sustainability

MDPI

Review

Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review

Muhammad Saad, Muhammad Khalid Khan and Maaz Bin Ahmad *

Karachi Institute of Economics and Technology (KIET), College of Computing and Information Sciences (CoCIS), Karachi 75190, Pakistan; muhammadsaad55@live.com (M.S.); khalid.khan@kiet.edu.pk (M.K.K.)
* Correspondence: maaz@kiet.edu.pk; Tel.: +92-33-3526-4960

Abstract: This systematic literature review provides an extensive categorization of the blockchain-enabled applications across the domain of vehicular ad hoc networks (VANETs). Within the paradigm of distributed ledger technology (DLT), the communication models and practices for VANETs have been revolutionized. An analytical review and a survey were conducted to explore the advancements of blockchain and VANETs. The techniques, limitations, and advantages of blockchain deployment in VANETs are discussed for the effective implementation of a decentralized network. To this end, 68 studies were selected on the basis of the procedural steps to provide a comprehensive overview of blockchain and the smart contracts in VANETs. In particular, a decentralized communication model is also proposed for the advanced implementation of blockchain in VANETs. Researchers and practitioners are being attracted to these technologies for applications for various industrial sectors. Therefore, this study also emphasizes the identification of any blockchain-related open issues for future prospects. The comprehension of blockchain applications for the Internet of Vehicles (IoV) is also explored in order to fill the research gap on advanced communication networks across the Internet of Things.

Keywords: blockchain; distributed ledger technology; Internet of Things; Internet of Vehicles; machine-to-machine; mobile ad hoc networks; roadside unit; software-defined network; vehicular ad hoc networks

Citation: Saad, M.; Khan, M.K.; Ahmad, M.B. Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review. *Sustainability* **2022**, *14*, 3919. https://doi.org/10.3390/su14073919

Academic Editors: Efthimios Bothos, Panagiotis Georgakis, Babis Magoutas and Michiel de Bok

Received: 16 January 2022
Accepted: 15 February 2022
Published: 25 March 2022

1. Introduction

A blockchain is the extended form of a decentralized network that is responsible for recording transactional data or information in the form of blocks that are sequentially linked to each other. The architecture of blockchain makes it difficult to tamper with and difficult to modify information without having a consensus mechanism. In 2008, blockchain technology emerged with the revolution in digital currency known as "bitcoin". The blockchain network provides immutability, security, transparency, and reliability. Therefore, the inherent characteristics of blockchain technology are being recognized by practitioners for their implementation in different sectors. The integration of blockchain technology with other domains helps to overcome the privacy and security limitations by providing a tamper-proof network system. For example, an intelligent transportation system heavily relies on information sharing across multiple entities. The open-channel information sharing presents several security issues, such as denial-of-service attack (DDoS), man-in-the-middle attacks, etc. The application of blockchain technology can make this information tamper-proof, transparent, and reliable. Similarly, it can be applied to the Internet of Things (IoT) and the Internet of Vehicles (IoV), as well as to other domains where secure data transmission is required.

In recent years, several studies, discussions, and projects regarding blockchain have been recognized by researchers. The concept of blockchain is based on distributed ledger technology (DLT), which delivers a radical change to the existing trust model in order

to overcome the limitations of centralized systems, and which provides an efficient data-trading mechanism. The conventional business processes are highly dependent on centralized systems (e.g., banks) to develop trust across the participants [1,2]. However, the centralized system always remains vulnerable to multiple attacks. Researchers have published several studies with the aim of mitigating the artificial alterations to the system using blockchain. The blockchain architecture that is based on trust is proposed by researchers to prevent security attacks, including Sybil, DDoS, and MAC layer attacks [3]. The challenge of security is one of the key areas of research in the realm of blockchain and its applications. Business operations and activities can be made secure, transparent, and immutable by using the emerging blockchain technology. The immutable, decentralized, and distributed characteristics of blockchain also bring innovation to other technologies as composite uses of DLT [4].

Blockchain is considered to be a connected chain of sequential blocks. Each individual block represents the record of a digital transaction that is secured using cryptographic techniques. A peer-to-peer network (P2P) assists in creating the blocks, along with their validation, and the consensus is achieved by having majority votes in a blockchain network. This method provides a transparent, secure, and trustworthy model of blockchain where the transactions between the nodes are concerned. DLT has emerged to automate business processes and operations without depending on a centralized third party [1,4]. The smart implementation of blockchain in healthcare is also gaining attention for the achievement of a decentralized system for remote patient monitoring [5], tamper-proof patient-data-storage management [6], and to preserve privacy in the healthcare sector [7]. Practitioners have also implemented the concepts of blockchain in various domains to omit the centralized systems by using distributed systems, such as in trade finance [8], healthcare, electronic voting [9], farming, and the insurance sector [10,11], in order to depict the significance of blockchain.

The vehicular ad hoc network (VANET) is one of the major components of intelligent transportation systems (ITSs). Therefore, the current research always takes care of VANETs in realm of intelligent transportation systems. The smart implementation of VANETs is imperative, and it offers several advantages for different industries. For example, oil marketing companies (OMCs) are eager to have a digitalized system to keep tabs on their fleets and drivers, along with the product movement. Similarly, logistics companies need to have an intelligent transportation system to minimize delays and maximize the performance of deliveries. The smart implementation of VANETs has the potential to take care of the needs of today's industries. The further applications of VANETs, with respect to the current era, are supply chain management, solid waste management, autonomous transportation, etc. The further detailed applications are discussed later in this review.

VANETs have gained significant importance in research areas since the last decade because of their distinctive characteristics, such as mobility, advance topology, and wireless connected vehicular technology. VANETs are being recognized by both the industry and academia for their implementation on larger scales [12]. In the VANETs, the communication across vehicles and the monitoring office plays a significant role. The objective of the dynamic vehicular network is to precisely circulate the notification of events, such as weather alerts, road blockages, and accidents, as well as emergencies such as roll overs, etc. However, there are limitations of the vehicular network for passing critical messages in the specified radius under a dynamic vehicular environment because of the presence of suspicious vehicles. The security issues of the traditional vehicular network are ultimately exposed. The research related to intelligent transportation systems determines and classifies the attacks and threats related to VANETs by period [13]. The malevolent node can transmit false information by disseminating other important real-time messages. This malicious behavior of nodes can result in the loss of lives and assets. Thus, this is identified as the greatest challenge for the VANET. The decentralized architecture of VANETs is proposed in this review to preserve security and privacy.

Extensive efforts have been applied to determine blockchain and their applications across various domains. This study proceeds from technical discussions on the feasibility of DLT-enabled IoT [14,15] applications [16], business processes, and even security issues [17], as well as other domains [18]. The information was gathered from 68 articles, including the impact factor publishers, IEEE, Springer, Elsevier, MDPI, and ACM, from 2016 to early 2022. This study classifies articles on the basis of the evolution of blockchain from the early stages until the present date. This study adopted methods to precisely outline the relationships between the challenges and the applied techniques.

The contemporary literature on blockchain applications in VANETs is diversified with respect to particular areas [19,20]. This study further highlights the significant research areas for practitioners with unorganized comprehensions of the article distribution. The research gap is identified across earlier studies on blockchain in the realm of VANETs because of the lack of peer-reviewed articles that could play significant roles in the extensive research. The first blockchain-enabled IoT literature survey was performed in [20], which covered up to 2016, with a peer-reviewed process in which 18 use cases and 35 examples were found and discussed in detail with regard to the blockchain-enabled IoT. The researchers contributed extensively to the integration of the IoT with blockchain and suggest subsequent research for the advancement of blockchain-enabled IoT applications.

This review culminates in the integration of blockchain and the IoT for a particular domain of VANETs, with its practical implementation unlike those in the existing general reviews. The articles on blockchain with other domains are rare, and there are hardly any available before 2019. Therefore, the earlier research studies are not sufficient to provide a precise overview of the integration. Therefore, an extensive literature review is targeted in this study because of the agile evolution of the IoT and the related domains, such as blockchain for the IoV and VANETs.

The existing literature on blockchain-enabled VANETs mainly focuses on the identification of the use cases, methods, and the safety and security aspects of intelligent transportation systems. However, this study is not only limited to the classification of studies with respect to use cases, privacy, and security, but it also provides a collaborative decentralized architecture for VANETs. The proposed blockchain-enabled architecture helps to achieve the efficient collaboration of entities, such as vehicles, RSUs, and cloud-based infrastructure, which is extended to the composite use of the techniques, in contrast to the existing studies. This study also places an emphasis on the identification of the research domains and methods for transportation industry and fleet owners to maximize their throughputs and improve their performances. For example, timely deliveries are critical for logistics, supply chain management, and oil marketing companies. Similarly, in the healthcare sector, the timely arrival of ambulances and the movement of medical equipment in pandemic-like situations is imperative. The major contributions of this study are the classifications and compositions of the techniques, the identification of the research areas, and the provision of a blockchain-enabled framework for a secure, transparent, and decentralized network using the collaborative efforts of the entities. The following table (Table 1) is used to provide a comparison of this study with the existing literature reviews in the realm of blockchain-enabled IoT technologies.

Table 1. Comparison of blockchain-enabled VANETs with the existing literature.

Studies	Composite Use of Methods to Improve Vehicular Network by Employing Blockchain	Provision of Blockchain-Enabled Decentralized Framework	Provision of Safety and Security for Intelligent Transportation System	Identification of Research Domains When Blockchain Meets IoT/VANETs	Identification of Use Cases for the Implementation of Blockchain-Enabled IoT/VANETs
[3] (Álvares et al., 2021)	✔	×	✔	✔	×
[13] (Wan et al., 2020)	×	×	×	×	✔
[20] (Lo et al., 2019)	✔	×	×	✔	✔
[21] (Conoscenti et al., 2016)	×	×	×	✔	✔
[22] (Iqbal et al., 2021)	✔	×	✔	×	×
[23] (Casino et al., 2019)	×	×	✔	✔	✔
[24] (Shen & Pena-Mora, 2018)	✔	✔	×	×	✔
Blockchain Enabled VANETs	✔	✔	✔	✔	✔

This study provides a more comprehensive classification of the blockchain-related domains and challenges. The advancement of blockchain, with its unique characteristics, has improved business operations [25,26], immutability, and trust across the participating nodes. The integration of the IoT and the IoV with blockchain is targeted to provide a decentralized architecture for VANETs. The comprehension of blockchain applications for the IoV is also explored in order to fill the research gap on the advance communication networks across the Internet of Things.

The explicit questions proposed in this study are related to identifying the needs and connections between the existing studies and the possibilities for future research.

The targeted research questions that are answered in this review are as follows:

RQ1: *What are major research areas when blockchain meets VANETs?*
RQ2: *How is blockchain used to improve VANETs through the employment of different research methodologies?*
RQ3: *What are the existing IoT and VANET challenges that can be addressed by employing blockchain technology?*
RQ4: *What are the limitations and challenges when blockchain meets with multiple domains, and which techniques and models can be employed to address these limitations?*

The systematic literature review procedure was adopted to classify the correlated issues that arise when blockchain meets VANETs, and to answer the research questions categorically. This study escalates the categorization of blockchain-enabled applications by performing a systematic review on modern studies. This study outlines the research gap between blockchain and the IoT by employing a blockchain in VANETs. This paper contributes towards blockchain applications in the IoT, and especially in VANETs, through an extensive analysis of the research articles. The several research areas and gaps are

highlighted in the results of this literature analysis for the prospective articles. The analysis of the literature review is sorted as follows: Section 2 defines the backgrounds of the technologies, such as DLT, blockchain, protocols/contracts, the IoT, the industrial IoT (IIoT), machine-to-machine communication (M2M), and VANETs and their evolution towards the IoV. Section 3 explains the procedure for conducting the review, the methodology, and the procedural steps. Sections 4–8 highlight the results, the descriptive corpus, and the findings from the literature analysis. Section 9 presents a discussion, and the review is concluded in Section 10.

2. Background

2.1. Distributed Ledger Technology (DLT)

DLT has gained in popularity among researchers since 2008, and it is being deployed in various sectors, for example, in financial services, energy, the supply chain, the IoT, the IIoT, and VANETs. Blockchain technology is based on DLT, which helps it to become decentralized, rather than having a centralized dependency. Blockchain enables organizations to eliminate trust and privacy issues by emphasizing security and privacy-preserving techniques. Blockchain can also be referred to as "distributed databases" that are managed to use an immutable hash tree that cannot be altered or modified in order to ensure security. In particular, the blocks represent records or data transactions in the blockchain. Every block has its own hash value, which creates the links between the different blocks.

The role of DLT in blockchain-enabled VANETs is critical to the achievement of efficient data trading across entities such as vehicles, RSUs, and infrastructure. It facilitates the avoidance of the dependency of entities on third parties by having a distributed shared ledger that consists of information such as traffic, incidents, collisions, weather, etc. The DLT also provides a trusted handshaking mechanism across the entities. This is an inherent characteristic of blockchain that is used to avoid malicious intrusion and to share data across trusted entities. The decentralized architecture of VANETs is proposed later in this study which is based on DLT, where entities, such as vehicles, RSUs, and clouds, store the perceived information in the form of a shared ledger. Similarly, Section 2.7. supports the use of DLT in blockchain-enabled VANETs by means of vehicle-to-everything communication.

The blockchain offers a variety of features for security and a distributed architecture that can be used for contact tracing. A consensus mechanism is important to achieving the integrity and consistency of the transactions within a chain. The common consensus mechanisms are proof of work (POW), proof of stake, and the direct acyclic graph. Bitcoin uses proof of work as the consensus mechanism in order to compete with computing resources. On the other hand, proof of stake is used for the coin's age competition rather than the computing power. The expansion of POW in the realm of blockchain-enabled VANETs is discussed later in this literature.

2.2. Blockchain

The analogy of blockchain is self-explanatory as it refers to a sequential chain of blocks. The individual block is responsible for holding the information on the transactions as records and as the address of the succeeding block. The header and the data of each block are encoded using a hashing mechanism to ensure the data integrity. Similarly, the blocks create a network that consists of participating nodes that are responsible for the transactions. Each participating node of the blockchain network copies the chain in its storage in order to have a complete digital ledger. The concept of blockchain is similar to Google spread sheets, where a document is distributed across multiple participants, and a trail record is maintained with respect to the changes.

There are three major types of blockchain: public, private, and federated blockchain. The public, or the permission less, blockchain is used where the participants are free to participate in the consensus mechanism and to avail the benefits accordingly. On the other hand, the private, or permissioned, blockchain is used for a small number of participants, where only the verified participants can participate in the consensus. The federated, or

consortium, blockchain inherits the properties of both the public and private blockchain, and it has therefore gained accordingly in popularity among researchers.

In ref. [27], Nakamoto proposes the decentralized system for digital currency known as "bitcoin". The idea of decentralization provides a mechanism for performing transactions and exchanging messages without depending on third parties or central authorities. The proposed architecture eliminates the single point of the failure mechanism associated with traditional centralized systems. Blockchain is based on DLT and consists of growing sequential blocks. The individual block not only holds the transactional information, but it also stores the link of the successive block [28]. The participating nodes also hold the copy of the chain consisting of the transactional information, known as "the ledger", with mutual coordination in a network. The DLT provides a trustless mechanism without relying heavily on traditional centralized systems. The P2P network builds trust among the participating nodes in a network having a shared ledger.

In the IoT context, the decentralized system and schemes may provide a baseline of trust without relying on centralized systems [29]. However, the blockchain could further communicate between the IoT nodes in order to improve traceability and message passing [30]. This further automates the operations and the communication across the sensors, actuators, and devices in the realm of the IoT. There are different variants of blockchain that can be applied in particular areas of the IoT in order to achieve this decentralized tendency.

2.3. Smart Contracts

A "smart contract" is also referred to as "an agreement between the participating nodes to complete the transactions" [31]. Sabzo proposed this concept in 1996, which is defined as the "computerized agreement between nodes to perform transactions". This mechanism builds trust among the nodes on the basis of certain conditions outlined in the contract to act accordingly [32]. The immutability in the blockchain and the smart contracts outperform the traditional contracts between the participants. This helps to execute transactions by eliminating the intermediaries by using the permissioned blockchain [33]. Smart contracts are also referred to as "programmable scripts", which can be deployed across the blockchain network with addresses to execute the functionalities [34]. Smart contracts are important for the data-centric executions in a network, especially when the blockchain meets the IoT and other particular domains.

Blockchain-enabled applications can reap benefits with the deployment of smart contracts. The rules and regulations can be defined for communication across the IoT objects. The blockchain network helps to transfer the contract to each participating node. The execution of the contract is triggered when a certain condition in the network is met [35]. This mechanism also eliminates the interference of other entities [36].

The emerging DLT is also being opted by well-known organizations, such as Maersk and IBM. They recently announced the adoption of blockchain technology for commercial pilot projects in order to achieve the smooth tracking of shipments, finance trading, and the automation of their other business operations. By using smart contracts, the traditional manual commercial processes can be eliminated [37]. Blockchain that uses smart contracts reduce intermediaries and the costs incurred for transactions, and they further improve trading and the automation of business operations.

The challenges of contracts, such as transaction ordering, contract vulnerabilities, and call stacks, are recognized by practitioners as open issues for future research. The validation and verification issues were also highlighted by Vaidya in 2020. These issues need to be addressed when the integration of blockchain with other domains is considered [38]. However, this mechanism still requires a systematic approach and mechanism in order to address the challenges and limitations.

2.4. Internet of Things (IoT)

The blockchain and IoT technologies are being considered as the technologies of the next generation, or of the information era. The current research highlights that 75 billion objects, including industrial devices, will be connected by 2026. On the other hand, the limitations and challenges of IoT device handshaking, connectivity, security, data transmission, and storage are important and need to be addressed; the IoT network will collapse if is not able to obtain a stable platform. However, blockchain technology is gaining major attention from researchers for the achievement of state-of-the-art access control schemes using blockchain, such as the attribute-based access control scheme for security, privacy, and decentralization [39], and the data privacy and security mechanism for IoT-enabled devices [40].

The growing blockchain technology has a long way to go in terms of other technologies, such as artificial intelligence, machine learning, the IoT, and the data sciences. In the past few years, an escalation in the research, discussions, and projects with regard to the IoT has gained the attention of practitioners. The implementation of the IoT and the particular subdomains is being applied in the different industrial sectors mentioned in Figure 1. The concept of the IoT is based on connecting things that deliver radical change to the network model of trust between the nodes or devices to solve the pain points of the human–machine or M2M interfaces. The traditional operations rely heavily on the recording of manual data to promote trust among the nodes. However, the manual processes often lead to victimization in the forms of suspicious attacks and intentional modifications. The evolution of the IoT and its extensive applications require a rethinking of the design and architecture.

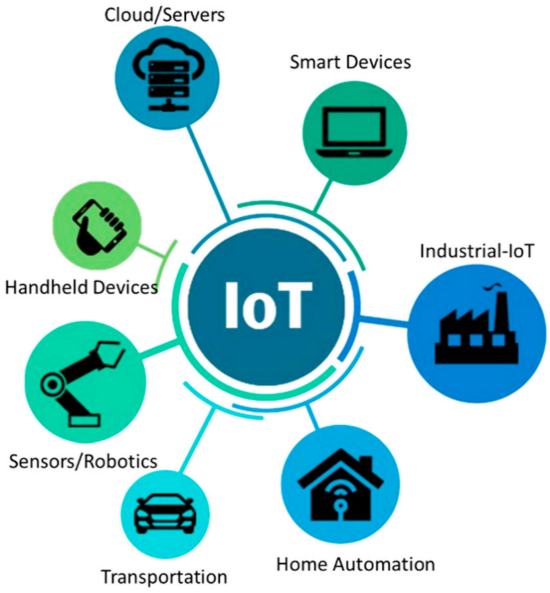

Figure 1. An overview of the IoT.

The advanced implementation of the IoT in the industrial sector is also referred to as the industrial Internet of Things (IIoT), where things are connected to wireless networks for data gathering and sharing. The IIoT has gained significant importance in different sectors and industries. The IIoT devices are also referred to as "actuators", "sensors", and "electronic chips". The IIoT works in a fashion in which things or sensors gather information from their surroundings, communicate with each other, and transmit over the air by using GSM/GPRS/LTE to drive meaningful information. There can be various applications of the IoT, e.g., home automation, fleet telematics, fuel chains, weather broadcasting, agriculture, general supply chains, etc. The industrial implementation of IoT devices automates and reinforces manufacturing, production, and industrial operations.

There are many applications of the IoT, or the IIoT, such as home automation, the Internet of Vehicles, fleet telematics, fuel telematics, digital card-based e-healthcare systems [41], smart car parking, etc. The IoT implementation in the industrial sector has led to the automation of the business operations and activities [21]. An overview of IIoT- and Industry-4.0-based applications is illustrated in Figure 2, which depicts the evolutions of the robotics, electronics, electricity, and mass production industries by the advanced implementation of the IoT.

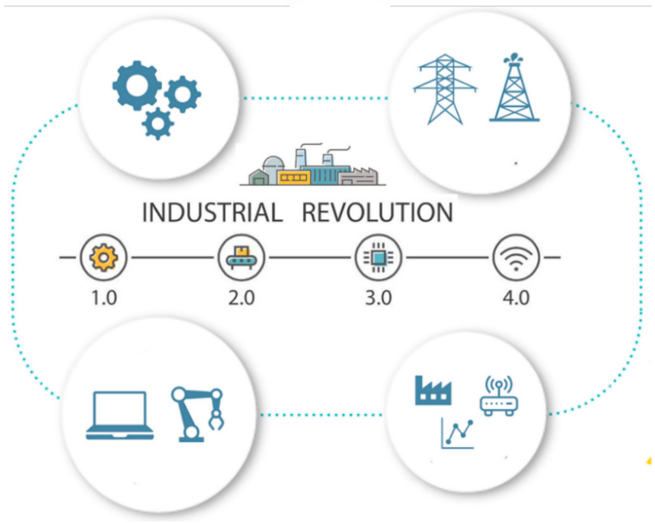

Figure 2. An overview of Industry 4.0 (mechanization, electricity, electronics, and the IoT).

The targets and estimates reveal that billions of devices will be connected in the coming years. The limitations and challenges of connectivity, security, and the cost of things in the IoT are the important factors for practitioners to consider when deploying blockchain technology in the IoT. MachNation forecasts that 75 billion devices will be connected by 2026, and that this will be directly proportional to the revenue, with an annual growth rate of 15%. The existing IoT solutions rely heavily on centralized management systems, but they will collapse when there are 75,000 billion devices wired for simultaneous connectivity. Therefore, decentralized architecture is required for the stability and scalability of IoT applications.

The IIoT infrastructure is designed in such a way that the actuators or sensors gather data from the surroundings and transmit it to the edge gateway in order to transit the raw data to the cloud, which further performs data-processing activities and derives meaningful information, as is illustrated in Figure 3.

2.5. Machine-to-Machine Communication (M2M)

M2M communication refers to technology that supports the data transmission and interaction of devices. This communication eliminates the human intervention in IIoT applications. M2M communication connects things, such as sensors, actuators, and objects, in order to gather information and transmit accordingly [42]. M2M communication provides a dynamic resource-sharing mechanism that allows IoT entities to share resources with each other by using artificial intelligence (AI), deep learning (DL), etc. It also provides advanced architecture for the smart communication of IoT devices with each other [43]. The ultramodern architecture is elaborated in Figure 4.

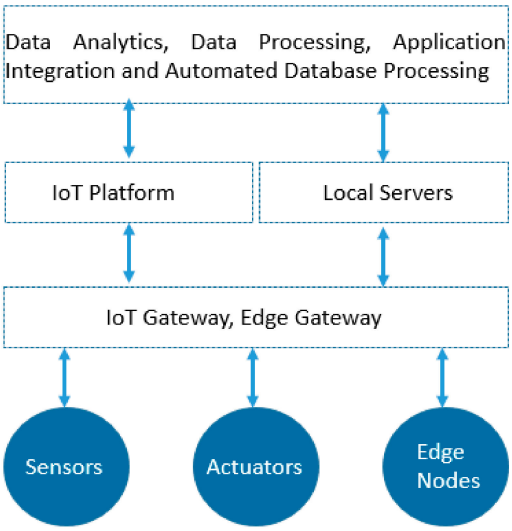

Figure 3. IIoT infrastructure and process diagram.

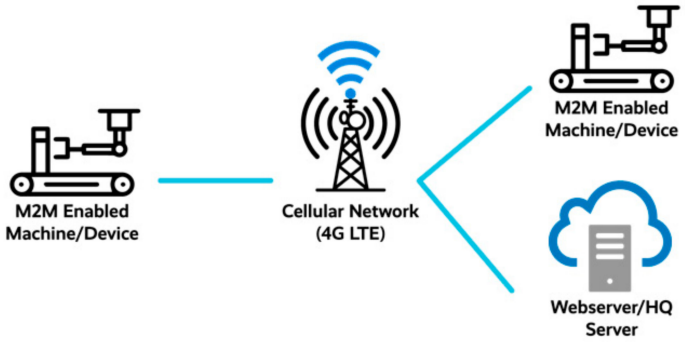

Figure 4. M2M communication and architecture.

2.6. Vehicular Ad Hoc Networks (VANETs)

VANETs introduce the network of self-organizing vehicles that act as mobile nodes. They confine the communication between vehicles and roadside units as V2V and V2R. They assists drivers in avoiding collisions, in picking the shortest route on the basis of traffic optimization, in identifying tolls and the nearest fuel stations, and in enhancing the safety of assets and lives [44]. They facilitate the communication of vehicles across the network for real-time data transmission. They improve the road safety mechanism and provide instant alerts or information in order to concern the authorities in cases of emergency situations, such as roll overs, accidents, etc. The existing architecture of VANETs also exposes vulnerabilities, such as data sniffing, impersonation, and ransomware attacks.

The applications related to VANETs are usually designed for the assistance of drivers and for the safety of assets. The emergency response system is studied in this review in order to enhance the safety and to assist drivers in cases of emergencies, for example, accidents, roll overs, fires, object collisions, and similar incidents. Real-time audio/video streaming is considered to be a major feature of surveillance applications, and it can be used to investigate and identify the real causes of incidents. VANET applications are time-critical applications because of the real-time transmission of messages across each vehicle or station for decision making.

2.7. Internet of Vehicles (IoV)

In the nascent studies, the vehicle receives environmental data and roadside information via a VANET [45]. The VANETs are defined as the subtypes of mobile ad hoc networks (MANETs). The vehicles act like nodes in the network. In the advanced stage, the VANET

evolves into the IoV, which promotes the interactions of vehicles with each other, or with surrounding units and humans. This phenomenon is similar to the evolution of M2M communication to the IoT. VANETs provide communication between vehicles, whereas the IoV connects the vehicles and humans within and around the vehicles. The IoV aggregates the actuators, vehicles, and other IoT devices to create a network system [46]. Cellular networks have evolved VANETs towards the IoV. Practitioners recognize the concept of the Internet of Vehicles because of its mobility through the use of GSM/LTE channels [47]. Figure 5 illustrates the communication architecture of VANETs in more detail.

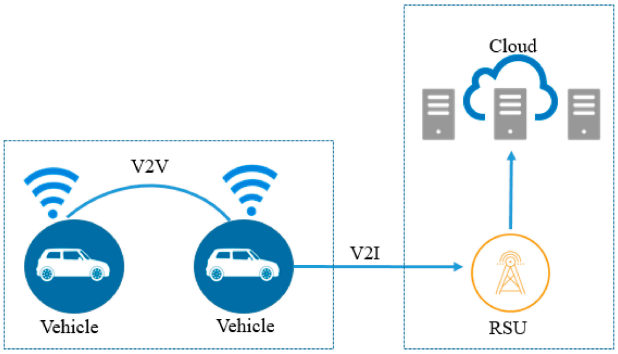

Figure 5. VANET communication and architecture.

In recent years, practitioners have been attracted to the growing technologies of the IoT. IoV, 5G, MQTT, and M2M technologies are being considered for implementation in time-critical systems. Vehicular sensor networks (VSNs) are considered to be the future of vehicular networks. VSNs not only ensure an unlimited power supply, but they are also endowed with low power consumption. Technological advancement has made fleet management more efficient. Still, there are a lot of issues for fleet managers to deal with when handling fleet telematics. With the increases in traffic and air pollution, there is an immense need for a secure and reliable intelligent transportation system (ITS) in order to facilitate fleet managers and drivers. The IoT sensors help by providing more awareness of the surroundings for the ITS. The vehicles are equipped with sensors for driver assistance, and the traffic lights and roadsides are mounted with cameras and sensors. Such a complex system can be handled well by 5G technology [47,48].

The IoV further facilitates the communication between human drivers and fleet monitoring staff for real-time decision making. The communication models in VANETs, such as V2V, V2I, V2R, etc., demonstrate the blockchain-enabled authentication schemes for VANETs [49]. The real-time communication of the Internet of Vehicles is bifurcated into five categories, which are presented in Figure 6.

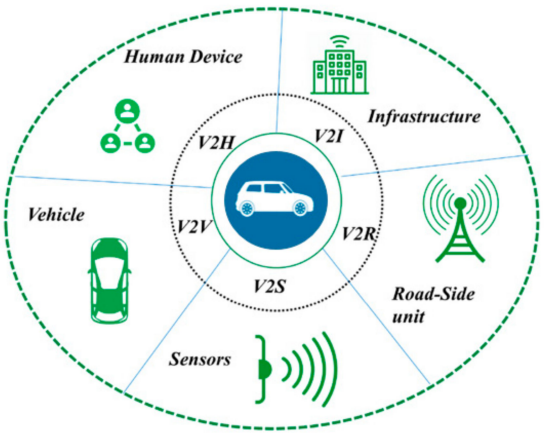

Figure 6. An overview of vehicle-to-everything communication.

2.7.1. Vehicle-to-Infrastructure (V2I) Communication

The V2I model supports the wireless communication across the RSUs and the supporting infrastructure.

2.7.2. Vehicle-to-Roadside Unit (V2R) Communication

The V2R communication model supports the wireless communication between vehicle and the RSUs to transmit information along the servers or the supporting infrastructure.

2.7.3. Vehicle-to-Sensor (V2S) Communication

V2S systems support the bi-directional communication between different kinds of sensors and onboard terminals for real-time insights. For example, the object detection sensors, the fuel level probes, and the load sensors can be connected to the terminal to provide accurate fuel level and distance information between the objects to avoid collision.

2.7.4. Vehicle-to-Vehicle (V2V) Communication

The V2V model supports the wireless communication across vehicles for sharing location data, and it consists of the speeds and coordinates. For example, V2V communication can be helpful in providing prior road blockage information to the respective on-route vehicles.

2.7.5. Vehicle-to-Human (V2H) Communication

The V2H model supports mobility and awareness for the nearest users, such as pedestrians, cyclists, and drivers. It further facilitates communication between the driver and the vehicle.

Cellular, or GSM/LTE/5G, technologies will make the above types of communication more reliable in the context of future research with regard to intelligent transportation. The blockchain-enabled reputation model is significant among the communication models. In reputation-enabled models, the provider reputation is validated before the storing of its data in the blockchain network [22]. The abovementioned composite communication types are also called "vehicle-to-everything (V2X)" communication.

2.8. Event-Driven Service-Oriented Architecture (EDSOA) for IoT

Service-oriented architecture (SOA) is used when there are heterogeneous devices and systems. The IoT also deals with heterogeneous devices. These are made by different manufacturers and follow different communication protocols. SOA provides technology and language independence. The further implementation of SOA with respect to the distributed systems has been evaluated by practitioners for the proposal of event-driven architecture. The EDSOA is being practiced in the field of the IoT to deal with real-time information. The request and response modes are processed by the service in the event-driven architecture [50], as is mentioned in Figure 7.

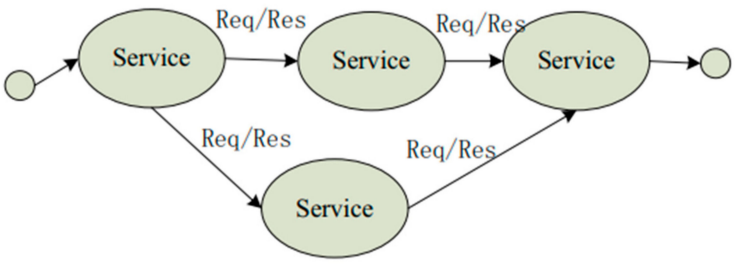

Figure 7. EDSOA service communication. Reprinted with permission from ref. [50]. Copyright Lan et al., 2015.

In traditional systems, the client/server approach is used for data communication. This process is time-consuming since the client must wait for the server to respond. The

traditional client/server approach has limitations for IoT-based real-time applications, such as vehicle tracking, router and journey management, and emergency response systems. The EDSOA has been analyzed by practitioners for VANETs for faster and more reliable communication across things.

3. Materials and Methods

The SLR was conducted according to the proposed guidelines of Kitchenham in [51]. The following steps were performed to answer the research questions: (1) Planning and conducting the review; (2) Inclusion/exclusion criteria; (3) Abstract and article examination; and (4) Results and descriptive analysis of the corpus.

3.1. Planning and Conducting the Review

This SLR was established to identify the relationship between the blockchain and the IoT towards the particular domain of VANETs. Since the emergence of blockchain technology, research studies, and the related works, practices, and standards related to blockchain, smart contracts, the IoT, and DLT are unfolding. We selected a period of six years (2016–2021 (extended to early 2022)) from which to adopt the most recent research work on blockchain-enabled VANETs. This study followed the research guidelines provided by Kitchenham in 2009 in [51] to develop the state-of-the-art replicable study. The articles from impact factor journals were targeted to maintain the quality of this study. We analyzed and explored the extant literatures on blockchain and VANETs. The search was applied on IEEE Xplore, Springer, Elsevier, MDPI, ACM, and Google Scholar, using the following search strings:

1. "Blockchain" <AND> "VANETS";
2. "Blockchain" <AND> "VANETS" <OR> "IoV" <OR> "Internet of Vehicles".

The step-by-step procedure for the literature searching and screening is demonstrated in Figure 8.

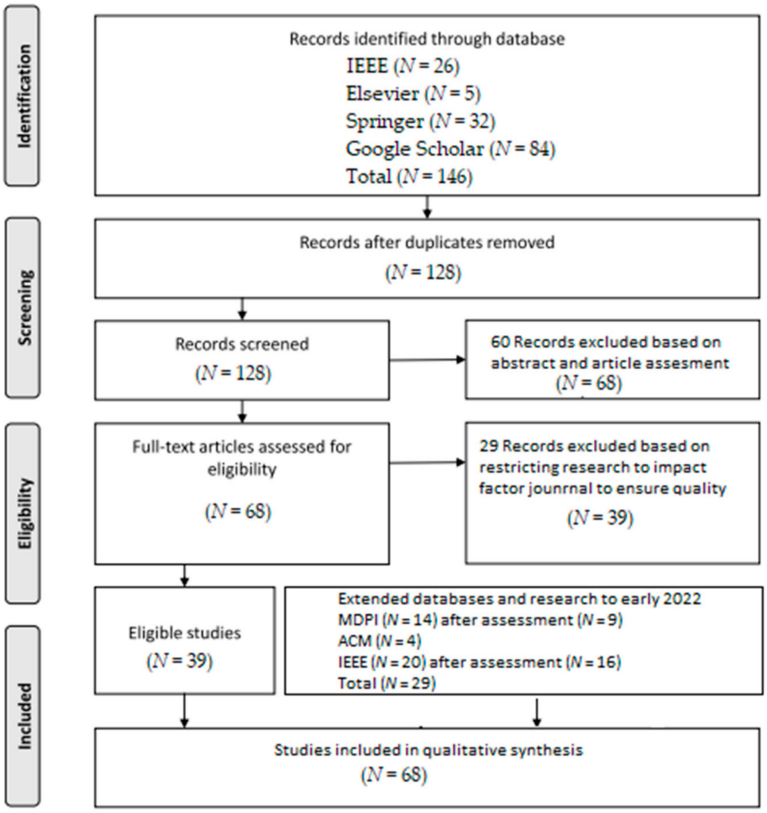

Figure 8. Procedural steps for article assessment.

3.2. Inclusion/Exclusion Criteria

The inclusion and exclusion criteria were established for the article assessment in order to extract highly authentic and relevant literature. The foci of the research were based on the key words related to blockchain and the particular domain of VANETs. The keywords, "blockchain", "VANETs", "IoV", and "Internet of Vehicles", were included on the basis of the research interests. A total of 146 articles were shortlisted in the first step of the searching among the impact factor journals and Google Scholar. A total of 18 articles were eliminated because of duplication, and the remaining 128 articles were selected for further analysis and examination.

3.3. Abstract and Article Assessment

In the screening step, a total 68 studies were selected out of the 128 studies on the basis of the abstract and literature assessment. The articles that were less focused on the targeted topics were removed from the study. The selection of 68 studies was based purely on the relevant and concrete findings and contributions. We further verified our process in order to maintain cohesion in the selection of articles. The quality was considered at each stage, and, during the screening, a further 29 articles were eliminated because they were non-impactor publications. The databases and research were further extended to early 2022, and 29 more studies were included after the assessment, as is presented in Figure 8. A total of 68 studies were included in this literature after all of the steps: identification, screening, eligibility, and extension.

4. Results

Descriptive Analysis of the Corpus

The 68 shortlisted studies are distributed in the form of graph with respect to the period of six years. This distribution demonstrates the escalation of blockchain technology over the years. The proliferation of blockchain technology also enables other domains to integrate and evolve. The evolution of blockchain was started in 2008 and, at that time, the research was mainly focused on digital currencies and the associated issues. Since 2016, it has attracted practitioners for the evolution of other domains. In particular, the evolution of blockchain in VANETs is demonstrated by the spread graph of the articles in Figure 9.

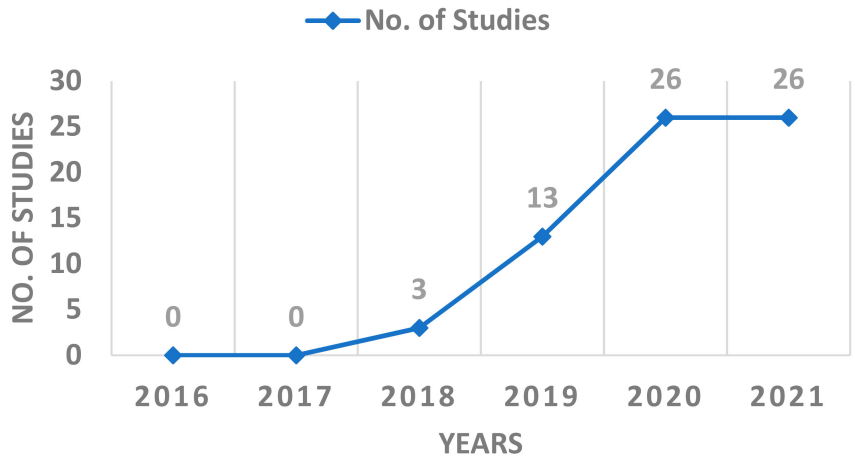

Figure 9. Spread of articles by period.

Figure 9 demonstrates the spread of the articles by period, and it can be observed that the graph of the studies increases for blockchain-enabled VANETs over the period of time. A further count of the studies, the publication years, and the references are presented in Table 2.

Table 2. Numbers of articles by year.

Year	No. of Studies	Articles
2018	3	[52] (Bao-Kun et al., 2018), [53] (Busygin et al., 2018), [54] (Lu et al., 2018)
2019	13	[15] (Li et al., 2019), [55] (Ali et al., 2019), [56] (Shrestha & Nam, 2019), [57] (Xie et al., 2019), [58] (Kim, 2019), [59] (Yang et al., 2019), [60] (Zhang & Wang, 2019), [61] (Butt et al., 2019), [62] (Lu et al., 2019), [63] (Feng et al., 2019), [64] (De Maio et al., 2019), [65] (Zhang et al., 2019), [66] (Zheng et al., 2019)
2020	26	[14] (Matheu et al., 2020), [19] (Bagga et al., 2020), [67] (Bonadio et al., 2020), [68] (Lei et al., 2020), [69] (Shrestha et al., 2020), [70] (Sutrala et al., 2020), [71] (Ahmad et al., 2020), [72] (Shala et al., 2020), [73] (Zhuo Ma et al., 2020), [74] (Ryu et al., 2020), [75] (Zhao et al., 2020)s, [76] (Li et al., 2020), [77] (Wang & Zhang, 2020), [78] (Malik et al., 2020), [79] (Shi et al., 2020), [80] (Yang et al., 2020), [81] (Cho & Perera, 2020), [82] (Jiang et al., 2020), [83] (Zhaowei Ma et al., 2020), [84] (Tomar, 2020), [85] (Ayaz et al., 2020), [86] (Hussain et al., 2020), [87] (Lin et al., 2020), [88] (Mershad, 2020), [89] (Zheng et al., 2020), [90] (Wang et al., 2020)
2021	26	[3] (Álvares et al., 2021), [40] (Singh et al., 2021), [45] (Peng et al., 2021), [49] (Abbas et al., 2021), [22] (Iqbal et al., 2021), [91] (Kudva et al., 2021), [92] (Shammar et al., 2021), [93] (Alharthi et al., 2021), [94] (Hei et al., 2021), [95] (Akhter et al., 2021), [96] (Azam et al., 2021), [97] (Chulerttiyawong & Jamalipour, 2021), [98] (Dwivedi et al., 2021), [99] (Firdaus et al., 2021), [100] (Ghovanlooy Ghajar et al., 2021), [101] (Jabbar et al., 2021), [102] (Kaltakis et al., 2021), [103] (Kapassa et al., 2021), [104] (Kebande et al., 2021), [105] (Kim, 2021), [106] (Li et al., 2021), [107] (Li et al., 2021), [108] (Liang & Ma, 2021)s, [109] (Ma et al., 2021), [110] (Maaroufi & Pierre, 2021), [111] (Sharma et al., 2021)

The emergency surrounding blockchain technology led to the first ever international conference, which was held in 2018 and entitled: "the 2018 international conference on blockchain". The focus of the conference was exclusively based on the applications of blockchain using smart contracts. Since then, the studies on blockchain and the related domains have been increasing in the major databases and currently still are. The sources and the year-wise classifications of the articles are further presented in Table 3 in order to highlight the research horizon across the databases.

Table 3. Sources and year-wise classification of articles.

Article	Year	Source
[3] (Álvares et al., 2021)	2021	IEEE
[40] (Singh et al., 2021)	2021	IEEE
[45] (Peng et al., 2021)	2021	Elsevier
[49] (Abbas et al., 2021)	2021	MDPI
[22] (Iqbal et al., 2021)	2021	IEEE
[91] (Kudva et al., 2021)	2021	Elsevier
[92] (Shammar et al., 2021)	2021	IEEE
[93] (Alharthi et al., 2021)	2021	IEEE
[94] (Hei et al., 2021)	2021	Springer
[95] (Akhter et al., 2021)	2021	MDPI
[96] (Azam et al., 2021)	2021	IEEE
[97] (Chulerttiyawong & Jamalipour, 2021)	2021	IEEE
[98] (Dwivedi et al., 2021)	2021	IEEE
[99] (Firdaus et al., 2021)	2021	MDPI

Table 3. *Cont.*

Article	Year	Source
[100] (Ghovanlooy Ghajar et al., 2021)	2021	MDPI
[101] (Jabbar et al., 2021)	2021	IEEE
[102] (Kaltakis et al., 2021)	2021	MDPI
[103] (Kapassa et al., 2021)	2021	MDPI
[104] (Kebande et al., 2021)	2021	MDPI
[105] (Kim, 2021)	2021	MDPI
[106] (Li et al., 2021)	2021	IEEE
[107] (Li et al., 2021)	2021	IEEE
[108] (Liang & Ma, 2021)	2021	IEEE
[109] (Ma et al., 2021)	2021	IEEE
[110] (Maaroufi & Pierre, 2021)	2021	IEEE
[111] (Sharma et al., 2021)	2021	IEEE
[14] (Matheu et al., 2020)	2020	MDPI
[19] (Bagga et al., 2020)	2020	IEEE
[67] (Bonadio et al., 2020)	2020	Springer
[68] (Lei et al., 2020)	2020	Springer
[69] (Shrestha et al., 2020)	2020	Elsevier
[70] (Sutrala et al., 2020)	2020	IEEE
[71] (Ahmad et al., 2020)	2020	IEEE
[72] (Shala et al., 2020)	2020	IEEE
[73] (Zhuo Ma et al., 2020)	2020	IEEE
[74] (Ryu et al., 2020)	2020	IEEE
[75] (Zhao et al., 2020)s	2020	Springer
[76] (Li et al., 2020)	2020	IEEE
[77] (Wang & Zhang, 2020)	2020	IEEE
[78] (Malik et al., 2020)	2020	Springer
[79] (Shi et al., 2020)	2020	Springer
[80] (Yang et al., 2020)	2020	IEEE
[81] (Cho & Perera, 2020)	2020	ACM
[82] (Jiang et al., 2020)	2020	ACM
[83] (Zhaowei Ma et al., 2020)	2020	ACM
[84] (Tomar, 2020)	2020	ACM
[85] (Ayaz et al., 2020)	2020	IEEE
[86] (Hussain et al., 2020)	2020	IEEE
[87] (Lin et al., 2020)	2020	IEEE
[88] (Mershad, 2020)	2020	IEEE
[89] (Zheng et al., 2020)	2020	IEEE
[90] (Wang et al., 2020)	2020	IEEE
[15] (Li et al., 2019)	2019	Springer
[55] (Ali et al., 2019)	2019	Elsevier
[56] (Shrestha & Nam, 2019)	2019	IEEE

Table 3. *Cont.*

Article	Year	Source
[57] (Xie et al., 2019)	2019	IEEE
[58] (Kim, 2019)	2019	IEEE
[59] (Yang et al., 2019)	2019	IEEE
[60] (Zhang & Wang, 2019)	2019	IEEE
[61] (Butt et al., 2019)	2019	IEEE
[62] (Lu et al., 2019)	2019	IEEE
[63] (Feng et al., 2019)	2019	IEEE
[64] (De Maio et al., 2019)	2019	ACM
[65] (Zhang et al., 2019)	2019	IEEE
[66] (Zheng et al., 2019)	2019	IEEE
[52] (Bao-Kun et al., 2018)	2018	Springer
[53] (Busygin et al., 2018)	2018	Springer
[54] (Lu et al., 2018)	2018	IEEE

5. RQ1: Blockchain Domains and Research Areas

The selected articles were classified with respect to the research domains in order to answer RQ1. The classification of the domains was achieved by giving consideration to the implementation of blockchain technology in VANETs. The research focus was to determine the corresponding fields when the blockchain meets VANETs, including the individual entities. The classification is demonstrated with the help of the pie chart presented in Figure 10.

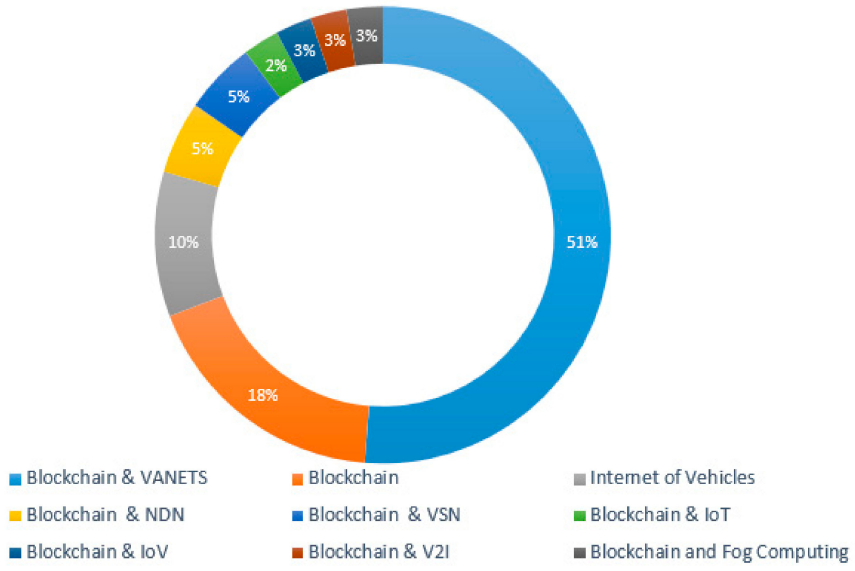

Figure 10. Classification of studies for blockchain-enabled VANETs.

Figure 10 highlights that 51% of the selected studies are related to blockchain and VANETs. The graph of the results emphasizes the advancement of blockchain technology in the realm of VANETs. The literature analysis confirms that researchers and practitioners are focusing on these technologies. In particular, the studies indicate the resolutions for the vehicle ad hoc network issues and challenges through the employment of DLT. Figure 10 also represents the general and particular areas when blockchain is integrated with VANETs. The areas of blockchain, the Internet of Vehicles, VANETs, named data

networking (NDN), video stream networks (VSNs), the IoT, V2I, and Fog Computing are the significant literature findings. The NDN is considered to be a future Internet architecture, similar to an IP address, in which the data names are used for the packet forwarding. NDN is in its earlier stages, and it can therefore be considered for future research in blockchain-enabled VANETs. Similarly, VSNs are used for multimedia sharing across entities, and blockchain can be applied to VSNs for data integrity and security over the air. Later in this section, the implementations of the other areas are discussed in detail.

6. RQ2: Blockchain Framework for VANETs

The blockchain-based research methodologies and techniques were determined from the selected articles to answer RQ2. The highlighted blockchain techniques can be employed to improve VANETs. There are 10 techniques that are examined in detail and illustrated in Figure 11, and the rest of the techniques are mentioned as "other". Figure 12 segregates the numbers of studies with regard to the techniques in order to demonstrate the significance of the studies against the techniques.

In Figure 11, the blockchain-based techniques are illustrated, and these can be employed to obtain blockchain-enabled VANETs. Blockchain-enabled frameworks [67], decentralized architectures, and techniques based on cryptography are discussed in the majority of the selected studies in relation to overcoming the integration of the blockchain and VANETs.

Figure 12 emphasizes the techniques of blockchain and their significance can be analyzed on the basis of the numbers of studies on them. Blockchain frameworks and decentralized authentication schemes are discussed in 24 aggregated studies out of 68, which shows that blockchain frameworks are being employed in different IoT sectors. Connected vehicles (CVs) are one of the most promising areas of research in the realm of blockchain. Therefore, the framework for blockchain and CVs is also studied in the most recent research in order to understand the dynamics [112]. Similarly, in this research on VANETs, eight studies presented innovative frameworks for integrating blockchain and VANETs.

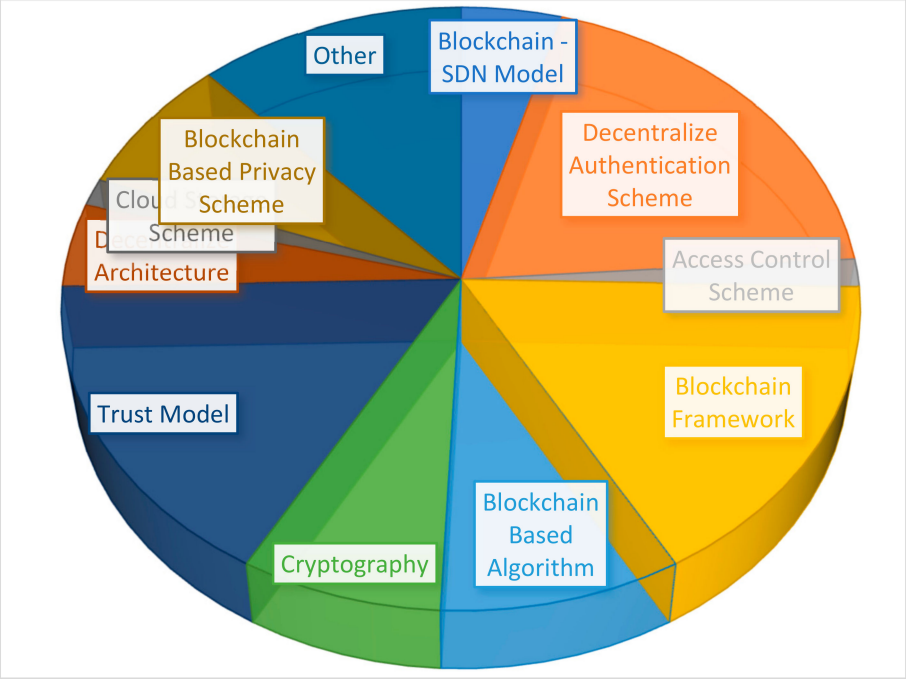

Figure 11. An overview and classification of blockchain techniques.

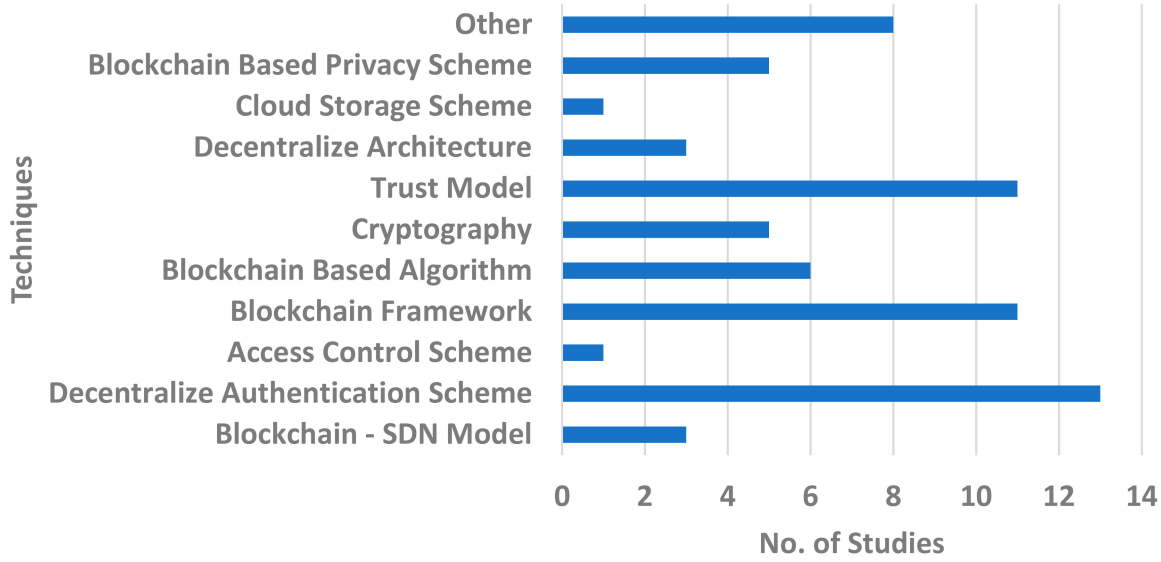

Figure 12. Blockchain techniques and publications.

6.1. Decentralized Architecture for VANETs

As can be seen in Figure 12, the blockchain framework and the decentralized authentication mechanism are discussed in a total of 24 studies out of 68 shortlisted articles. Furthermore, the practically possible decentralized architecture is discussed in only 3 studies out of 68. Therefore, an advanced decentralized architecture is one of the most prominent needs of our time. The state of the architecture is determined thoroughly in this study and is demonstrated in Figure 13.

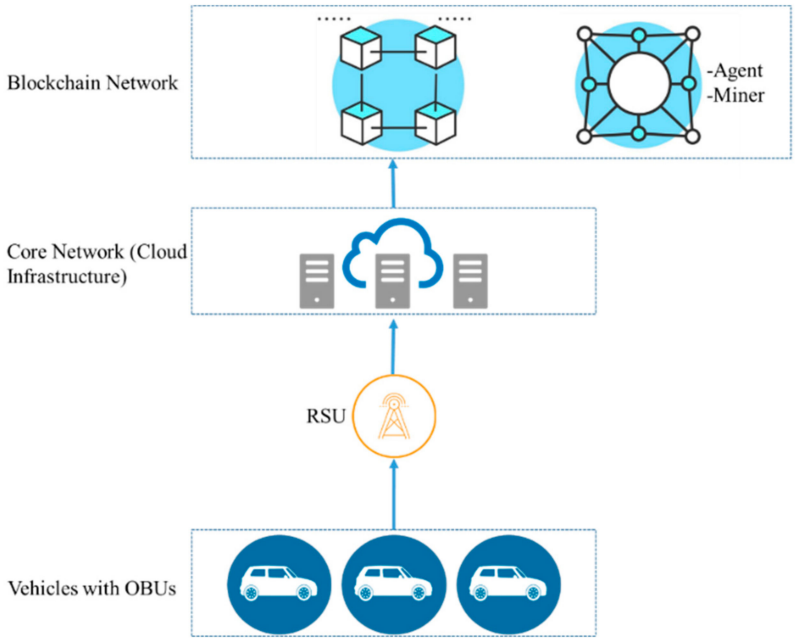

Figure 13. Decentralized architecture for VANETs.

The identity and privacy of vehicles and their locations were analyzed using the construction approach of the IoT chain architecture and private blockchain [5,38] to obtain a blockchain-based architecture for VANETs, as is shown in Figure 13. The rectified and analyzed architecture is based on eight different components: vehicles, the roadside unit (RSU), the onboard unit (OBU), the infrastructure, the blockchain network, the smart contract, the miner, and the agent node.

6.1.1. Vehicles

Vehicles are considered to be one of the essential moving components of blockchain-enabled VANETs. The onboard units installed in vehicles help facilitate communication with the core network.

6.1.2. On-Board Unit

The OBU is also known as a tracking device, or a data terminal, which is mounted on the vehicle. This component is responsible for the vehicle communication with servers or adjacent nodes.

6.1.3. Roadside Unit

The RSU is considered to be an access point in the network. This unit is responsible for collecting data from the OBUs and transmitting it to the core network in real time. The RSU also transmits traffic, emergency, and weather-related information for the assistance of drivers and fleet staff.

6.1.4. Core Network

The core network consists of several servers and ensures connectivity with vehicles for the data transmission through the RSU. The CA, database, application, and web servers lie in the core network. All the data stored on these servers is encrypted in order to confirm the data integrity and security. The core network is responsible for maintaining all the communication messages in real time for further decision making.

6.1.5. Blockchain Network

This literature review analyzes the blockchain network with the aim of ensuring privacy protection in the blockchain-based architecture for VANETs. The private chain architecture was examined, in which all the hash values are stored in the network to avoid malicious attacks. However, the data cannot be tampered with or changed because the blockchain is immutable.

6.1.6. Smart Contracts

The protocols (referred to as "contracts") are clearly defined for the authentication, anonymity, data encoding and decoding, etc. The use of contracts also helps to save transaction costs.

6.1.7. Agent Node

The participant is considered to be an agent node in a decentralized network. The participants participate in a consensus mechanism and ensure the backup of the network. The agent node also provides correctness across transactions.

6.1.8. Miner

The special agent node is considered to be a miner node when it tries to solve the mathematical problem and solves it successfully. The miner node solves the puzzle and obtains the legal right to keep the block. The miner node is also responsible for the mining and validating of new blocks. The updated data is saved in a newly established block, and all of the other participants update the respective storage accordingly in the blockchain.

The components of the blockchain-based framework for VANETs are discussed above, and their interactions are demonstrated in Figure 14.

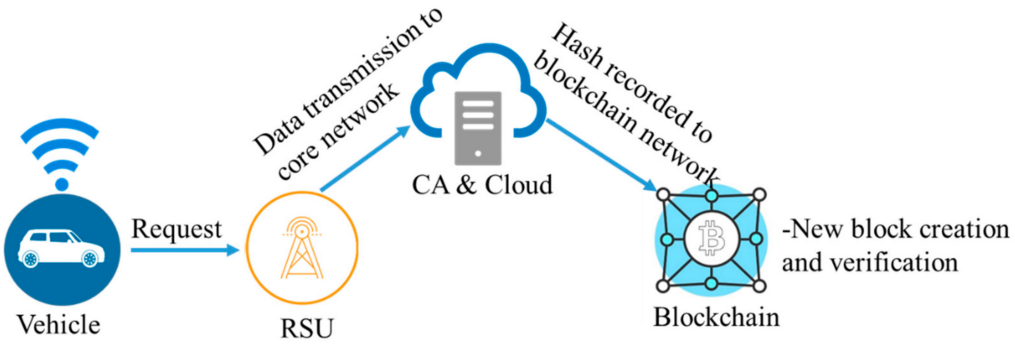

Figure 14. Blockchain-enabled VANET communication architecture.

7. RQ3: Blockchain and the IoT/VANET Challenges, Limitations, and Techniques

To answer RQ3, Table 4 explains the methods, challenges and limitations when blockchain integration takes place with VANETs. The advantages and challenges of the traditional models are described as follows: The Bayesian inference model [113] provides the mechanism for decentralized trust management and ensures the consistency and reliability of the storage or database. The composition of the trust management and privacy preservation is one of the major drawbacks of this methodology. The proof of work (POW) is used as a consensus mechanism to validate the authentic and deserving nodes that have good reputations and computing power. In our proposed architecture, the message exchange and identification of malicious nodes can be managed by using POW. The provision of information sharing will only be available across vehicles or entities having the capability to prove their worth by solving a puzzle. The POW [91] needs further enhancement to deal with the crucial event message dissemination in dynamic topology in order to achieve low computation and maximum throughput. The proof of driving mechanism is also highlighted by practitioners to mitigate the issues of the POW and proof of stake. The conditional anonymity and improved transparency are observed in the blockchain-based anonymous reputation system (BARS) [114], but it is also vulnerable to various attacks. The certificate less public key signature (CL-PKS) [55] is recognized as one of the efficient methods for vehicle-to-infrastructure communication with lower computation costs. However, it needs to be enhanced more for vehicle-to-vehicle communication. The hierarchical temporal memory (HTM) method [115] was found to be effective and efficient for identifying malicious users, but the challenge of battling frequent attacks persists for this methodology. Similarly, the implementation of an improved growing hierarchical self-organizing map (I-GHSOM) is critically important to achieving intrusion detection functionality. It can be used in the proposed decentralized architecture as a composite mechanism to handle the large number of vehicles in dynamic topology, and to intercept intrusions accordingly for faster and more secure message transmission. The I-GHSOM [116] is quick compared to other methods for detecting multiple types of attacks. The message-by-vehicle can be mined quickly by using this method. However, it needs to be improved in terms of the management of the overheads. The better effectiveness and enhanced data transmission were analyzed under the methodology of unified trust management, but this lacks security because of virtualization and software-defined networks [117] Lastly, the methodology of blockchain-based VANETs [9] was analyzed and was recognized as having one of the most effective data processing times, as well as privacy protection. Earlier, this methodology depended on trusted centralized entities, but the advancement of blockchain has made it decentralized and distributed. However, this methodology is regarded as the most useful for when blockchain meets VANETs.

Table 4. Methods/techniques lead to blockchain-enabled VANETs.

Article	Year	Method	Advantages	Drawbacks
[15] (Li et al., 2019)	2019	Blockchain Based VANETs	This is the most advanced methodology used for state of the art privacy protection and real time data transmission across vehicle to everything	In nascent stages, this methodology relied on trusted centralized entities with a drawback of center point failure, but the advancement of blockchain has made it decentralized and distributed in all as aspects. However, this methodology is regarded as the most useful when blockchain meets VANETs.
[113] (Xia et al., 2020)	2020	Bayesian Model	This method provides mechanism for decentralize trust management and ensures consistency and reliability of the storage or database	The composition of trust management and privacy preservation is one of the major drawbacks of this methodology.
[91] (Kudva et al., 2021)	2020	Proof of Work	This method provides trustworthiness without storage overheads	It needs enhancement to deal with crucial event message dissemination for better performance.
[114] (She et al., 2019)	2019	BARS	This method provides transparency and anonymity and also ensure effective and robust mechanism	This methodology is more vulnerable to various attacks.
[55] (Ali et al., 2019)	2019	CL-PKS	This method provides reliable communication between vehicles to infrastructure with less computational cost.	This method lacks in vehicle-to-vehicle communication.
[115] (Hasrouny et al., 2019)	2019	HTM	This method provides trustworthiness with quick and effective identification of malicious users	This method cannot handle frequent attacks which makes it more vulnerable against the frequent attacks.
[116] (Liang et al., 2019)	2019	I-GHSOM	This method has the ability to detect the attacks rapidly. It also ensure quick encoding of real time messages transmitted by vehicles.	This method needs to improve in terms of management of overheads.
[117] (He et al., 2019)	2019	Unified Trust Management	This method provides effective data transmission and trust management mechanism	This method lacks in security due to virtualization and security of software-defined networks.

Table 4 defines the methodologies and highlights the challenges for VANETs, which are addressed by employing the inherent characteristics of blockchain technology. The detailed list of the blockchain issues is presented in Figure 14, and these are addressed by integrating the blockchain with IoT technologies. Figure 15 highlights that 14 out of 68 studies discuss the issues of trust management and its resolutions. Privacy management is discussed in 13 out of 68 studies, with general security issues discussed in 16 selected studies, which makes it still one of the most prominent issues in blockchain-based VANETs.

Issues regarding the proposed frameworks of blockchain are discussed in three of the selected studies and were validated accordingly.

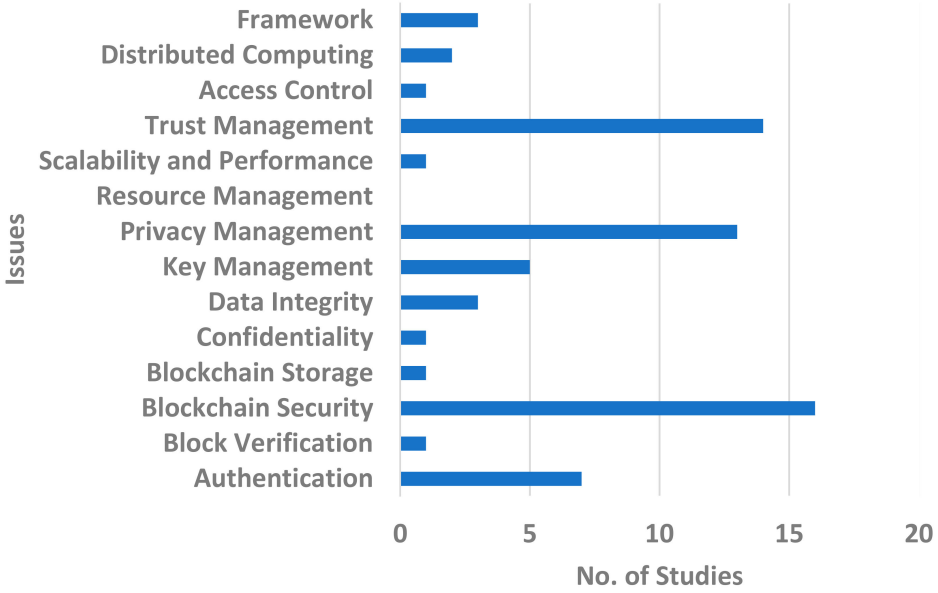

Figure 15. General blockchain issues and numbers of studies.

Lastly, distributed and fog computing are also hot areas for practitioners since the blockchain conference took place in 2018 for future research and directions.

8. RQ4: General Blockchain Limitations and Techniques

To answer RQ4, and to determine the corresponding limitations and challenges faced by blockchain, we classified the studies with respect to the challenges and the applied techniques and models to overcome the limitations. The challenges of security, privacy, and key and trust management affect every domain when they meet with blockchain. Therefore, we not only identify the major issues, but we also highlight the techniques and models to overcome the challenges. The research focus is to fill the research gap in terms of the challenges that arise when blockchain meets with any of the other domains. Table 5 presents the classification of the studies with respect to the major issues, and the techniques for overcoming the limitations. Table 5 presents the limitations and the corresponding techniques and models along with the source, which can be adopted to solve the problems of blockchain-enabled VANETs.

Table 5. Techniques and limitations of blockchain when met with multiple domains.

Article	Limitations	Techniques/Models
[9] (Poniszewska-Marańda & Kryvinska, 2018)	Transparency and auditability	Intelligent agents and multi-agent architecture for auditable blockchain
[15] (Li et al., 2019)	Identity and privacy protection	Blockchain based VANET & UGG, IPP and LPP algorithm for identity protection
[19] (Bagga et al., 2020)	Data Integrity, open channel Security and secure data transmission	Pay-go protocol
[118] (Buterin, 2014)	Consensus issues	proof of work based blockchain
[114] (She et al., 2019)	Malicious attacks and suspicious node detection	Blockchain trust model (BTM) and smart contracts
[55] (Ali et al., 2019)	Message exchange authentication	Certificate less public key signature (CL-PKS) scheme using bilinear pairing

Table 5. *Cont.*

Article	Limitations	Techniques/Models
[119] (Khelifi et al., 2020)	Security for content delivery and caching	NDN based security architecture Reputation-based blockchain mechanism
[68] (Lei et al., 2020)	Cache poisoning, key management and access control	Blockchain-based security architecture
[120] (Minoli & Occhiogrosso, 2018)	Security (End-End) Mitigation	Permission less blockchain using cryptographic schemes
[69] (Shrestha et al., 2020)	Time critical message dissemination	Public blockchain mechanism for message cohesion
[56] (Shrestha & Nam, 2019)	Mobility, latency, trust management, security and 51% attack	Regional blockchain model
[93] (Alharthi et al., 2021)	security vulnerabilities such as denial-of-service (DoS), replay attacks and Sybil attacks	Biometrics blockchain framework
[121] (Luo et al., 2019)	Malicious attacks and data spoofing	blockchain enabled trust based location privacy protection scheme
[52] (Bao-Kun et al., 2018)	Privacy management	Blockchain based data sharing scheme using Paillier cryptosystem
[70] (Sutrala et al., 2020)	Security attacks: replay, traceability, man-in-the-middle and impersonation	Privacy preserving batch verification-based authentication mechanism using elliptic curve cryptography
[71] (Ahmad et al., 2020)	Man-in-the-middle (MiTM) attack and Trust Management	MiTM attack resistance trust model
[122] (Abou-Nassar et al., 2020)	Vehicular data confidentiality, accessibility and information reliability	Blockchain decentralized interoperable trust framework (DIT) and indirect trust inference system (ITIS)
[72] (Shala et al., 2020)	Trust and security of vehicular information	multi-layer adaptive and trust-based weighting model using control loops and smart contracts
[57] (Xie et al., 2019)	Malicious node identification in VANETs	Software-defined network (SDN) architecture
[123] (Tan & Chung, 2019)	Resource management and key distribution	Secure authentication and key management scheme using consortium blockchain
[124] (Hu et al., 2019)	Security, authentication and consensus issues	Byzantine fault tolerance algorithm
[73] (Ma et al., 2020)	Attacks: DoS, public key tampering and collusion and key management	Blockchain enabled decentralized key management mechanism (DB-KMM), key agreement protocol based on the bivariate polynomial
[59] (Yang et al., 2019)	Data correctness, reliability and tamper proofing	Proof of event consensus
[60] (Zhang & Wang, 2019)	Data confidentiality, privacy and information repudiation	ElGamal encryption and group signature algorithm
[75] (Zhao et al., 2020)	Resource allocation, malicious attacks, trust value management	Decentralized trust management architecture, joint proof-of-stake and modified PoS-mPBFT algorithm
[76] (Li et al., 2020)	Privacy management and security of vehicular data	fine-grained access control scheme based on cipher text-based attribute encryption (CPABE)

Table 5. *Cont.*

Article	Limitations	Techniques/Models
[77] (Wang & Zhang, 2020)	Secure information exchange, forwarding and limitations of proxy re-encryption algorithm	Data sharing and customized services based on the consortium blockchain using cipher text-policy attribute-based proxy re-encryption algorithm
[94] (Hei et al., 2021)	Storage, data integrity and non-accountability of denial of service attack	P2P cloud storage scheme with smart contracts on ethereum
[62] (Lu et al., 2019)	Distributed authentication, identity privacy and security attacks	privacy preserving authentication (BPPA) scheme and Merkle Patricia tree (MPT)
[63] (Feng et al., 2019)	Authentication and privacy management	Blockchain assisted privacy preserving authentication system (BPAS)
[54] (Lu et al., 2018)	Privacy management	Blockchain-based anonymous reputation system (BARS) and reputation evaluation algorithm
[78] (Malik et al., 2020)	Node trust ability prediction, privacy preservation and data sanitization	Sea lion explored-whale optimization algorithm

9. Discussions

The inherent characteristics of blockchain have received an immense amount of attention from researchers and practitioners in the last decade. The escalation and implementations of blockchain with IoT are being experimented on as pilot projects in various sectors. The DLT has achieved both theoretical and practical endorsements from the academic and industrial perspectives. The classifications of the studies with respect to the theoretical, simulation, and experiment-based results are presented in Figure 16. There are 32 studies out of 68 that are based on theoretical analyses, 23 studies that are based on simulation results, and only 13 studies that are based on experimental results. Figure 16 highlights the significance of the practical implementation as future research for the practitioners.

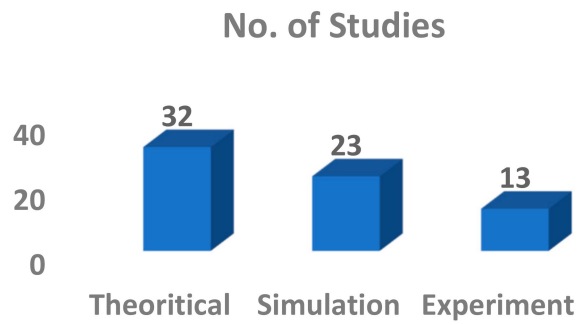

Figure 16. Result-wise classification of studies.

The research questions are answered in this review to determine the future directions of blockchain technology in the particular domain of VANETs. There is a research gap between blockchain and its applications, and particularly for vehicular networks. The major research issues for integrating blockchain and VANETs are security, traceability, and transparency. The major implementation of VANETs is in the digitalization of fleet telematics. Further details with regard to the issues and implementations are presented in the following sections.

9.1. Security, Traceability, and Transparency

The traceability, security, and transparency are always challenges for VANETs and other related technologies. These challenges arise when handshaking protocols are required

for better hand-offs in centralized architecture. The DLT can be applied in VANETs because of the immense number of characteristics for overcoming such challenges of security. It also provides trust and consensus mechanisms to increase the reliability and traceability. The ledger is shared among the nodes to prevent the loss of data integrity. The major players at the sensory layer, including the actuators, gateways, routers, and things, have shared ledgers to permit access on a per need basis for the process flows. The blockchain, with an immense number of features and advantages, eliminates the centralized systems and promotes immutable, transparent, and efficient architecture for other domains.

9.2. IoV and Fleet Management Digitalization

The VANETs and the corresponding technologies are critical for ITS. This is a network of connected vehicles. The connection modes are facilitated through satellite (GPS) or cellular networks (3G, 4G, 5G), and this depends on the onboard unit (OBU) embedded inside the vehicle. Some OBUs provide multiple modes of connection in order to provide reliability and coverage. RFID technology can provide each driver with a unique digital identity. Remote fleet managers can track the driver's performance, and provide warnings for bad performances and rewards for good performances, which can boost the driver's motivation to perform well on the road. Fleet management systems, such as food delivery fleet management, taxi fleet management, oil distribution fleet management, etc., can benefit significantly from the implementation of blockchain-enabled VANETs. The surveillance cameras can also be attached to the OBU for vehicle surveillance for the fleet managers. Parameters, such as the engine speed, the tank temperature, the tire pressure, and the fuel consumption can be monitored through sensors and can be controlled remotely for vehicle safety control. Figure 17 illustrates VANETs and their applications in fleet management.

Figure 17. An overview of fleet management system and its components.

9.3. Blockchain-Enabled VANET Applications

The research implication of blockchain-enabled IoT was found suitable for the areas described in the following sections, where its immediate implementation can completely change the perspective.

9.3.1. Fleet and Journey Management for ITS

The efficient movement of vehicles with containers is always challenging for fleet owners. Blockchain-enabled VANETs can help fleet owners track their fleets in real time by preserving the coordinates, speeds, altitudes, angles, temperatures, and fuel levels using a real-time messaging system. In general supply chains and fuel supply chains,

blockchain promote trust among all the authorities, and it also enables the quick and efficient movement of products with greater consensus.

9.3.2. Asset Tracking

The compliance with safety and security is always a challenge for authorities when they are attempting to ensure efficient asset movement. The blockchain-enabled VANETs can help to store data in shared ledgers throughout the product's lifecycle. The ledger information can be shared with the concerned authorities, consignees, manufacturers, and shippers. The blockchain technology in asset management is easy to implement, secure, and transparent, with the cutting-edge feature of cost-effectiveness.

9.3.3. Data Science and Management

Data science and management applications can be developed on blockchain technology to ensure tamper-free maintenance and operational data. This helps to maintain the data integrity in data sciences to prevent prediction anomalies. The trusted ledger of the data changes can also be shared with the appropriate authorities for further compliance and management.

9.3.4. Solid Waste Management

Researchers have surveyed blockchain-and-VANET-based waste management models for the advancement of waste collection procedures in developing cities. The key components of waste management models are waste collection, truck routing, transportation, and the monitoring of the recycling of certain types of garbage. Researchers propose intelligent algorithms for the collection, disposal, and recycling of trash.

9.3.5. Contact Tracing and Social Distancing

The only way to prevent pandemics is to maintain social distancing. The decentralized model of contact tracing is endorsed by an international consortium, which consists of Google and Apple, in order to ensure transparency and privacy. Researchers have surveyed blockchain- and IoT-enabled techniques for contact tracing to preserve privacy, transparency, and security. The analyzed composition of blockchain and IoV can provide digital contact tracing mechanisms for the prevention of pandemics such as COVID-19.

10. Conclusions

This study encapsulates a systematic review and analysis that is based on multidisciplinary research studies, and that addresses the issues that can occur when blockchain meets the IoT, and especially VANETs. It further provides a comprehensive classification of the articles on the basis of the methods and techniques used to overcome the challenges of VANETs. The complete decentralized architecture of VANETs is derived from the extensive literature review and is referred to as "blockchain-enabled VANET architecture".

The substantial contribution of this review is that it highlights the significance of blockchain in other domains with the inherent characteristics. The particular area of VANETs was selected in this review in order to validate the potentials of blockchain technology. The decentralized architecture was also derived for vehicular networks on the basis of DLT. The specific mechanisms of VANETs, as well as the IoT, such as handshaking, hand-offs, and data communication, are also discussed in the light of blockchain technology.

The challenges, limitations, and open issues of blockchain-enabled applications are also classified for future prospects. This study is not only limited to the integration of blockchain and VANETs, but it also discusses the potential blockchain issues that may be addressed in future research. The interoperability, scalability, and storage-related technical issues still need to be addressed by practitioners. Lastly, this study also provides a classification of the articles that is based on the result types, such as the theoretical, simulation, and experimental results. This classification highlights that blockchain-enabled pilot projects are rare. Therefore, practical implementation should be considered by practitioners for a

more concrete implementation of blockchain in different domains. This study also sheds light on an overview of the extant blockchain-enabled IoT chain research as future works.

As part of the future work, research can commence on 5G-enabled blockchain-based VANETs using narrowband-IoT (NB-IoT) technologies for high mobility and latency, and low power consumption. This study could also lead to the implementation of blockchain in different sectors, such as blockchain-enabled healthcare transportation for door-to-door vaccination, which can be targeted to handle pandemic-like situations. The future implications of this study could also be helpful for contact tracing and isolation management in the realm of the IoT. The proposed decentralized architecture can also be extended to the design of state-of-the-art journey management systems for autonomous vehicles and drones.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Cole, R.; Stevenson, M.; Aitken, J. Blockchain technology: Implications for operations and supply chain management. *Supply Chain. Manag. Int. J.* **2019**, *24*, 469–483. [CrossRef]
2. Tönnissen, S.; Teuteberg, F. Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. *Int. J. Inf. Manag.* **2020**, *52*, 101953. [CrossRef]
3. Álvares, P.; Silva, L.; Magaia, N. Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives. *Telecom* **2021**, *2*, 108–140. [CrossRef]
4. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.-K.R. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access* **2019**, *7*, 176935–176951. [CrossRef]
5. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
6. Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics* **2021**, *10*, 3003. [CrossRef]
7. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
8. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain Technology in Finance. *Computer* **2017**, *50*, 14–17. [CrossRef]
9. Pawlak, M.; Poniszewska-Marańda, A.; Kryvinska, N. Towards the intelligent agents for blockchain e-voting system. *Procedia Comput. Sci.* **2018**, *141*, 239–246. [CrossRef]
10. Sheth, A.; Subramanian, H. Blockchain and contract theory: Modeling smart contracts using insurance markets. *Manag. Financ.* **2019**, *46*, 803–814. [CrossRef]
11. Jha, N.; Prashar, D.; Khalaf, O.I.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S. Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers. *Sustainability* **2021**, *13*, 8921. [CrossRef]
12. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access* **2019**, *7*, 176838–176869. [CrossRef]
13. Wan, P.K.; Huang, L.; Holtskog, H. Blockchain-Enabled Information Sharing within a Supply Chain: A Systematic Literature Review. *IEEE Access* **2020**, *8*, 49645–49656. [CrossRef]
14. Matheu, S.N.; Robles Enciso, A.; Molina Zarca, A.; Garcia-Carrillo, D.; Hernández-Ramos, J.L.; Bernal Bernabe, J.; Skarmeta, A.F. Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems. *Sensors* **2020**, *20*, 1882. [CrossRef] [PubMed]
15. Li, H.; Pei, L.; Liao, D.; Sun, G.; Xu, D. Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1178–1193. [CrossRef]
16. Košťál, K.; Helebrandt, P.; Belluš, M.; Ries, M.; Kotuliak, I. Management and Monitoring of IoT Devices Using Blockchain. *Sensors* **2019**, *19*, 856. [CrossRef] [PubMed]

17. Morse, E.A. From Rai stones to Blockchains: The transformation of payments. *Comput. Law Secur. Rev.* **2018**, *34*, 946–953. [CrossRef]
18. Sander, F.; Semeijn, J.; Mahr, D. The acceptance of blockchain technology in meat traceability and transparency. *Br. Food J.* **2018**, *120*, 2066–2079. [CrossRef]
19. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Park, Y. Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. *IEEE Access* **2020**, *8*, 54314–54344. [CrossRef]
20. Lo, S.K.; Liu, Y.; Chia, S.Y.; Xu, X.; Lu, Q.; Zhu, L.; Ning, H. Analysis of Blockchain Solutions for IoT: A Systematic Literature Review. *IEEE Access* **2019**, *7*, 58822–58835. [CrossRef]
21. Conoscenti, M.; Vetrò, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [CrossRef]
22. Iqbal, S.; Noor, R.M.; Malik, A.W. A review of blockchain empowered vehicular network: Performance evaluation of trusted task offloading scheme. In Proceedings of the IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Shah Alam, Malaysia, 3–4 April 2021; pp. 367–371.
23. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
24. Shen, C.; Pena-Mora, F. Blockchain for Cities—A Systematic Literature Review. *IEEE Access* **2018**, *6*, 76787–76819. [CrossRef]
25. Dutta, P.; Choi, T.-M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef] [PubMed]
26. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted business process monitoring and execution using blockchain. In Proceedings of the International conference on business process management, Rio de Janeiro, Brazil, 18–22 September 2016; pp. 329–347.
27. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, *4*, 21260. [CrossRef]
28. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 71.
29. Casey, M.J.; Wong, P. Global supply chains are about to get better, thanks to blockchain. *Harv. Bus. Rev.* **2017**, *13*, 1–6.
30. Toyoda, K.; Mathiopoulos, P.T.; Sasase, I.; Ohtsuki, T. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access* **2017**, *5*, 17465–17477. [CrossRef]
31. Szabo, N. Smart contracts: Building blocks for digital markets. *EXTROPY J. Transhumanist Thought* **2016**, *18*, 28.
32. Magazzeni, D.; McBurney, P.; Nash, W. Validation and Verification of Smart Contracts: A Research Agenda. *Computer* **2017**, *50*, 50–57. [CrossRef]
33. Sato, T.; Himura, Y. Smart-contract based system operations for permissioned blockchain. In Proceedings of the 29th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–6.
34. Watanabe, H.; Fujimura, S.; Nakadaira, A.; Miyazaki, Y.; Akutsu, A.; Kishigami, J.J. Blockchain contract: A complete consensus using blockchain. In Proceedings of the IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 27–30 October 2015; pp. 577–578.
35. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts. 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
36. Wang, Y.; Kogan, A. Designing confidentiality-preserving Blockchain-based transaction processing systems. *Int. J. Account. Inf. Syst.* **2018**, *30*, 1–18. [CrossRef]
37. Chang, S.E.; Chen, Y.-C.; Wu, T.-C. Exploring blockchain technology in international trade: Business process re-engineering for letter of credit. *Ind. Manag. Data Syst.* **2019**, *119*, 1712–1733. [CrossRef]
38. Vaidya, B.; Mouftah, H.T. IoT Applications and Services for Connected and Autonomous Electric Vehicles. *Arab. J. Sci. Eng.* **2020**, *45*, 2559–2569. [CrossRef]
39. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access* **2019**, *7*, 38431–38441. [CrossRef]
40. Singh, S.; Hosen, A.S.M.S.; Yoon, B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
41. Ray, P.P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases. *IEEE Syst. J.* **2020**, *15*, 85–94. [CrossRef]
42. Saad, M.; Bin, M.; Ahmad, A.; Muhammad, M.; Khalid, A.G.; Mohammad, A. Social Distancing and Isolation Management Using Machine-to-Machine Technologies to Prevent Pandemics. *Comput. Mater. Contin.* **2021**, *67*, 3545–3562. [CrossRef]
43. Mehmood, Y.; Marwat, S.N.K.; Kuladinithi, K.; Förster, A.; Zaki, Y.; Görg, C.; Timm-Giel, A. M2M Potentials in logistics and transportation industry. *Logist. Res.* **2016**, *9*, 15. [CrossRef]
44. Sun, G.; Song, L.; Yu, H.; Chang, V.; Du, X.; Guizani, M. V2V Routing in a VANET Based on the Autoregressive Integrated Moving Average Model. *IEEE Trans. Veh. Technol.* **2018**, *68*, 908–922. [CrossRef]
45. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2021**, *7*, 295–307. [CrossRef]

46. Moloisane, N.R.; Malekian, R.; Bogatinoska, D.C. Wireless machine-to-machine communication for intelligent transportation systems: Internet of Vehicles and vehicle to grid. In Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 411–415.
47. Hussain, R.; Hussain, F.; Zeadally, S. Integration of VANET and 5G Security: A review of design and implementation issues. *Futur. Gener. Comput. Syst.* **2019**, *101*, 843–864. [CrossRef]
48. Kurugollu, F.; Ahmed, S.H.; Hussain, R.; Ahmad, F.; Kerrache, C.A. Vehicular Sensor Networks: Applications, Advances and Challenges. *Sensors* **2020**, *20*, 3686. [CrossRef] [PubMed]
49. Abbas, S.; Abu Talib, M.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.-H. Blockchain-Based Authentication in Internet of Vehicles: A Survey. *Sensors* **2021**, *21*, 7927. [CrossRef] [PubMed]
50. Lan, L.; Wang, B.; Zhang, L.; Shi, R.; Li, F. An Event-driven Service-oriented Architecture for Internet of Things Service Execution. *Int. J. Online Biomed. Eng.* **2015**, *11*, 4–8. [CrossRef]
51. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic literature reviews in software engineering—A systematic literature review. *Inf. Softw. Technol.* **2009**, *51*, 7–15. [CrossRef]
52. Bao-Kun, Z.; Lie-Huang, Z.; Shen, M.; Gao, F.; Zhang, C.; Yan-Dong, L.; Yang, J. Scalable and privacy-preserving data sharing based on blockchain. *J. Comput. Sci. Technol.* **2018**, *33*, 557–567.
53. Busygin, A.G.; Konoplev, A.S.; Zegzhda, D.P. Providing Stable Operation of Self-Organizing Cyber-Physical System via Adaptive Topology Management Methods Using Blockchain-Like Directed Acyclic Graph. *Autom. Control Comput. Sci.* **2018**, *52*, 1080–1083. [CrossRef]
54. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
55. Ali, I.; Gervais, M.; Ahene, E.; Li, F. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *J. Syst. Archit.* **2019**, *99*, 101636. [CrossRef]
56. Shrestha, R.; Nam, S.Y. Regional Blockchain for Vehicular Networks to Prevent 51% Attacks. *IEEE Access* **2019**, *7*, 95033–95045. [CrossRef]
57. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
58. Kim, S. Impacts of Mobility on Performance of Blockchain in VANET. *IEEE Access* **2019**, *7*, 68646–68655. [CrossRef]
59. Yang, Y.-T.; Chou, L.-D.; Tseng, C.-W.; Tseng, F.-H.; Liu, C.-C. Blockchain-Based Traffic Event Validation and Trust Verification for VANETs. *IEEE Access* **2019**, *7*, 30868–30877. [CrossRef]
60. Zhang, X.; Wang, D. Adaptive Traffic Signal Control Mechanism for Intelligent Transportation Based on a Consortium Blockchain. *IEEE Access* **2019**, *7*, 97281–97295. [CrossRef]
61. 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]
62. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2019**, *27*, 2792–2801. [CrossRef]
63. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4146–4155. [CrossRef]
64. De Maio, V.; Brundo Uriarte, R.; Brandic, I. Energy and profit-aware proof-of-stake offloading in blockchain-based VANETs. In Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, Auckland, New Zealand, 2–5 December 2019; pp. 177–186.
65. Zhang, D.; Yu, F.R.; Yang, R. Blockchain-Based Distributed Software-Defined Vehicular Networks: A Dueling Deep *Q*—Learning Approach. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 1086–1100. [CrossRef]
66. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs. *IEEE Access* **2019**, *7*, 117716–117726. [CrossRef]
67. Bonadio, A.; Chiti, F.; Fantacci, R.; Vespri, V. An integrated framework for blockchain inspired fog communications and computing in Internet of Vehicles. *J. Ambient Intell. Humaniz. Comput.* **2019**, *11*, 755–762. [CrossRef]
68. Lei, K.; Fang, J.; Zhang, Q.; Lou, J.; Du, M.; Huang, J.; Wang, J.; Xu, K. Blockchain-Based Cache Poisoning Security Protection and Privacy-Aware Access Control in NDN Vehicular Edge Computing Networks. *J. Grid Comput.* **2020**, *18*, 593–613. [CrossRef]
69. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [CrossRef]
70. Sutrala, A.K.; Bagga, P.; Das, A.K.; Kumar, N.; Rodrigues, J.J.P.C.; Lorenz, P. On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5535–5548. [CrossRef]
71. Ahmad, F.; Kurugollu, F.; Adnane, A.; Hussain, R.; Hussain, F. MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles. *IEEE Internet Things J.* **2020**, *7*, 3310–3322. [CrossRef]
72. Shala, B.; Trick, U.; Lehmann, A.; Ghita, B.; Shiaeles, S. Blockchain and trust for secure, end-user-based and decentralized iot service provision. *IEEE Access* **2020**, *8*, 119961–119979. [CrossRef]
73. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An Efficient Decentralized Key Management Mechanism for VANET With Blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5836–5849. [CrossRef]

74. Ryu, K.; Kim, W.; Lee, E.-K. payGo: Incentive-Comparable Payment Routing Based on Contract Theory. *IEEE Access* **2020**, *8*, 70095–70110. [CrossRef]
75. Zhao, N.; Wu, H.; Zhao, X. Consortium Blockchain-Based Secure Software Defined Vehicular Network. *Mob. Netw. Appl.* **2020**, *25*, 314–327. [CrossRef]
76. Li, H.; Pei, L.; Liao, D.; Chen, S.; Zhang, M.; Xu, D. FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain. *IEEE Access* **2020**, *8*, 85190–85203. [CrossRef]
77. Wang, D.; Zhang, X. Secure Data Sharing and Customized Services for Intelligent Transportation Based on a Consortium Blockchain. *IEEE Access* **2020**, *8*, 56045–56059. [CrossRef]
78. Malik, N.; Nanda, P.; He, X.; Liu, R.P. Vehicular networks with security and trust management solutions: Proposed secured message exchange via blockchain technology. *Wirel. Netw.* **2020**, *26*, 4207–4226. [CrossRef]
79. Shi, K.; Zhu, L.; Zhang, C.; Xu, L.; Gao, F. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. *Multimed. Tools Appl.* **2020**, *79*, 8085–8105. [CrossRef]
80. Yang, W.; Dai, X.; Xiao, J.; Jin, H. LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5749–5759. [CrossRef]
81. Cho, E.M.; Perera, M.N.S. Efficient certificate management in blockchain based Internet of Vehicles. In Proceedings of the 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, Australia, 11–14 May 2020; pp. 794–797.
82. Jiang, X.; Ma, Z.; Yu, F.R.; Song, T.; Boukerche, A. Edge computing for video analytics in the Internet of Vehicles with blockchain. In Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Alicante, Spain, 16–20 November 2020; pp. 1–7.
83. Ma, Z.; Yu, F.R.; Jiang, X.; Boukerche, A. Trustworthy Traffic Information Sharing Secured via Blockchain in VANETs. In Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Alicante, Spain, 16–20 November 2020; pp. 33–40.
84. Tomar, R. Maintaining Trust in VANETs using Blockchain. *ACM SIGAda Ada Lett.* **2020**, *40*, 91–96. [CrossRef]
85. Ayaz, F.; Sheng, Z.; Tian, D.; Guan, Y.L. A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination. *IEEE Internet Things J.* **2020**, *8*, 2468–2482. [CrossRef]
86. Hussain, R.; Lee, J.; Zeadally, S. Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 2553–2571. [CrossRef]
87. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K.-K.R. BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 7408–7420. [CrossRef]
88. Mershad, K. SURFER: A Secure SDN-Based Routing Protocol for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *8*, 7407–7422. [CrossRef]
89. Zheng, X.; Li, M.; Chen, Y.; Guo, J.; Alam, M.; Hu, W. Blockchain-Based Secure Computation Offloading in Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4073–4087. [CrossRef]
90. Wang, C.; Shen, J.; Lai, J.-F.; Liu, J. B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1386–1396. [CrossRef]
91. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards secure and practical consensus for blockchain based VANET. *Inf. Sci.* **2021**, *545*, 170–187. [CrossRef]
92. Shammar, E.A.; Zahary, A.T.; Al-Shargabi, A.A. A Survey of IoT and Blockchain Integration: Security Perspective. *IEEE Access* **2021**, *9*, 156114–156150. [CrossRef]
93. Alharthi, A.; Ni, Q.; Jiang, R. A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET. *IEEE Access* **2021**, *9*, 87299–87309. [CrossRef]
94. Hei, Y.; Liu, Y.; Li, D.; Liu, J.; Wu, Q. Themis: An accountable blockchain-based P2P cloud storage scheme. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 225–239. [CrossRef]
95. Akhter, A.; Ahmed, M.; Shah, A.; Anwar, A.; Zengin, A. A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET. *Sustainability* **2021**, *13*, 400. [CrossRef]
96. Azam, F.; Yadav, S.K.; Priyadarshi, N.; Padmanaban, S.; Bansal, R.C. A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. *IEEE Access* **2021**, *9*, 31309–31321. [CrossRef]
97. Chulerttiyawong, D.; Jamalipour, A. A Blockchain Assisted Vehicular Pseudonym Issuance and Management System for Conditional Privacy Enhancement. *IEEE Access* **2021**, *9*, 127305–127319. [CrossRef]
98. Dwivedi, S.K.; Amin, R.; Vollala, S. Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1913–1922. [CrossRef]
99. Firdaus, M.; Rahmadika, S.; Rhee, K.-H. Decentralized Trusted Data Sharing Management on Internet of Vehicle Edge Computing (IoVEC) Networks Using Consortium Blockchain. *Sensors* **2021**, *21*, 2410. [CrossRef]
100. Ghajar, F.G.; Sratakhti, J.S.; Sikora, A. SBTMS: Scalable Blockchain Trust Management System for VANET. *Appl. Sci.* **2021**, *11*, 11947. [CrossRef]
101. 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]

102. Kaltakis, K.; Polyzi, P.; Drosatos, G.; Rantos, K. Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 9792. [CrossRef]
103. Kapassa, E.; Themistocleous, M.; Christodoulou, K.; Iosif, E. Blockchain Application in Internet of Vehicles: Challenges, Contributions and Current Limitations. *Future Internet* **2021**, *13*, 313. [CrossRef]
104. Kebande, V.R.; Awaysheh, F.M.; Ikuesan, R.A.; Alawadi, S.A.; Alshehri, M.D. A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles. *Sensors* **2021**, *21*, 6018. [CrossRef] [PubMed]
105. Kim, S.-K. Enhanced IoV Security Network by Using Blockchain Governance Game. *Mathematics* **2021**, *9*, 109. [CrossRef]
106. Li, F.; Guo, Z.; Zhang, C.; Li, W.; Wang, Y. ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4011–4021. [CrossRef]
107. Li, X.; Liu, J.; Obaidat, M.S.; Vijayakumar, P.; Jiang, Q.; Amin, R. An Unlinkable Authenticated Key Agreement With Collusion Resistant for VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 7992–8006. [CrossRef]
108. Liang, J.; Ma, M. Co-Maintained Database Based on Blockchain for IDSs: A Lifetime Learning Framework. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1629–1645. [CrossRef]
109. Ma, J.; Li, T.; Cui, J.; Ying, Z.; Cheng, J. Attribute-based secure announcement sharing among vehicles using blockchain. *IEEE Internet Things J.* **2021**, *8*, 10873–10883. [CrossRef]
110. Maaroufi, S.; Pierre, S. BCOOL: A Novel Blockchain Congestion Control Architecture Using Dynamic Service Function Chaining and Machine Learning for Next Generation Vehicular Networks. *IEEE Access* **2021**, *9*, 53096–53122. [CrossRef]
111. Sharma, S.; Kaushik, B.; Rahmani, M.K.I.; Ahmed, E. Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles. *IEEE Access* **2021**, *9*, 147114–147128. [CrossRef]
112. Xu, X.; Zeng, Z.; Yang, S.; Shao, H. A Novel Blockchain Framework for Industrial IoT Edge Computing. *Sensors* **2020**, *20*, 2061. [CrossRef]
113. Xia, S.; Lin, F.; Chen, Z.; Tang, C.; Ma, Y.; Yu, X. A Bayesian Game Based Vehicle-to-Vehicle Electricity Trading Scheme for Blockchain-Enabled Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6856–6868. [CrossRef]
114. She, W.; Liu, Q.; Tian, Z.; Chen, J.-S.; Wang, B.; Liu, W. Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 38947–38956. [CrossRef]
115. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. Trust model for secure group leader-based communications in VANET. *Wirel. Netw.* **2019**, *25*, 4639–4661. [CrossRef]
116. Liang, J.; Chen, J.; Zhu, Y.; Yu, R. A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position. *Appl. Soft Comput.* **2019**, *75*, 712–727. [CrossRef]
117. He, Y.; Yu, F.R.; Wei, Z.; Leung, V. Trust management for secure cognitive radio vehicular ad hoc networks. *Ad Hoc Netw.* **2019**, *86*, 154–165. [CrossRef]
118. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 13.
119. Khelifi, H.; Luo, S.; Nour, B.; Moungla, H.; Ahmed, S.H.; Guizani, M. A blockchain-based architecture for secure vehicular Named Data Networks. *Comput. Electr. Eng.* **2020**, *86*, 106715. [CrossRef]
120. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *IOT* **2018**, *1–2*, 1–13. [CrossRef]
121. Luo, B.; Li, X.; Weng, J.; Guo, J.; Ma, J. Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2034–2048. [CrossRef]
122. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.-Y.; Bashir, A.K.; El-Latif, A.A.A. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
123. Tan, H.; Chung, I. Secure Authentication and Key Management with Blockchain in VANETs. *IEEE Access* **2019**, *8*, 2482–2498. [CrossRef]
124. Hu, W.; Hu, Y.; Yao, W.; Li, H. A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles. *IEEE Access* **2019**, *7*, 139703–139711. [CrossRef]