC used the performance metric used to evaluate the proposed blockchain integration as well as the key findings.

Table 5. Summary of applications of blockchain-based IoV.

References	Application	BC Type	Performance Metric	Solution Provided
[83]	Resource sharing	Consortium blockchain	Propagation delay, block processing time, consensus delay, computation cost, storage cost, and communication cost	Increased consensus delay and throughput over the same level of security
[97]	Resource sharing	Public blockchain	Hash value verification after encryption	Developed model was able to protect video privacy, and the encrypted video is made public in Ethereum
[98]	Resource sharing	Proof of Reputation (PoR)	Reputation value	Proposed model achieved over 30% increase in the pricing scheme compared to the unified pricing schemes
[99]	Resource trading	Consortium blockchain	Communication cost, computation time	Achieved lightweight BC and lead to communication and computation overheads on the network resources
[100]	Resource sharing	Byzantine Faults Tolerate Algorithm (BFT)	Computation time	The proposed CreditCoin maintained the reliability of announcements without revealing users' privacy
[101]	Data management	Hyperledger Fabric	Throughput, latency, and transaction success ratio	Developed model significantly improved the performance of the blockchain system in terms of the throughput, latency, and transaction success ratio
[102]	Traffic control	Joint Proof-of-Work (PoW) and Proof-of-Stake (PoS)	Ratings and trust value offsets, generation time intervals of blocks, and the communication overheads of this system	Achieved a reliable decentralized trust management system capable of evaluating the credibility of neighboring nodes and ensure safe and efficient transportation system
[88]		Proof of work	Time consumption	The proposed STCTSC model achieved the protection of messages and users' identities
[89]		PBFT algorithm	Transaction cost	The proposed model achieved data transmission and traffic condition dissemination between vehicles
[103]		Hyperledger Fabric	Latency, throughput	Proposed approach was effective for real-time traffic management while preserving the data privacy requirements
[95]	Smart parking	Raft consensus algorithm	Storage cost overhead	The proposed model was able to ensure security, transparency, and availability of a smart parking system using blockchain.
[96]	Infotainment	Proof-of-Stake at Deposit (PoSD)	Total transaction times, average round trip time (RTT)	The proposed autoCoin enabled two vehicles to exchange a 50 MB file and tokens within about a minute

Table 5. *Cont.*

References	Application	BC Type	Performance Metric	Solution Provided
[85]	Vehicle platooning	Proof-of-Work	Certificate time, joining speed per number of blocks	Proposed model was able to verify the integrity of vehicles in a platoon without the assistance of a third party or RSUs
[104]		Ethereum	Financial cost, time consumption	The proposed BAVPM scheme ensured vehicles could join and leave the platoon at any time and at a low cost
[84]		Smart contract	Number of matching vehicles, actual final reputation value, percentage of fuel savings, average service charge, and total revenue of PH	The proposed model was superior in terms of fuel consumption

3.7. Challenges in Blockchain-Based IoV

Blockchain-based IoV architectures are predisposed to challenges such as security, trust and privacy concerns, performance issues, consensus algorithm optimization problems, and a selection of appropriate incentive mechanisms [8,10,25]. Another challenge faced by BC-based IoV systems is storage and scalability concerns [10,27,61]. Due to the voluminous amount of data generated in IoV systems, there is usually not enough storage capacity to accommodate these data [10]. Choosing the appropriate consensus mechanism can be one effective way of handling the scalability issues [27]. Proof-based consensus mechanisms do not suffer scalability concerns as individual components in the network do not require validation. Other issues with regards to appropriate choice of consensus mechanisms include fault tolerance level, mode of communication, and energy consumption requirements [27].

The use of BC introduces concerns relating to encryptions that limit access to data [10]. Private BC only permits few authorized participants into the network, and this limits access to data. The use of public BC is limited, and often discouraged by researchers [8]. This is due to its open nature, which ultimately impacts the privacy and security concerns of the IoV system. Recent efforts ae now considering lightweight encryption schemes to lower the communication overhead [8,99].

Choice of Blockchain Architecture

The appropriate choice of the blockchain platform for a particular application could critically impact the performance of the system [105]. For multi-layered architectures, testing utilizes several platforms that provide dedicated features to enhance adaptability. Some of the well-used blockchain platforms include Hyperledger, IOTA Tangle, Ethereum blockchain, etc.

Researchers are projecting that ML or AI would be an efficient solution to the many BC-based IoV challenges [25], assisting, particularly, with the huge amount of generated data in the IoV system.

4. Machine Learning (ML)-Based Internet of Vehicles

The use of ML has infiltrated every aspect of the human sphere. ML is a branch of artificial intelligence that particularly focuses on the collections of learning algorithms that enable the learning of a task [9,20]. ML gradually learns from data fed into it, like how humans learn, without inherently being programmed [9,106]. IoV systems can be configured to be more efficient by applying ML techniques [20]. Examples of ML techniques that have been applied in IoV systems include support vector machine (SVM), decision trees (DT), recurrent neural networks (RNN), and convolutional neural networks (CNNs) [20,21].

4.1. Neural Networks (NN)

NN are a sub-type of ML that adopts the human brain functionality dynamics to learn and predict outcome from input data [9]. ML approach was popularized by the NN after it was first proposed in 2012 [9,107]. NN are composed of neurons or nodes interconnected in layers that perform data processing and yield outcome after learning from input data [9]. The feedforward neural network is the simplest NN; it is composed of a single input layer, one or more hidden layers, and a single output layer [9]. They are configured to accept different types of inputs data and train the data to return an output as close as possible to the desired one [9,107]. Deep neural networks (DNNs) are the more complex NN, owing to an increasing number of hidden neurons in the layers [9]. DNNs are capable of learning from complex data and contain large number of neurons in the layers. The r hyperparameters that control the learning process of a DNN model include activation functions, the learning rate, the decay, the number of epochs, the type, and the sequence of layers arrangement [9].

The ANN was the first NN that was proposed, Consequently, numerous other architectures have been developed [9]. Some of the more popular NNs deployed for different

ML applications include convolutional neural networks (CNNs), recurrent neural networks (RNNs), etc. ANNs are nonlinear models; they are also non-parametric and are employed to determine the approximate functioning of a system for a real-life application [107].

4.2. Types of Machine Learning Techniques

Depending on the desired task, ML can be grouped under three categories: supervised learning, unsupervised learning, and reinforcement learning [9,20,43].

4.2.1. Supervised Machine Learning Technique

ML models that fall under the supervised learning type include random forest (RF), k-nearest neighbor (k-NN), linear/logistic regression, support vector machine (SVM), naïve bayes (NB), and many other NN techniques [9,20]. These classes of ML work with a pre-labeled numerical dataset [15,20,108]. The outcomes of supervised ML are often determined with mapping functions that relate it to its input data features [20]. SL is the most frequently used ML approach [43].

4.2.2. Unsupervised Machine Learning Technique

In this type of ML, the analysis does not rely on pre-labeled datasets but instead analyzes the similarity and dissimilarity between data points to develop a logical pattern. A data mining approach is favored in this type of ML [20]. Unsupervised learning requires only the input data to give an output [64].

4.2.3. Reinforcement Machine Learning Technique

This type of machine learning is based on the interaction between the input and the output decision through trial and error [9,109,110]. Training in reinforcement learning requires a large amount of data, and this makes it computationally demanding [21,64]. In RL, data is being collected from the environment, and the model learns from the collected data and improves on its decision making. Typical application areas of RL in ML-based IoV include routing, network resource management, content caching, and edge task offloading [20]. A detailed breakdown of ML techniques classification is summarized in Figure 5.

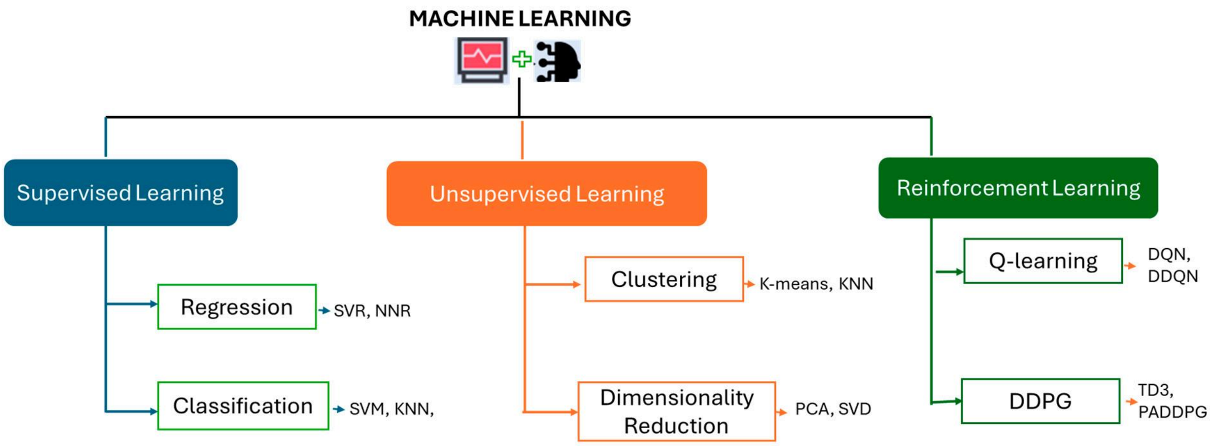

Figure 5. Breakdown of the classification of the different ML approaches.

Figure 6 highlights a typical architecture of a machine learning framework for a neural network implemented for traffic state predictions. It consists of the input layer, hidden layers, and an output layer.

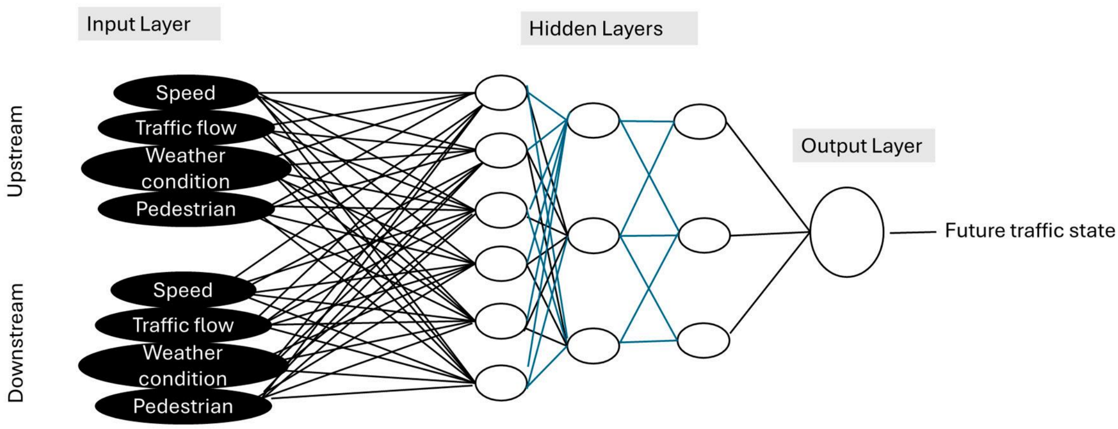

Figure 6. A deep learning configuration for smart transport system application.

4.3. Applications of Machine Learning-Based IoV System

The use of ML in IoV can be deployed into the IoV based on the different architectural layers. For instance, in the perception layer, ML-based application can be beneficial in the detection of moving objects (vehicles, pedestrians, cyclists, traffic signs, road markings, etc.) through input data from visual or sensors with high speed and accuracy [20]. Furthermore, ML can be applied to improve vehicle position accuracy by analyzing input data from GPS sensors and other location-based data. Such accurate and improved vehicle positioning could potentially reduce errors and enhance location information for IoV applications. Collision avoidance is another aspect of interest for ML-based applications in IoV. ML model can be built from input data from radar and cameras, and the model could accurately detect and classify stationary or moving vehicles or objects, predict their speed or trajectory, and alert other participants in the IoV system to avoid collision and ensure safety in the system. AV applications, in particular, have ranged from just mediated perceptions like traffic sign recognition, the detection of the road, and lane change to real-time integrated decision making from scene understanding [34].

Routing is another area where ML finds application in the IoV system. The ML model can be deployed to analyze traffic patterns, road and weather conditions, and user preferences, and make predictions for optimal route planning [111], evaluate traffic dynamics, and make intelligent decisions. Some of the outputs of a ML-based IoV could be in accident forecasting or prediction [112–115]. ML-based IoV applied to routing can be effective in lowering travel time by minimizing traffic congestion [115,116] and guarantee overall efficiency in IoV routing [117,118]. In the network layer, one way the ML-based IoV is utilized is in network resource management. ML can enhance the selection of content cache at the edge network by learning from input data such as traffic patterns, user behavior, and content popularity [20,119,120]. Such intelligent decisions could yield low latency and reduce bandwidth consumption in the IoV system.

ML can be integrated into the IoV physical, network, or infrastructure layer for effective attack, fault, and anomaly detection [20]. Data from sensors and network sources can be monitored continuously and analyzed for the possibility of a fault, attack, or anomality in the IoV system. This could ensure overall system security and reliability as security threats or potential attacks, or system malfunction could be detected early and mitigated in real-time. An anomality in an IoV system could be detected or estimated in the driver/vehicle behavior [121,122]. Advanced ML approaches such as FL have been explored for privacy protection in a data fusion scenario for traffic state estimation application [123]. Vertical FL was leveraged to ensure that multiple collaborating parties could jointly train a model without compromising or exchanging their private data. However, authors worked on the assumptions that parties involved are honest and provided authentic and accurate data.

Table 6 provides a summary of ML-based IoV applications and their commonly used models.

Table 6. Summary of application of ML based IoV.

References	IoV Application	Model Applied	Accuracy
[124]	Traffic identification system	Adaptive Boosting Classifier and Random Forest Algorithm (ABC-RFA)	Acc = 98.90
[125]	Traffic information detection	CNN, LSTM, and LSTM-CNN	FI = 0.9042
[111] [118]	Transportation network planning or routing	GA, SA, and AIS.	Gain of the total travel time SD = 3–5.5%
[112]	Accident forecasting and detection	ANN NLMR	R^2 = 0.76 R^2 = 0.78
[126]		TLRN	Acc = 90–94%
[114]		GRU, RNN, and LSTM	Acc Dec = 94.2% Acc Pre = 75%
[115]		DT, RF, LR, and NB	Acc = 73%
[113]	Traffic accident estimation	ANN GA	RMSE = 2337 RMSE = 4453
[127]		Rare-events logistic regression	McFadden-R^2 = 106.6–106.9
[128]	Incident detection	MLF	Detection rate = 90%
[129]	Traffic flow prediction	MTL	Acc = 81.53–91.74%
[130]		SAE	Acc = 86–90%
[131]		DNN	AC = 0.80–0.83
[132]		ANN	Acc = 92.98
[133]	Short-term speed prediction	BPNN, NARXNN, SVM-RBF, SVM-LIN, MLR	RPE = 88.26–95.46%
[134]	Incident detection	NLP and SVM.	Acc = 88.28%
[135]	Network traffic classification		Acc = 96.89–99.29%
[136] [122]	Driver distraction evaluation	CNNs, BiLSTM	Acc = 92.7%

4.4. Challenges in ML-Based IoV Applications

Most ML-based IoV applications are often characterized by several technical and implementational challenges. We will discuss a few of those under this section.

4.4.1. Unexplainable Model Decision

ML based models make decisions that cannot be explained or reviewed [9,10]. ML models operate as a "black box" [10,136] and do not provide any analysis as to how the independent variables were influenced throughout the prediction process [10,136].

4.4.2. Data Scarcity Concerns

ML models work with a large dataset with good variability to efficiently extract meaningful patterns and output accurate results with meaningful generalization [9,20]. This phenomenon often results in long processing times, network delays, and communication issues. Another issue with large data is the challenge of scalability and trust in the relayed data [20].

4.4.3. Latency Concerns

Most ML-based IoV applications require real-time or near-real-time decision making. In V2I and V2V communications for intelligent transportation systems, real-time decisions are critical for effective application. Hence, latency is a considerable challenge for several machine learning applications [43].

4.4.4. Security and Privacy

With the advent of big data came the accompanying security risk breaches [43]. Data privacy and security is critical in IoV applications. Since ML algorithms process whatever input data they are fed, events where corrupted and unsecure data are processed by ML would yield unfavorable outcomes. Input data to the ML algorithms must be secured and incorruptible. BC has been shown to address some of these data privacy and security concerns [10,43,48].

Machine learning-based solutions promise great exploits for augmenting the functionality and security of blockchain-enabled IoVs. The key features of both technologies could be harnessed in a complementary manner to analyze data, optimize operations, enhance trust, and guarantee a user-friendly IoV system [20,43]. They can also unlock a new array of technological opportunities for safer, more efficient transportation networks. As research further evolves in this field, it is expected that the synergy between machine learning and blockchain would be tapped to reshape the future landscape of smart mobility and autonomous driving, paving the way for intelligent, interconnected vehicles that prioritize safety, sustainability, and user experience.

5. Convergence of ML and Blockchain in IoV

Researchers have alluded to the tremendous benefit of convergence in technology [9,16,21]. Convergence is the merging of know-hows, features, related tools or methods of different technologies to solve a more critical problems, discover technologies, and optimize existing methodology [16]. Convergence often results in the birth of new technology, devices, or industry [10,16]. It forges innovative endeavors, across different domains and helps improve overall individual performance and developmental growth. Technological convergence (TC) as a concept is credited to Nathan Rosenberg in 1960 before it was further developed in 1991 by Kodama [137,138]. TC brings together ICT, digital information, science, and electronics [16,137]. Particularly for the IoV domain, integrating BC and ML together could potentially force a paradigm shift in the IoV domain [9,10]. The integration of ML together with blockchain into the IoV domain could potentially solve IoV issues including security, latency, consensus, scalability, and interoperability [8,9]. The attributes of individual technology can be leveraged in a complementary design to improve the IoV system. The resulting application from the merger can be disruptive innovation that can open new opportunities for businesses and industry. Figure 7 illustrates the beneficial contribution of the convergence of BC and ML to IoV applications.

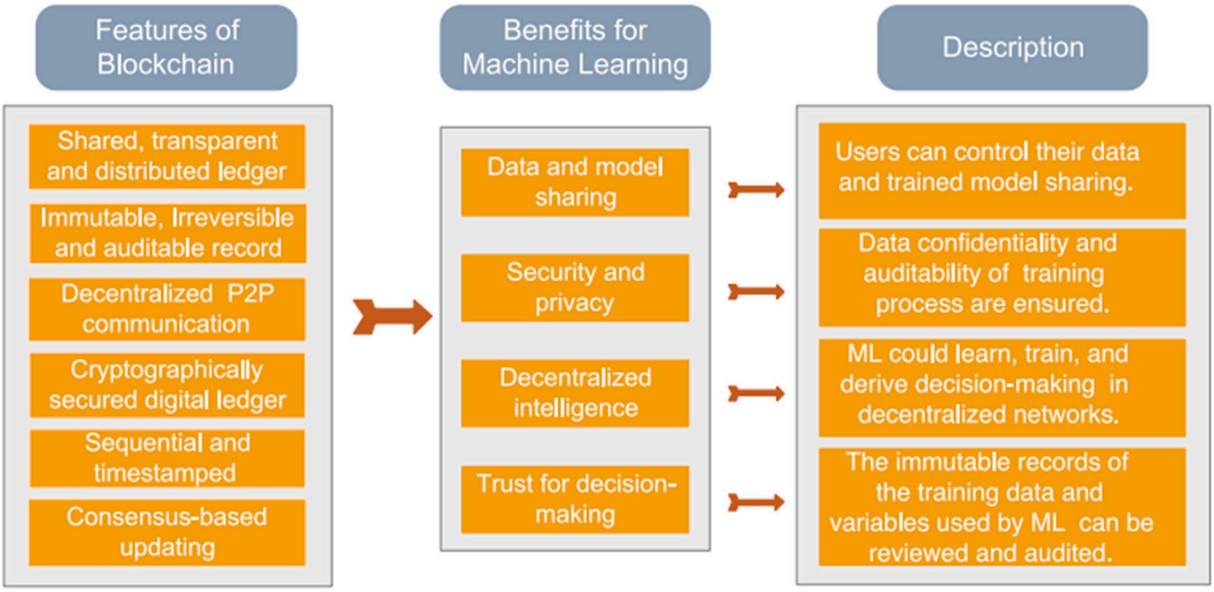

Figure 7. Summary of key contribution of blockchain and machine learning in IoV. Adapted from Liu et al. [139].

5.1. Prospects of ML and BC Convergence for IoV System

5.1.1. Traffic Incidence-Related Applications

ML and BC have been integrated for traffic incident detection [105]. In this study, the authors proposed a framework to manage traffic incidence and provide evidence for road accidence situations. The combination of cooperative event correlation and trust model (Long Short-term Memory (LSTM) and Bayesian model) was employed to predict the next event label at vehicle based on past sequence, while a three-layer hierarchy blockchain framework was incorporated to enhance the security of the traffic incident reporting application. Compared to existing approaches for traffic incident management, the study reported that average network overhead was lowered by 66.24%. The authors also highlighted the significance of the ML (LSTM) approach by comparing the performance of the approach with and without the machine learning in terms of the system overhead.

In a similar study for effective traffic flow predictions, Qi et al. [140] proposed a consortium blockchain-based federated learning framework. The authors leveraged a dBFT-based consortium blockchain to develop a decentralized FL framework. While the blockchain provided a secure defend against poisoning attacks, the FL approach ensured the protection of the privacy of the vehicle data. The results shows that effective robustness to data and poisoning attacks. Furthermore, the study illustrated the impact of blockchain integration by comparing model performance that integrates blockchain and without blockchain. As seen in Figure 8, blockchain incorporation into the proposed scheme ensured that attack success rate (ASR) stayed minimum, compared to the scheme without blockchain, thereby showing the efficacy of blockchain integration with machine learning methods in achieving the optimization of IoV applications. A similar thread has also been highlighted for autonomous driving applications, where blockchain proved robust against a malicious attack with increasing node participation [141]. This is illustrated in Figure 9. It can be noticed that as the number of nodes increased, the success rate remained constant with the proposed blockchain approach, while the collective learning without blockchain showed a decline in the success ratio as the nodes increased.

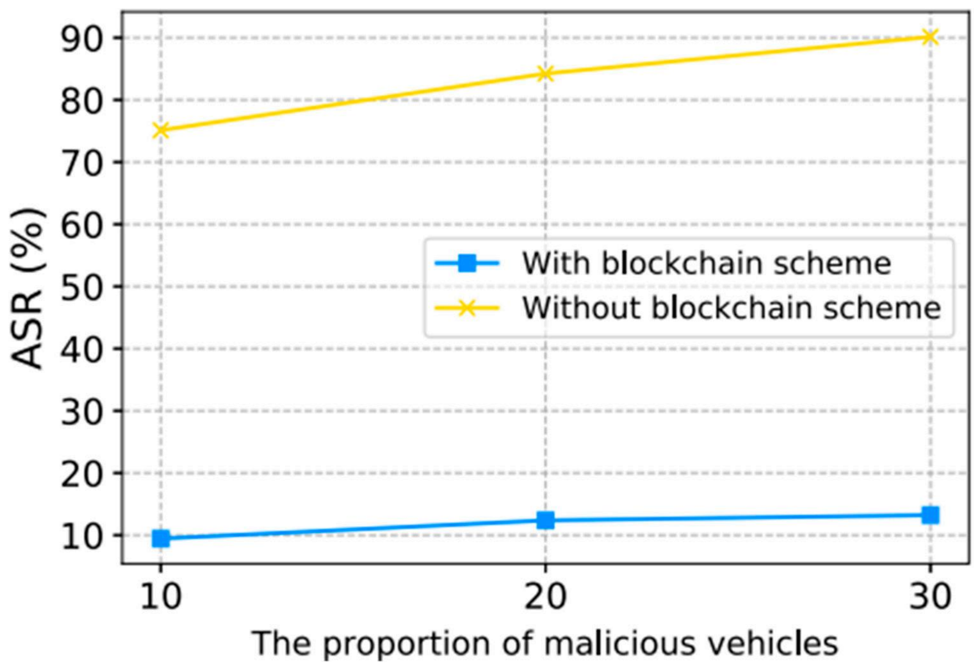

Figure 8. Comparison of the impact of blockchain on the different proportions of malicious vehicles on the attack success rate (ASR). Adapted from Qi et al. [140].

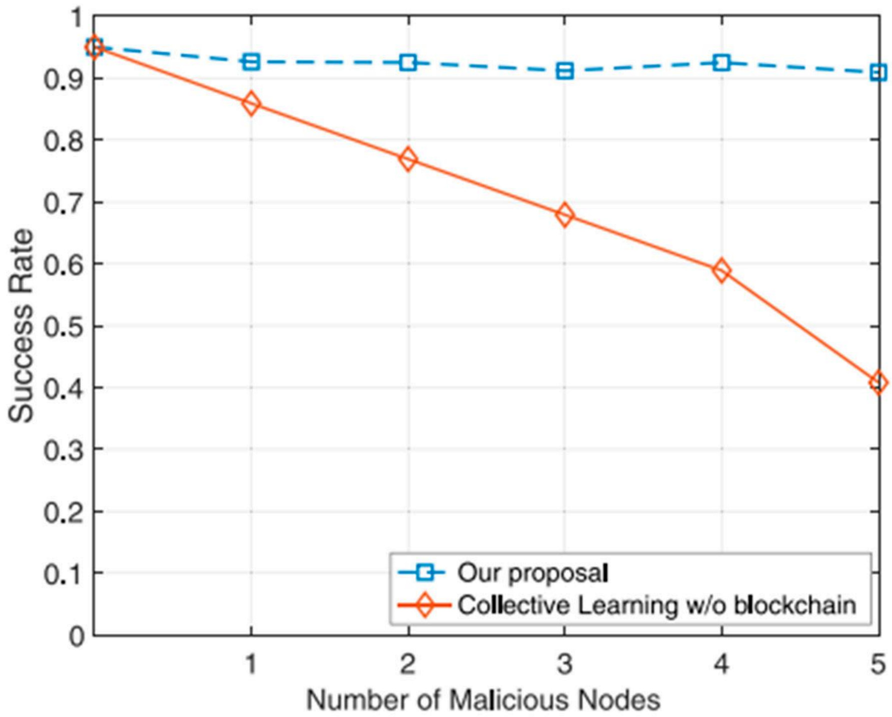

Figure 9. Comparison of two approaches with blockchain integration and without blockchain integration for autonomous driving lane change application. Ratio of successful driving with malicious nodes. Adapted from Fu et al. [141].

For other traffic scenario applications, the DL approach has been combined with blockchain to enhance cooperative positioning for vehicles [142]. The authors reported a robust and secured framework with improved distance prediction performance. FL was deployed in convergence with blockchain for the effective privacy preservation of traffic data [143]. The proposed model showed improvement in terms of model accuracy, computation overhead, and effective consensus mechanism in securely preserving the privacy of traffic data. Similar findings were observed for the applications to ensure a decentralized traffic information collection system [144], for crowdsensing traffic data collection in 5G IoV systems [145], for efficient crowdsensing traffic data management [146], for effective real-time traffic prediction [147], and to achieve a secure incentive-enabled traffic information-sharing scheme [148].

5.1.2. Intrusion Detection Systems

An efficient vehicular network's infrastructure requires that it is built securely and free from attacks. The increased usage of electronic software has evolved into a surge of constant cyber-attacks, thus making the security of these network of paramount importance. Researchers are now finding ways to leverage the convergence of BC and ML to address this critical challenge. Rajan et al. [149] proposed Blockchain-based Multi-Layer Federated Extreme Learning Machines (MLFEM) to enhance an intruder-safe system for secure data transfers. The authors employed FL to develop the MLFEM scheme hosted by the RSU and connected vehicles to achieve efficient resource use without sacrificing security, while blockchain is utilized to record and share training models. The results show that the proposed algorithm after testing on a real-time dataset was able to detect different scenarios of attacks to an accuracy of 98%. Ferrag et al. [150] proposed an IDS that integrates BC and ML for an effective cyber security system against the electricity grid. The authors deployed a recurrent neural network (RNN) for the detection of fraudulent attacks and any network attack to secure a blockchain-based energy network. A PBFT algorithm was used for the consensus mechanism and the authors reported improvement in the results.

5.1.3. Privacy Protection

Wang et al. [143] proposed a BPFL scheme for preserving the privacy of sensitive data in the IoV by means of FL. In this study, Multi-Krum technology was applied to achieve distributed verification and filtering at the ciphertext level. A consortium-based smart contract was used to facilitate the privacy protection by incorporating model verification and a filtering mechanism. A total of 500 clients were selected for the experiment and simulation was performed on the Go (v-1.10.3) platform. The authors reported model performance based on model accuracy, the computation overhead of the verification, and the effectiveness of the incentive mechanism. The proposed model, through its distributed parallel verification mechanism, improved the accuracy of the model, lowered the runtime overhead of the verification contract and effectively managed nodes allocation and honest behaviors of the FL nodes joining the system.

He et al. [151] proposed a fully decentralized ML system combined with FL and then integrated it with a blockchain for the privacy preservation of CAVs. The authors developed a Bift model that enabled a distributed CAVs to train ML models locally their own driven data, using their own while a Proof of Federated Learning (PoFL) was used as the consensus algorithm to resist a security breach in the system. Their results showed that Bift model achieved superior performance in terms of privacy preservation, storage system, and consensus algorithm. Other privacy-preserving approaches have been explored integrating ML and BC for an efficient learning, and data-preserving applications have been reported [152–154], with all showing varying success in the different applications.

5.1.4. Cross-Domain Object Detection, Knowledge Sharing, and Training for Autonomous Driving

A model-sharing approach was developed for training autonomous cars [155]. A YOLOv2 model was designed to enhance the performance of autonomous driving in cross-domain object detection. The authors applied DTL for training the car with a blockchain-enabled MEC technology. BC provides the reliability of model sharing by means of consensus algorithm while MEC enabled low delay and real-time computational strength. Simulations were carried out on a public dataset and the results indicate that the proposed model achieved better efficiency and reliability. Blockchain has also been integrated in the learning process of autonomous cars to enhance knowledge sharing [156]. In this study, the authors proposed the concept of collective learning, where the entire car produced in a batch could be trained simultaneously using RL simply by training only one car and subsequently using BC to share the knowledge with other cars. The authors concluded that integrating blockchain features to the ML training of autonomous vehicles enhances its efficiency and optimize the training process. Similar studies have considered different framework for efficient knowledge sharing applications.

Chai et al. [157] developed a hierarchical blockchain-enabled federated learning algorithm for effective knowledge sharing in intelligent vehicles. By using a hierarchical blockchain framework coupled with a hierarchical FL framework, the authors were able to reduce the computation consumption and improve the learning accuracy and overall efficiency of the system. Lu et al. [158] combined the DAG-based blockchain together with asynchronous FL scheme to develop an effective data sharing framework for IoV. In this study, an asynchronous federated learning mechanism enabled by Deep Reinforcement Learning (DRL) was utilized for effective node selection, while the blockchain ensured the reliability of shared data by executing a two-stage verification process. The authors reported higher learning accuracy as well as faster convergence of the overall process. Similar studies include efficient traffic data sharing [153], blockchain-based collective learning (BCL) framework for autonomous lane-changing systems [141,159], effective learning framework for autonomous cars for efficient heuristic service in the supply chain industry [160], and efficient adaptive sharding to enhance driving experience [161].

5.1.5. Content Caching

In the Cognitive Internet of Vehicles (CIoV), user experience is improved by means of content caching. It brough about added features such as vehicle-deployment monitoring and resource allocation. Through content caching, cognitive engines can gauge the content requirements of users and provide such content to requesters. In this application, privacy is paramount to both users and requesters as there is a possibility of data leakage. In a bid to address that, Qian et al. [162] proposed a blockchain-based privacy-aware content caching approach in CIoV. ML provides the perception through deep learning by learning the need of the participating vehicles, analyzing such perceptual data and sending feedback to the system. Blockchain is used to ensure secured content sharing transactions. The authors analyzed the performance of their approach by the cache hit ratio under different Zipf parameters as well as under different vehicle requesters. They reported that the proposed approach's content caching was superior to the traditional content caching scheme. Shen et al. [163] proposed a privacy-protecting predictive cache method based on blockchain and machine learning (BML-PPPCM). BML-PPPCM provides a method for obtaining services by broadcasting cached data via CPs to reduce query requests. In this study, the authors implemented a Bi-directional Long-Short Term Memory (Bi-LSTM) model is to enhance query prediction, before a deep Q-learning (DQN) was utilized to determine the optimal cache decision.

Blockchain was used to improve system protection by securely storing the transaction and trust data. The authors compared simulated results with similar studies and found that the newly proposed BML-PPPCM achieved a higher cache hit ratio and a better malicious response than other similar schemes. By integrating BC and ML, this study showed improvement in the privacy protection and suppression of malicious and incentive denial of service attacks. A permissioned blockchain was employed to address the trust issues in content caching [164]. The authors applied a lightweight Proof-of-Utility (PoU) approach that served as block verifier selection metric while a e DRL provided the output for intelligent content caching. The results tested on an Uber dataset showed that the proposed scheme attained better performance when compared to existing approaches.

5.1.6. Secure Energy-Trading System

Electric vehicles (EVs) in the IoV system require charging to be operational. During their charging regime, they establish a vehicular network (VN) that connects them to charging stations, roadside units (RSU), and other EVs. Participants in this VN share, among other things, road and weather information, nearby charging EVs stations, and other important information in RSUs. This predisposes them to issues such as privacy, trust, or the inefficient use of shared information. To address all these, researchers are exploring different approaches for privacy-preserving solutions.

Ashfaq et al. [165] proposed a blockchain-based secure energy-trading system that integrates machine learning for optimal energy trading scheme. In this study, the k-NN algorithm was used to calculate the shortest distance between a charging station and an EV, while the blockchain provided a solution to the transaction redundancy problem through a hashing algorithm. The authors report that the proposed mechanism enhanced evaluation of the energy request by an EV and suggested the amount of energy and the closet available at the charging station. A summary of all the different IoV applications where technical solutions is provided by the integrated approach involving blockchain and machine learning towards an improved ITS is provided in Table 7.

Table 7. Summary of applications of ML in blockchain-based IoV.

Ref.	Application	BC Type/Consensus Mechanism	ML Adopted	Key Findings
Wang et al. [144]	Secure traffic information collection	Proof-of-Work (PoW)	TE-LSTM	The proposed scheme was able to protect users' identities and travel traces, and defend against Byzantine attacks and Sybil attacks.
Wang et al. [143]	Secure traffic data management	Consortium Blockchain (PBFT)	FL	The proposed scheme achieved improvement in the runtime overhead and model accuracy.
Wang et al. [145]	Secured vehicular data collection system	Proof of Computing (PoC)	DRL	The proposed approach achieved a good tradeoff between latency and safety, and greatly lowered the uploading delay.
Philip and Saravanaguru [105]	Efficient traffic incident reporting	Ethereum blockchain	LSTM	The proposed scheme achieved improvement in the overall efficiency.
Qi et al. [140]	Effective traffic flow prediction	dBFT-based consortium blockchain	FL	The proposed schemes effectively enabled data poisoning attacks defense and achieved improved privacy protection for traffic flow prediction.
Mao et al. [166]	Accurate credit evaluation	Hyperledger	LSTM	The proposed approach was effective in the supervision and management of the food supply chain.
Pokhrel and Choi [152]	Efficient vehicular communication networking	Proof-of-Work (PoW)	FL	The proposed method minimized system delay.
Jiang et al. [155]	Enabled vehicle data sharing	DPoS	DDL	The proposed method improved the mAP by 6.32% and ensured secure data sharing between vehicles.
Gandhi and Chaudhary [156]	Efficient knowledge haring and collective learning	Public ledger	RL	The proposed approach actualized synchronous car learning and knowledge sharing.
Chai et al. [157]	Efficient knowledge sharing	Proof-of-Knowledge (PoK)	hierarchical FL	The proposed scheme enhanced the sharing efficiency and increased learning accuracy and optimal utility during the sharing process.
He et al. [151]	Efficient data sharing for CAVs	Proof of Federated Learning (PoFL)	FL	The proposed model showed better performance in terms of privacy preserving, secure storage, incentive mechanism, robustness, gradient encryption, and distribution of the system.

Table 7. *Cont.*

Ref.	Application	BC Type/Consensus Mechanism	ML Adopted	Key Findings
Lu et al. [158]	Efficient data sharing	Permissioned blockchain (Directed Acyclic Graph (DAG)	Asynchronous FL	The proposed scheme achieved improved learning accuracy as well as faster convergence.
Li et al. [153]	Efficient traffic data sharing	BFT-DPOS	Opportunistic FL	
Ning et al. [146]	Efficient traffic data management	DPOF	DRL	The proposed approach achieved minimizing the system latency and improved the data safety and user utility.
Meese et al. [147]	Efficient traffic prediction	Permissioned blockchain	FL	The proposed system enabled a decentralized model training.
Alam et al. [148]	Effective incentive-enabled traffic information sharing	PoS	ANN-based ANFIS	The proposed system enhanced the security and privacy of the system and enabled improved user participation.
Fu et al. [141]	Efficient autonomous lane-changing behavior	BFT-DPoS	DRL	The proposed model achieved over 96.5% ratio of successful lane changes and was robust in defending against malicious nodes.
Fu et al. [159]	Effective collective learning for autonomous driving	BFT-DPoS	DRL	The proposed approach's average positioning performance increased by 83.78% and achieved the smallest positional error for the same number of cooperators.
Ahamed and Karthikeyan [160]	Effective learning for autonomous cars	Public blockchain	RL	The proposed method demonstrated better performance in terms of service time and data traffic than the existing heuristic search methods.
Lin et al. [161]	Efficient adaptive sharding	PBFT	DRL	The proposed approach lowered the communication overhead and was adaptive.
Song et al. [142]	Efficient information sharing for accurate cooperative positioning	DPoS	DL	The proposed approach improved the positioning accuracy of vehicles with increase in speed of vehicle.
Qian et al. [162]	Secure content caching			The proposed scheme achieved privacy protection and secure content transaction.
Shen et al. [163]	Secure predictive caching system		Bi-LSTM, deep Q-learning (DQN)	The proposed scheme attained higher cache hit ratio than other compared approaches and also ensured data privacy protection.

Table 7. *Cont.*

Ref.	Application	BC Type/Consensus Mechanism	ML Adopted	Key Findings
Ashfaq et al. [165]	Secure EV charging system	Consortium Blockchain	k-NN	The proposed approach attained great reduction in computational delay and resolved inherent storage issues.
Dai et al. [164]	Effective content caching system	PoU	DRL	The proposed approach achieved the minimum cumulative average reward as compared to two known methods.
Rajan et al. [149]	Intrusion detection system for energy grid		FL	The proposed system achieved improvement in security and privacy in data transmission.
Ferrang et al. [150]	Secure electricity network	PBFT	RNN	The proposed approach achieved an accuracy of 96.82%.

6. Discussion and Future Directions

6.1. Consensus Algorithm

A consensus algorithm is defined as a mechanism through which agreement is attained between nodes in a distributed system. This process ensures that system reliability is obtained even when dealing with malicious or faulty nodes from different networks [167]. An event leading to a failed consensus between the nodes is called "fork" [167]; this occurs when no agreement is reached by the different nodes in a network. For integrated applications of ML and BC, some of the utilized consensus algorithms includes PoK, PoC, PoFL, PoS, and PoU, among others [164].

6.2. Federated Learning

FL is a type of machine learning strategy that is distributed in its approach, where models are allowed to be trained over decentralized devices or servers while keeping local data [8,39,168]. In FL, participants collaboratively receive a global model obtained from the central server, train the model locally, and submit local update to the central server without releasing the raw data [140]. The aggregates from all the local model updates are then collected by the central server to form a new global model [140]. This process continues repeated until convergence is achieved. This FL approach has enabled the removal of privacy threats for vehicles by performing TFP tasks locally, though FL still heavily relies on the central server to collate and manage the local model update [168]. FL was developed by Google in 2016 to solve the problem of data integration in vehicular networks [140]. One of the shortfalls of FL system is that model updates are obtained from centralized sources—the global server. This makes the system vulnerable to attacks such as single-point failure [39].

6.3. Challenges and Considerations

6.3.1. Communication Overhead Cost for FL

For most applications, FL has shown promising success with regard to model accuracy. In Figure 8, Rajan et al. [149] compared its performance to a traditional ML approach. It shows that FL was more effective in addressing IDS problems. However, the communication overhead cost for FL is somewhat expensive [158]. This has an overall impact on the performance of the FL-enabled framework. To mitigate that, effective algorithms and frameworks that would lower the communication overhead could be developed.

6.3.2. Scalability Issues in Blockchain-Based IoV

The problem of scalability arises as IoV system expands and the number of vehicles begin to increase, leading to increased number of blockchain nodes as well [8]. Other factors that affect scalability include block size, the number of transactions, and the consensus protocols employed [8,169]. Latency also experiences increment as vehicles are added into the IoV system. Protocols that seek to address scalability issues in IoV systems often make tradeoffs between solutions, which leads to an increase in latency at the expense of high scalability. Finding optimal solutions would involve developing efficient consensus algorithms designed towards improving scalability in the IoV system.

6.4. Performance Evaluation Metrics

For most applications of IoV, some of the metrics used to evaluate a blockchain performance include time, cost, key transfer time, power, reputation value, detection rate, utility, detection accuracy, throughput, end-to-end delay, packet loss ratio, energy, and network congestion [28]. Time is the more favored metric for BC performance, and the interval with the average execution rate is 70–80 s [30]. Particularly for data and information-sharing applications where data privacy, learning accuracy, and the participation of the vehicles are explored, the performance criteria that researchers try to evaluate include model accuracy, computational overhead, and the effectiveness of the incentive mechanism [143]. The apprehensiveness of a consensus mechanism can be evaluated by two approaches; the first is the communication rounds and accuracy approach, and the other approach is by evaluating the block confirmation delay [153]. Other evaluation metrics for blockchain and ML integrated applications include security, communication cost, anonymity, attack probability, average transaction confirmation time, and average transaction speed [148].

6.4.1. Cache Hit Ratio

The cache hit ratio is an important indicator in privacy-preserving applications [163]. Higher values of the cache hit ratio indicate less possibility of privacy leakage.

6.4.2. Throughput

Throughput is determined by the ratio of the number of trusted data to the number of services requested [163]. It is measured in transactions per seconds (TPS) and reveals the number of transactions processed by the blockchain network during a testing cycle [147].

6.4.3. Packet Delivery Rate (PDR)

PDR [170] is the ratio of the total number of data packets successfully received at the destination pt to the total number of data packets coming from the source node.

6.5. Future Directions

The paradigm of ML-assisted blockchain IoV applications promises groundbreaking and cutting-edge research prospects. It allows for leveraging the strengths of both technologies in overcoming the inherent limitations of individual technologies. Some of the identified prospective research areas are enumerated below.

6.5.1. Incentive Mechanism Exploration

Future research should investigate different combination of ML algorithms, and BC incentive mechanisms can be explored to achieve optimal efficiency in terms of energy cost and computational complexity. In AV applications, reinforcement learning can be integrated with heuristic search methods to enhance the routes planning for self-driving cars in the IoV system for supply-chain applications. Furthermore, a more efficient IoV system can be developed by exploring BC-enabled data collection set-ups, and such secure and reliable data can be utilized to train ML models in autonomous vehicles. This approach could greatly improve overall system performance.

6.5.2. Further Integration with Novel and Complementary Technologies

The convergence of ML, BC, and IoV promises great potential as a remarkable technological breakthrough. However, further improvement can be attained by combining this achievement with other cutting-edge technologies. Some of these high-end technologies include digital twins, MEC, Fog computing, etc. [171–173]. Consequently, future research efforts should be directed towards discussing the potential of integration with other cutting-edge technologies for improvement in intelligent transportation systems.

6.5.3. Exploration of Node Selection Mechanisms

Frameworks that are use-specific are evolving in the IoV integration of BC and ML. For example, approaches such as hierarchical FL, asynchronous FL, Opportunistic FL, and synchronous FL have now been proposed to enhance performance and optimize the FL deployment [153,157,158]. A similar development is witnessed in the deployment of consensus algorithms. Some of the recently developed consensus algorithms include Proof of Federated Learning (PoFL) [151], BFT-DPoS [153], PoU [164], etc. These have all shown to be effective in their application. Future studies could develop novel and innovative algorithms and adaptable frameworks for optimal implementation. There is also a need to optimize the mechanism of node selection [153]. Solutions that consider factors such as energy consumption, scalability, communication cost, computational cost, and the overall system running time should be explored in future studies. This will lead to enhancements in system applicability and performance in ITS.

7. Conclusions

In this review article, we have provided an overview of IoV, blockchain, ML, and the intersection of these three fields. The benefits to the transportation system while transforming from the traditional, unintelligent, and isolated VANET system to the new smart, intelligent, and multi-connected one have been expanded. The applications of the convergence of BC, ML, and IoV were also cataloged. The major objective of these applications are traffic-incidence management and reporting, safe and secure data and knowledge sharing, intrusion and fault detection, and optimal resource allocation, among others. Now, the studies predominantly reported have been simulations, and no real-life application has been deployed yet. Future research should focus on real-world applications and testing. Though research into the integration of blockchain and machine learning for IoV is still very recent, its promises to revolutionize the field of the intelligent transport system. It is expected that passengers, pedestrians, vehicle vendor companies, transportation agencies, and emergency service providers are among the parties that would leverage these massive innovations and real-time services provided in IoV.

Author Contributions: Conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, E.E.O.; writing—review and editing, visualization, supervision, project administration, funding acquisition, V.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

Acknowledgments: We acknowledge the contribution of the reviewers and the editor for the kind consideration of this manuscript and the robust feedback that has improved the content of the final paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Abduljabbar, R.; Dia, H.; Liyanage, S.; Bagloee, S.A. Applications of Artificial Intelligence in Transport: An Overview. *Sustainability* **2019**, *11*, 189. [CrossRef]
2. Wang, C.; Cheng, X.; Li, J.; He, Y.; Xiao, K. A survey: Applications of blockchain in the Internet of Vehicles. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 77. [CrossRef]
3. Liang, J.; Li, Y.; Yin, G.-D.; Xu, L.; Lu, Y.; Feng, J.; Shen, T.; Cai, G. A MAS-Based Hierarchical Architecture for the Cooperation Control of Connected and Automated Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 1559–1573. [CrossRef]
4. Huang, S.; Sun, D.; Zhao, M. Distributed MPC-Based Hierarchical Cooperative Control for Mixed Vehicle Groups with T-CPS in the Vicinity of Traffic Signal Light. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 8003–8016. [CrossRef]
5. Cherbal, S.; Zier, A.; Hebal, S.; Louail, L.; Annane, B. Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *J. Supercomput.* **2024**, *80*, 3738–3816. [CrossRef]
6. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1212–1239. [CrossRef]
7. Zhu, S.; Cai, Z.; Hu, H.; Li, Y.; Li, W. zkCrowd: A Hybrid Blockchain-Based Crowdsourcing Platform. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4196–4205. [CrossRef]
8. Hildebrand, B.; Baza, M.; Salman, T.; Tabassum, S.; Konatham, B.; Amsaad, F.; Razaque, A. A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions. *Comput. Sci. Rev.* **2023**, *48*, 100547. [CrossRef]
9. Ressi, D.; Romanello, R.; Piazza, C.; Rossi, S. AI-enhanced blockchain technology: A review of advancements and opportunities. *J. Netw. Comput. Appl.* **2024**, *225*, 103858. [CrossRef]
10. Singh, P.; Elmi, Z.; Lau, Y.Y.; Borowska-Stefańska, M.; Wiśniewski, S.; Dulebenets, M.A. Blockchain and AI technology convergence: Applications in transportation systems. *Veh. Commun.* **2022**, *38*, 100521. [CrossRef]
11. Gaurav, A.; Gupta, B.B.; Panigrahi, P.K. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterp. Inf. Syst.* **2023**, *17*, 2023764. [CrossRef]
12. Tanwar, S.; Bhatia, Q.; Patel, P.; Kumari, A.; Singh, P.K.; Hong, W.C. Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. *IEEE Access* **2020**, *8*, 474–488. [CrossRef]

13. Russell, S.J.; Norvig, P. *Artificial Intelligence: A Modern Approach*, 3rd ed.; Pearson Publishers: Upper Saddle River, NJ, USA, 2005.
14. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
15. Rahouti, M.; Xiong, K.; Ghani, N. Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. *IEEE Access* **2018**, *6*, 67189–67205. [CrossRef]
16. Fazel, E.; Nezhad, M.Z.; Rezazadeh, J.; Moradi, M.; Ayoade, J. IoT convergence with machine learning & blockchain: A review. *Internet Things* **2024**, *26*, 101187. [CrossRef]
17. Zhang, Y.; Liu, Y.; Chen, C.-H. Survey on Blockchain and Deep Learning. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2020.
18. Trivedi, M.; Kakkar, R.; Gupta, R.; Agrawal, S.; Tanwar, S.; Niculescu, V.-C.; Raboaca, M.S.; Alqahtani, F.; Saad, A.; Tolba, A. Blockchain and Deep Learning-Based Fault Detection Framework for Electric Vehicles. *Mathematics* **2022**, *10*, 3626. [CrossRef]
19. Agrawal, K.; Aggarwal, M.; Tanwar, S.; Sharma, G.; Bokoro, P.N.; Sharma, R. An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions. *IEEE Access* **2022**, *10*, 116858–116906. [CrossRef]
20. Zamanirafe, M.; Mansourian, P.; Zhang, N. Blockchain and Machine Learning in Internet of Vehicles: Applications, Challenges, and Opportunities. *IEEE Internet Things Mag.* **2023**, *6*, 98–103. [CrossRef]
21. Alkashto, H.; Elewi, A. Integration of blockchain and machine learning for safe and efficient autonomous car systems: A survey. *Turk. J. Eng.* **2023**, *8*, 282–299. [CrossRef]
22. Hemmati, A.; Zarei, M.; Souri, A. Blockchain-based internet of vehicles (BIoV): A systematic review of surveys and reviews. *Secur. Priv.* **2023**, *6*, e317. [CrossRef]
23. Biswas, A.; Wang, H.C. Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain. *Sensors* **2023**, *23*, 1963. [CrossRef] [PubMed]
24. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in internet of vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]
25. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S. Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey. *IEEE Internet Things J.* **2021**, *8*, 4157–4185. [CrossRef]
26. Karger, E.; Jagals, M.; Ahlemann, F. Blockchain for smart mobility-literature review and future research agenda. *Sustainability* **2021**, *13*, 13268. [CrossRef]
27. Abbas, S.; Talib, M.A.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.H. Blockchain-based authentication in internet of vehicles: A survey. *Sensors* **2021**, *21*, 7927. [CrossRef]
28. Kumar, S.; Velliangiri, S.; Karthikeyan, P.; Kumari, S.; Kumar, S.; Khan, M.K. A survey on the blockchain techniques for the Internet of Vehicles security. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4317. [CrossRef]
29. Sargolzaei, A. Security of Cyber-Physical Systems. Available online: www.mdpi.com/journal/electronics (accessed on 29 October 2024).
30. Mikavica, B.; Kostić-Ljubisavljević, A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey. *J. Supercomput.* **2021**, *77*, 9520–9575. [CrossRef]
31. Saad, M.; Khan, M.K.; Ahmad, M.B. Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review. *Sustainability* **2022**, *14*, 3919. [CrossRef]
32. Jabbar, R.; Fetais, N.; Kharbeche, M.; Krichen, M.; Barkaoui, K.; Shinoy, M. Blockchain for the Internet of Vehicles: How to Use Blockchain to Secure Vehicle-to-Everything (V2X) Communication and Payment? *IEEE Sens. J.* **2021**, *21*, 15807–15823. [CrossRef]
33. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Veh. Commun.* **2022**, *34*, 100458. [CrossRef]
34. Ma, Y.; Wang, Z.; Yang, H.; Yang, L. Artificial intelligence applications in the development of autonomous vehicles: A survey. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 315–329. [CrossRef]
35. Gangwani, D.; Gangwani, P. Applications of Machine Learning and Artificial Intelligence in Intelligent Transportation System: A Review. In *Lecture Notes in Electrical Engineering*; Springer Science and Business Media Deutschland GmbH: Berlin/Heidelberg, Germany, 2021; pp. 203–216. [CrossRef]
36. Iyer, L.S. AI enabled applications towards intelligent transportation. *Transp. Eng.* **2021**, *5*, 100083. [CrossRef]
37. Dibaei, M.; Zheng, X.; Xia, Y.; Xu, X.; Jolfaei, A.; Bashir, A.K. Investigating the Prospect of Leveraging Blockchain and Machine Learning to Secure Vehicular Networks: A Survey. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 683–700. [CrossRef]
38. Javed, A.R.; Hassan, M.A.; Shahzad, F.; Ahmed, W.; Singh, S.; Baker, T.; Gadekallu, T.R. Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors* **2022**, *22*, 4394. [CrossRef] [PubMed]
39. Sameera, K.M.; Nicolazzo, S.; Arazzi, M.; Nocera, A.; Rehiman, K.R.; Vinod, P.; Conti, M. Privacy-preserving in Blockchain-based Federated Learning systems. *Comput. Commun.* **2024**, *222*, 38–67. [CrossRef]
40. Astarita, V.; Giofrè, V.P.; Mirabelli, G.; Solina, V. A Review of Blockchain-Based Systems in Transportation. *Information* **2020**, *11*, 21. [CrossRef]
41. Butt, T.A.; Iqbal, R.; Salah, K.; Aloqaily, M.; Jararweh, Y. Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions. *IEEE Access* **2019**, *7*, 79694–79713. [CrossRef]
42. Jabbar, R.; Dhib, E.; Said, A.B.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 20995–21031. [CrossRef]

43. Yazici, İ.; Shayea, I.; Din, J. A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Eng. Sci. Technol. Int. J.* **2023**, *44*, 101455. [CrossRef]
44. Taslimasa, H.; Dadkhah, S.; Neto, E.C.P.; Xiong, P.; Ray, S.; Ghorbani, A.A. Security issues in Internet of Vehicles (IoV): A comprehensive survey. *Internet Things* **2023**, *22*, 100809. [CrossRef]
45. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2018**, *5*, 3701–3709. [CrossRef]
46. Yang, F.; Li, J.; Lei, T.; Wang, S. Architecture and key technologies for Internet of Vehicles: A survey. *J. Commun. Inf. Netw.* **2017**, *2*, 1–17. [CrossRef]
47. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of Internet of Vehicles. *China Commun.* **2014**, *11*, 1–15. [CrossRef]
48. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
49. Alkarim, A.S.; Al-Ghamdi, A.S.A.-M.; Ragab, M. The Internet of Vehicles (Iov) Technology: Challenges and Solutions. *J. Theor. Appl. Inf. Technol.* **2023**, *101*, 7629–7639.
50. Su, T.; Shao, S.; Guo, S.; Lei, M. Blockchain-Based Internet of Vehicles Privacy Protection System. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8870438. [CrossRef]
51. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.-T. Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. *IEEE Access* **2016**, *4*, 5356–5373. [CrossRef]
52. Xu, W.; Zhou, H.; Cheng, N.; Lyu, F.; Shi, W.; Chen, J.; Shen, X. Internet of vehicles in big data era. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 19–35. [CrossRef]
53. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-based batch authentication protocol for Internet of Vehicles. *J. Syst. Archit.* **2021**, *113*, 101877. [CrossRef]
54. Elliott, D.; Keen, W.; Miao, L. Recent advances in connected and automated vehicles. *J. Traffic Transp. Eng.* **2019**, *6*, 109–131. [CrossRef]
55. Contreras-Castillo, J.; Zeadally, S.; Ibáñez, J.A.G. A seven-layered model architecture for internet of vehicles. *J. Inf. Telecommun.* **2017**, *1*, 4–22. [CrossRef]
56. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N. Blockchain-Based Trust Management for Internet of Vehicles. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1397–1409. [CrossRef]
57. Chen, C.; Wu, J.; Lin, H.; Chen, W.; Zheng, Z. A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9110–9121. [CrossRef]
58. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. [CrossRef]
59. Marin, O.; Cioara, T.; Anghel, I. Blockchain Solution for Buildings' Multi-Energy Flexibility Trading Using Multi-Token Standards. *Future Internet* **2023**, *15*, 177. [CrossRef]
60. Liu, M.; Teng, Y.; Yu, F.R.; Leung, V.C.M.; Song, M. Deep Reinforcement Learning Based Performance Optimization in Blockchain-Enabled Internet of Vehicle. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
61. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
62. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: www.bitcoin.org (accessed on 29 October 2024).
63. Astarita, V.; Giofrè, V.P.; Guido, G.; Vitale, A. The convergence of Internet of Things, Blockchain and Connected Vehicles: Conceptual Advantages and Disadvantages of a new Cooperative Intelligent Transportation System. *Int. J. Traffic Transp. Manag.* **2021**, *3*, 33–41. [CrossRef]
64. Pandl, K.D.; Thiebes, S.; Schmidt-Kraepelin, M.; Sunyaev, A. On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda. *IEEE Access* **2020**, *8*, 57075–57095. [CrossRef]
65. Wei, H.; Feng, W.; Zhang, C.; Chen, Y.; Fang, Y.; Ge, N. Creating efficient blockchains for the internet of things by coordinated satellite-terrestrial networks. *IEEE Wirel. Commun.* **2020**, *27*, 104–110. [CrossRef]
66. Shrivas, M.K.; Yeboah, T. The Disruptive Blockchain: Types, Platforms and Applications. In Proceedings of the 5th Texila World Conference for Scholars (TWCS), 2018 on Transformation: The Creative Potential of Interdisciplinary & Multidisciplinary Knowledge Exchange, Georgetown, Guyana, 27–29 December 2018. [CrossRef]
67. Hussain, A.A.; Al-Turjman, F. Artificial intelligence and blockchain: A review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4268. [CrossRef]
68. Mitra, A.; Bera, B.; Das, A.K.; Jamal, S.S.; You, I. Impact on blockchain-based AI/ML-enabled big data analytics for Cognitive Internet of Things environment. *Comput. Commun.* **2023**, *197*, 173–185. [CrossRef]
69. Arooj, A.; Farooq, M.S.; Umer, T. Unfolding the blockchain era: Timeline, evolution, types and real-world applications. *J. Netw. Comput. Appl.* **2022**, *207*, 103511. [CrossRef]
70. Ji, B.; Zhang, M.; Xing, L.; Li, X.; Li, C.; Han, C.; Wen, H. Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digit. Commun. Netw.* **2023**, *9*, 47–55. [CrossRef]
71. Jiang, T.; Fang, H.; Wang, H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet Things J.* **2019**, *6*, 4640–4649. [CrossRef]

72. Di Vaio, A.; Varriale, L. Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. *Int. J. Inf. Manag.* **2020**, *52*, 102014. [CrossRef]
73. Aktas, E.; Demir, S.; Paksoy, T. *The Use of Blockchain in Aviation Safety Reporting Systems: A Framework Proposal*; Routledge: Oxfordshire, UK, 2022. [CrossRef]
74. Poleshkina, I. Blockchain in air cargo: Challenges of new World. *MATEC Web Conf.* **2021**, *341*, 00021. [CrossRef]
75. Ahmad, R.W.; Salah, K.; Jayaraman, R.; Hasan, H.R.; Yaqoob, I.; Omar, M. The Role of Blockchain Technology in Aviation Industry. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 4–15. [CrossRef]
76. Li, X.; Lai, P.-L.; Yang, C.-C.; Yuen, K.F. Determinants of blockchain adoption in the aviation industry: Empirical evidence from Korea. *J. Air Transp. Manag.* **2021**, *97*, 102139. [CrossRef]
77. Revin, V.; Shevcheko, Y. The opportunities and challenges of implementation of blockchain in aviation industry. *Young Sci.* **2019**, *4*, 206–209. [CrossRef]
78. Lopes, D.P.; Rita, P.; Treiblmaier, H. The impact of blockchain on the aviation industry: Findings from a qualitative study. *Res. Transp. Bus. Manag.* **2021**, *41*, 100669.
79. Naser, F. Review: The potential use of blockchain technology in railway applications: An introduction of a mobility and speech recognition prototype. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 4516–4524.
80. Pokusaev, O.; Kupriyanovsky, V.; Namiot, D.; Lazutkina, V.; Zazhigalkin, A.; Kupriyanovsky, P. Blockchain on the digital railway in Germany. *Int. J. Open Inf. Technol.* **2018**, *6*, 43–53.
81. Kuperberg, M. Scaling a Blockchain-based Railway Control System Prototype for Mainline Railways: A Progress Report. 2021. Available online: http://arxiv.org/abs/2103.08304 (accessed on 29 October 2024).
82. Subramanian, N.; Chaudhuri, A.; Kayikci, Y. Blockchain Applications and Future Opportunities in Transportation. In *Blockchain and Supply Chain Logistics*; Palgrave Pivot: Cham, Switzerland, 2020; pp. 39–48.
83. Vishwakarma, L.; Das, D. SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain. *Veh. Commun.* **2022**, *33*, 100429. [CrossRef]
84. Chen, C.; Xiao, T.; Qiu, T.; Lv, N.; Pei, Q. Smart-Contract-Based Economical Platooning in Blockchain-Enabled Urban Internet of Vehicles. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4122–4133. [CrossRef]
85. Wagner, M.; McMillin, B. Cyber-physical transactions: A method for securing VANETs with Blockchains. In Proceedings of the IEEE Pacific Rim International Symposium on Dependable Computing, PRDC, IEEE Computer Society, Taipei, Taiwan, 4–7 December 2018; pp. 64–73. [CrossRef]
86. Pourvahab, M.; Ekbatanifard, G. Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology. *IEEE Access* **2019**, *7*, 153349–153364. [CrossRef]
87. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
88. Cheng, L.; Liu, J.; Xu, G.; Zhang, Z.; Wang, H.; Dai, H.-N.; Wu, Y.; Wang, W. SCTSC: A Semicentralized Traffic Signal Control Mode with Attribute-Based Blockchain in IoVs. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1373–1385. [CrossRef]
89. Ren, Q.; Man, K.L.; Li, M.; Gao, B.; Ma, J. Intelligent design and implementation of blockchain and Internet of things–based traffic system. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719870653. [CrossRef]
90. Chai, H.; Leng, S.; Wu, F.; He, J. Secure and Efficient Blockchain-Based Knowledge Sharing for Intelligent Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 14620–14631. [CrossRef]
91. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J.* **2019**, *6*, 4660–4670. [CrossRef]
92. Shivers, R.; Rahman, M.A.; Shahriar, H. Toward a Secure and Decentralized Blockchain-based Ride-Hailing Platform for Autonomous Vehicles. *arXiv* **2019**, arXiv:1910.00715.
93. Li, M.; Zhu, L.; Lin, X. CoRide: A Privacy-Preserving Collaborative-Ride Hailing Service Using Blockchain-Assisted Vehicular Fog Computing. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 408–422. [CrossRef]
94. Li, M.; Zhu, L.; Lin, X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J.* **2019**, *6*, 4573–4584. [CrossRef]
95. Al Amiri, W.; Baza, M.; Banawan, K.; Mahmoud, M.; Alasmary, W.; Akkaya, K. Towards Secure Smart Parking System Using Blockchain Technology. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; Volume 8, pp. 1214–1229. [CrossRef]
96. Kim, W.; Ryu, K. Autocoin: Secure content sharing based on blockchain for vehicular cloud. *Electronics* **2021**, *10*, 1477. [CrossRef]
97. Kim, K.; Kim, T.; Jung, I.Y. Blockchain-Based Information Sharing between Smart Vehicles for Safe Driving. Available online: http://developers.hyundai.com/ (accessed on 29 October 2024).
98. Chai, H.; Leng, S.; Zhang, K.; Mao, S. Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles. *IEEE Access* **2019**, *7*, 175744–175757. [CrossRef]
99. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Aggarwal, S.; Kumar, N.; Choo, K.K.R. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Comput. Secur.* **2019**, *85*, 288–299. [CrossRef]

100. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220. [CrossRef]
101. Gao, J.; Agyekum, K.O.-B.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *IEEE Internet Things J.* **2020**, *7*, 4278–4291. [CrossRef]
102. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2019**, *6*, 1495–1505. [CrossRef]
103. Li, W.; Guo, H.; Nejad, M.; Shen, C.C. Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. *IEEE Access* **2020**, *8*, 181733–181743. [CrossRef]
104. Ying, Z.; Ma, M.; Yi, L. BAVPM: Practical Autonomous Vehicle Platoon Management Supported by Blockchain Technique. In Proceedings of the ICITE 2019: The 4th IEEE International Conference on Intelligent Transportation Engineering, Singapore, 5–7 September 2019.
105. Philip, A.O.; Saravanaguru, R.A.K. Multisource traffic incident reporting and evidence management in Internet of Vehicles using machine learning and blockchain. *Eng. Appl. Artif. Intell.* **2023**, *117*, 105630. [CrossRef]
106. Gasmi, R.; Hammoudi, S.; Lamri, M.; Harous, S. Recent Reinforcement Learning and Blockchain Based Security Solutions for Internet of Things: Survey. *Wirel. Pers. Commun.* **2023**, *132*, 1307–1345. [CrossRef]
107. Alahmadi, R.Y. Applications of Artificial Intelligence in Transportation. *Int. J. Adv. Res. Eng. Technol. (IJARET)* **2020**, *11*, 1074–1083. [CrossRef]
108. Saravanan, R.; Sujatha, P. A State of Art Techniques on Machine Learning Algorithms: A Perspective of Supervised Learning Approaches in Data Classification. In Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018), Madurai, India, 14–15 June 2018.
109. Sutton, R.S.; Barto, A.G. *Reinforcement Learning: An Introduction*; MIT Press: Cambridge, MA, USA, 1998; ISBN 0-262-19398-1.
110. Barto, A.G. Reinforcement Learning: Connections, Surprises, Challenges. *AI Mag.* **2019**, *40*, 3–96. [CrossRef]
111. Król, A. The Application of the Artificial Intelligence Methods for Planning of the Development of the Transportation Network. *Transp. Res. Procedia* **2016**, *14*, 4532–4541. [CrossRef]
112. Doğan, E.; Akgüngör, A.P. Forecasting highway casualties under the effect of railway development policy in Turkey using artificial neural networks. *Neural Comput. Appl.* **2013**, *22*, 869–877. [CrossRef]
113. Akg, A.P.; Doğan, E. An artificial intelligent approach to traffic accident estimation: Model development and application. *Transport* **2009**, *24*, 135–142. [CrossRef]
114. Azhar, A.; Rubab, S.; Khan, M.M.; Bangash, Y.A.; Alshehri, M.D.; Illahi, F. Detection and prediction of traffic accidents using deep learning techniques. *Clust. Comput.* **2023**, *26*, 477–493. [CrossRef]
115. Santos, D.; Saias, J.; Quaresma, P.; Nogueira, V.B. Machine learning approaches to traffic accident analysis and hotspot prediction. *Computers* **2021**, *10*, 157. [CrossRef]
116. Dia, H. An Object-Oriented Neural Network Approach to Short-Term Trac Forecasting. *Eur. J. Oper. Res.* **2001**, *131*, 253–261. [CrossRef]
117. Yanglong, S.; Sun, Y.; Lin, Y.; Tang, Y. A Reinforcement Learning-based Routing Protocol in VANETs. 2017. Available online: https://www.researchgate.net/publication/321508587 (accessed on 29 October 2024).
118. Wen, S.Y.; Li, Y. Fastest complete vehicle routing problem using learning multiple ant colony algorithm. *Adv. Mater. Res.* **2011**, *217–218*, 1044–1049. [CrossRef]
119. Dai, Y.; Xu, D.; Lu, Y.; Maharjan, S.; Zhang, Y. Deep Reinforcement Learning for Edge Caching and Content Delivery in Internet of Vehicles. In Proceedings of the 2019 IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 11–13 August 2019.
120. Liu, J.; Ahmed, M.; Mirza, M.A.; Khan, W.U.; Xu, D.; Li, J. RL/DRL Meets Vehicular Task Offloading Using Edge and Vehicular Cloudlet: A Survey. *IEEE Internet Things J.* **2022**, *9*, 8315–8338. [CrossRef]
121. Mase, J.M.; Chapman, P.; Figueredo, G.P.; Torres, M.T. A Hybrid Deep Learning Approach for Driver Distraction Detection. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 21–23 October 2020.
122. Mansourian, P.; Zhang, N.; Jaekel, A.; Zamanirafe, M.; Kneppers, M. Anomaly Detection for Connected Autonomous Vehicles Using LSTM and Gaussian Naïve Bayes. In *Wireless and Satellite Systems Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Springer: Cham, Switzerland, 2023; pp. 31–43. [CrossRef]
123. Wang, Q.; Yang, K. Privacy-Preserving Data Fusion for Traffic State Estimation: A Vertical Federated Learning Approach. 2024. Available online: http://arxiv.org/abs/2401.11836 (accessed on 29 October 2024).
124. Natarajan, R.; Ranjith, C.P.; Mohideen, M.K.; Gururaj, H.L.; Flammini, F.; Thangarasu, N. Utilizing a machine learning algorithm to choose a significant traffic identification system. *Int. J. Inf. Manag. Data Insights* **2024**, *4*, 100218. [CrossRef]
125. Chen, Y.; Lv, Y.; Wang, X.; Li, L.; Wang, F.Y. Detecting traffic information from social media texts with deep learning approaches. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 3049–3058. [CrossRef]
126. Dia, H.; Rose, G. Development and evaluation of neural network freeway incident detection models using field data. *Transp. Res. Part C Emerg. Technol.* **1997**, *5*, 313–331. [CrossRef]
127. Theofilatos, A.; Yannis, G.; Kopelias, P.; Papadimitriou, F. Predicting Road Accidents: A Rare-events Modeling Approach. *Transp. Res. Procedia* **2016**, *14*, 3399–3405. [CrossRef]

128. Gu, Y.; Qian, Z.; Chen, F. From Twitter to detector: Real-time traffic incident detection using social media data. *Transp. Res. Part C Emerg. Technol.* **2016**, *67*, 321–342. [CrossRef]
129. Huang, W.; Song, G.; Hong, H.; Xie, K. Deep architecture for traffic flow prediction: Deep belief networks with multitask learning. *IEEE Trans. Intell. Transp. Syst.* **2014**, *15*, 2191–2201. [CrossRef]
130. Lv, Y.; Duan, Y.; Kang, W.; Li, Z.; Wang, F.Y. Traffic Flow Prediction with Big Data: A Deep Learning Approach. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 865–873. [CrossRef]
131. Wu, Y.; Tan, H.; Qin, L.; Ran, B.; Jiang, Z. A hybrid deep learning based traffic flow prediction method and its understanding. *Transp. Res. Part C Emerg Technol.* **2018**, *90*, 166–180. [CrossRef]
132. More, R.M.A. Road Traffic Prediction and Congestion Control using Artificial Neural Network. In Proceedings of the 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, 19–21 December 2016.
133. Jiang, H.; Zou, Y.; Zhang, S.; Tang, J.; Wang, Y. Short-Term Speed Prediction Using Remote Microwave Sensor Data: Machine Learning versus Statistical Model. *Math. Probl. Eng.* **2016**, *2016*, 9236156. [CrossRef]
134. Angelica, S.; Panagiotis, G.; Yannis, P. Incident Detection Using Data from Social Media. In Proceedings of the IEEE ITSC 2017: 20th International Conference on Intelligent Transportation Systems: Mielparque Yokohama in Yokohama, Kanagawa, Japan, 16–19 October 2017.
135. Park, J.T.; Shin, C.Y.; Baek, U.J.; Kim, M.S. Fast and Accurate Multi-Task Learning for Encrypted Network Traffic Classification. *Appl. Sci.* **2024**, *14*, 3073. [CrossRef]
136. Buhrmester, V.; Münch, D.; Arens, M. Analysis of Explainers of Black Box Deep Neural Networks for Computer Vision: A Survey. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 966–989. [CrossRef]
137. Lee, J.; Sohn, S.Y. Recommendation system for technology convergence opportunities based on self-supervised representation learning. *Scientometrics* **2021**, *126*, 1–25. [CrossRef]
138. Kim, K.; Jung, S.; Hwang, J. Technology convergence capability and firm innovation in the manufacturing sector: An approach based on patent network analysis. *R D Manag.* **2019**, *49*, 595–606. [CrossRef]
139. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C.M. Blockchain and Machine Learning for Communications and Networking Systems. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1392–1431. [CrossRef]
140. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Gener. Comput. Syst.* **2021**, *117*, 328–337. [CrossRef]
141. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhang, Y. An Autonomous Lane-Changing System with Knowledge Accumulation and Transfer Assisted by Vehicular Blockchain. *IEEE Internet Things J.* **2020**, *7*, 11123–11136. [CrossRef]
142. 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]
143. Wang, N.; Yang, W.; Wang, X.; Wu, L.; Guan, Z.; Du, X.; Guizani, M. A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. *Digit. Commun. Netw.* **2024**, *10*, 126–134. [CrossRef]
144. Wang, Q.; Ji, T.; Guo, Y.; Yu, L.; Chen, X.; Li, P. TrafficChain: A Blockchain-Based Secure and Privacy-Preserving Traffic Map. *IEEE Access* **2020**, *8*, 60598–60612. [CrossRef]
145. Wang, S.; Sun, S.; Wang, X.; Ning, Z.; Rodrigues, J.J.P.C. Secure Crowdsensing in 5G Internet of Vehicles: When Deep Reinforcement Learning Meets Blockchain. *IEEE Consum. Electron. Mag.* **2021**, *10*, 72–81. [CrossRef]
146. Ning, Z.; Sun, S.; Wang, X.; Guo, L.; Guo, S.; Hu, X. Blockchain-Enabled Intelligent Transportation Systems: A Distributed Crowdsensing Framework. *IEEE Trans. Mob. Comput.* **2022**, *21*, 4201–4217. [CrossRef]
147. Meese, C.; Chen, H.; Asif, S.A.; Li, W.; Shen, C.C.; Nejad, M. BFRT: Blockchained Federated Learning for Real-time Traffic Flow Prediction. In Proceedings of the 22nd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGrid 2022, Taormina, Sicily, Italy, 16–19 May 2022; pp. 317–326. [CrossRef]
148. Alam, I.; Kumar, S.; Kumar, M.; Kashyap, P.K.; Kashyap, K. Blockchain Based Intelligent Incentive Enabled Information Sharing Scheme in Future Generation IoV Networks. 2021. Available online: https://assets-eu.researchsquare.com/files/rs-714669/v1_covered.pdf?c=1631874048 (accessed on 29 October 2024).
149. Rajan, D.; Eswaran, P.; Srivastava, G.; Ramana, K.; Iwendi, C. Blockchain-based multi-layered federated extreme learning networks in connected vehicles. *Expert. Syst.* **2023**, *40*, e13222. [CrossRef]
150. Ferrag, M.A.; Maglaras, L. DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1285–1297. [CrossRef]
151. He, Y.; Huang, K.; Zhang, G.; Yu, F.R.; Chen, J.; Li, J. Bift: A Blockchain-Based Federated Learning System for Connected and Autonomous Vehicles. *IEEE Internet Things J.* **2022**, *9*, 12311–12322. [CrossRef]
152. Pokhrel, S.R.; Choi, J. Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges. *IEEE Trans. Commun.* **2020**, *68*, 4734–4746. [CrossRef]
153. Li, Q.; Wang, W.; Zhu, Y.; Ying, Z. BOppCL: Blockchain-Enabled Opportunistic Federated Learning Applied in Intelligent Transportation Systems. *Electronics* **2024**, *13*, 136. [CrossRef]
154. Asad, M.; Shaukat, S.; Javanmardi, E.; Nakazato, J.; Bao, N.; Tsukada, M. Secure and Efficient Blockchain-Based Federated Learning Approach for VANETs. *IEEE Internet Things J.* **2024**, *11*, 9047–9055. [CrossRef]
155. Jiang, X.; Yu, F.R.; Song, T.; Ma, Z.; Song, Y.; Zhu, D. Blockchain-Enabled Cross-Domain Object Detection for Autonomous Driving: A Model Sharing Approach. *IEEE Internet Things J.* **2020**, *7*, 3681–3692. [CrossRef]

156. Gandhi, G.M.; Chaudhary, S. Artificial Intelligence Integrated Blockchain For Training Autonomous Cars. In Proceedings of the 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 14–15 March 2019.
157. Chai, H.; Leng, S.; Chen, Y.; Zhang, K. A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3975–3986. [CrossRef]
158. 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]
159. Fu, Y.; Yu, F.R.; Li, C.; Luan, T.H.; Zhang, Y. Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles. *IEEE Wirel. Commun.* **2020**, *27*, 197–203. [CrossRef]
160. Ahamed, N.N.; Karthikeyan, P. A Reinforcement Learning Integrated in Heuristic search method for self-driving vehicle using blockchain in supply chain management. *Int. J. Intell. Netw.* **2020**, *1*, 92–101. [CrossRef]
161. Lin, Y.; Gao, Z.; Du, H.; Kang, J.; Niyato, D.; Wang, Q. DRL-Based Adaptive Sharding for Blockchain-Based Federated Learning. *IEEE Trans. Commun.* **2023**, *71*, 5992–6004. [CrossRef]
162. Qian, Y.; Jiang, Y.; Hu, L.; Hossain, M.S.; Alrashoud, M.; Al-Hammadi, M. Blockchain-based privacy-aware content caching in cognitive internet of vehicles. *IEEE Netw.* **2020**, *34*, 46–51. [CrossRef]
163. Shen, Z.; Wang, Y.; Wang, H.; Liu, P.; Liu, K.; Liu, M. Privacy-protecting predictive cache method based on blockchain and machine learning in Internet of vehicles. *Veh. Commun.* **2024**, *47*, 100771. [CrossRef]
164. Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S.; Zhang, Y. Deep Reinforcement Learning and Permissioned Blockchain for Content Caching in Vehicular Edge Computing and Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4312–4324. [CrossRef]
165. Ashfaq, T.; Khalid, M.I.; Ali, G.; Affendi, M.E.; Iqbal, J.; Hussain, S.; Ullah, S.S.; Yahaya, A.S.; Khalid, R.; Mateen, A. An Efficient and Secure Energy Trading Approach with Machine Learning Technique and Consortium Blockchain. *Sensors* **2022**, *22*, 7263. [CrossRef]
166. Mao, D.; Wang, F.; Hao, Z.; Li, H. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1627. [CrossRef]
167. Kim, S.; Ibrahim, A.S. Byzantine-Fault-Tolerant Consensus via Reinforcement Learning for Permissioned Blockchain-Empowered V2X Network. *IEEE Trans. Intell. Veh.* **2023**, *8*, 172–183. [CrossRef]
168. Moulahi, T.; Jabbar, R.; Alabdulatif, A.; Abbas, S.; El Khediri, S.; Zidi, S.; Rizwan, M. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert. Syst.* **2022**, *40*, e13103. [CrossRef]
169. Mazlan, A.A.; Daud, S.M.; Sam, S.M.; Abas, H.; Rasid, S.Z.A.; Yusof, M.F. Scalability Challenges in Healthcare Blockchain System-A Systematic Review. *IEEE Access* **2020**, *8*, 23663–23673. [CrossRef]
170. Sajid, M.B.E.; Ullah, S.; Javaid, N.; Ullah, I.; Qamar, A.M.; Zaman, F. Exploiting Machine Learning to Detect Malicious Nodes in Intelligent Sensor-Based Systems Using Blockchain. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 7386049. [CrossRef]
171. Ye, X.; Li, M.; Si, P.; Yang, R.; Sun, E.; Zhang, Y. Blockchain and MEC-Assisted Reliable Billing Data Transmission over Electric Vehicular Network: An Actor-Critic RL Approach. Emerging Technologies & Applications. *China Commun.* **2021**, *18*, 279–296.
172. Vangala, A.; Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Park, Y. Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems. *IEEE Sens. J.* **2021**, *21*, 15824–15838. [CrossRef]
173. Philip, O.A.; Saravanaguru, R.A.K. Blockchain based Framework for Investigating Pedestrian and Cyclist Hit and Run Cases in the Internet of Vehicles Era. In Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021, Palladam, India, 11–13 November 2021; pp. 110–118. [CrossRef]