future internet

MDPI

Review

Blockchain Application in Internet of Vehicles: Challenges, Contributions and Current Limitations

Evgenia Kapassa *, Marinos Themistocleous, Klitos Christodoulou and Elias Iosif

Institute for the Future, Department of Digital Innovation, University of Nicosia, Nicosia 2414, Cyprus; themistocleous.m@unic.ac.cy (M.T.); christodoulou.kl@unic.ac.cy (K.C.); iosif.e@unic.ac.cy (E.I.)
* Correspondence: kapassa.e@unic.ac.cy

Abstract: Blockchain technology is highly coupled with cryptocurrencies; however, it provides several other potential use cases, related to energy and sustainability, Internet of Things (IoT), smart cities, smart mobility and more. Blockchain can offer security for Electric Vehicle (EV) transactions in the Internet of Vehicles (IoV) concept, allowing electricity trading to be performed in a decentralized, transparent and secure way. Additionally, blockchain provides the necessary functionalities for IoV decentralized application development, such as data exchange, personal digital identity, sharing economy and optimized charging pattern. Moreover, blockchain technology has the potential to significantly increase energy efficiency, decrease management costs and guarantee the effective use of the energy recourses. Therefore, its application in the IoV concept provides secure, autonomous and automated energy trading between EVs. While several studies on blockchain technology in smart grids have been conducted, insufficient attention has been given to conducting a detailed review and state-of-the-art analysis of blockchain application in the IoV domain. To this end, this work provides a systematic literature review of blockchain-based applications in the IoV domain. The aim is to investigate the current challenges of IoV and to highlight how blockchain characteristics can contribute to this emerging paradigm. In addition, limitations and future research directions related to the integration of blockchain technology within the IoV are discussed. To this end, this study incorporates the theoretical foundations of several research articles published in scientific publications over the previous five years, as a method of simplifying our assessment and capturing the ever-expanding blockchain area. We present a comprehensive taxonomy of blockchain-enabled applications in the IoV domain, such as privacy and security, data protection and management, vehicle management, charging optimization and P2P energy trading, based on a structured, systematic review and content analysis of the discovered literature, and we identify key trends and emerging areas for research. The contribution of this article is two-fold: (a) we highlight the limitations presented in the relevant literature, particularly the barriers of blockchain technology and how they influence its integration into the IoV and (b) we present a number of research gaps and suggest future exploratory areas.

Keywords: blockchain; Internet of Vehicles; Electric Vehicles; opportunities; limitations; systematic literature review

Citation: Kapassa, E.; Themistocleous, M.; Christodoulou, K.; Iosif, E. Blockchain Application in Internet of Vehicles: Challenges, Contributions and Current Limitations. *Future Internet* **2021**, *13*, 313. https://doi.org/10.3390/fi13120313

Academic Editor: Daniel Gutiérrez Reina

Received: 9 November 2021
Accepted: 8 December 2021
Published: 10 December 2021

1. Introduction

1.1. Motivation and Problem Statement

Given the technological breakthroughs in communications, sensors, and electrical systems, traditional embedded systems and controllers are being overtaken with a more advanced system, known as a Cyber–Physical System (CPS). This CPS is typically linked to internet technologies to provide a link between the cyber and physical worlds [1]. CPS has recently gained popularity and has already been widely used in various parts of our lives. One example of CPS is the Intelligent Transportation System (ITS). The main objective of ITS is to create comfortable, secure, dynamic, and efficient transportation within ITS and smart cities in general [2]. Within the ITS, a concept named Internet of Vehicles (IoV) is presented,

which is powered by smart vehicles, Internet of Things (IoT), and Artificial Intelligence (AI) methods. Cars are becoming smart vehicles that can communicate with other vehicles, drivers, passengers, and road-side units (RSUs) through the Internet and Dedicated Short Range Communication (DSRC) technology (i.e., short-range to medium-range wireless communication channels) [3]. Internet of Vehicles, in conjunction with the fast deployment of Electric Vehicles (EVs) and the use of renewable energy in the day-to-day activities of energy users, is leading to the emergence of a greener, smarter community. Nevertheless, load-balancing issues, security concerns, privacy leaks, and a lack of incentive mechanisms remain unsolved [4]. Another issue for IoV is the rapidly increasing number of cars and objects linked to the IoV [5]. As a result of this circumstance, a significant volume of data has to be managed on a wide scale. When the data amount is huge, the reliability of data propagation in the network becomes a major concern. Many techniques have been proposed in the literature to address the aforementioned issues [6,7]. However, due to the resource and time demands of basic cryptographic computations on network devices, these techniques are insufficient to produce good results. In most situations, energy trading systems use a centralized method to manage transactions between EVs and other IoV objects (e.g., charging stations). This approach raises the probability of a single point of failure and, thus, the respective cost increases [8]. Moreover, dynamic wireless charging is a promising technology to charge EVs using on-road charging segments. In order to ensure the effective utilization of wireless charging, communication and coordination need to be established between the EVs and the different network entities [9]. Therefore, forming an IoV is required in this scenario. However, considering the V2X communication, wireless EV charging presents significant challenges in terms of reliable communication and secure authentication [10]. Thus, due to the aforementioned limitations, the present system and the communication protocols cannot provide sufficient response to the underlying IoV requirements and the emerging EV use cases.

1.2. Blockchain Value in IoV

Trying to overcome the aforementioned challenges, blockchain has emerged as a transformative technology in the context of the ITS and smart grids, enabling secure and reliable Peer to Peer (P2P) energy trading (i.e., P2P energy trading allows local distributed energy generators to sell their electricity at the desired price to consumers willing to pay that price) between Distributed Energy Resources (DERs), including EVs [11]. Due to blockchain's nature, a stable, open and decentralized ledger could be established for all data and transactions, related to energy production and consumption [12]. In addition, smart contracts can enable transparent and immutable transactions on the IoV and promote interconnections between EVs, RSU and charging stations in a decentralized and fault-tolerant environment [13]. Thus, a solution such as blockchain that does not have a central trust authority to ensure energy transactions in the IoV [14], is essential for creating a highly available, secure and privacy-protected environment. Furthermore, blockchain can deliver a significant number of novel solutions in most of IoV applications. The majority of such applications are real-time and mobile, generating and exchanging a huge quantity of data. Incorporating blockchain into IoV enhances system efficiency and automation while also increasing security, privacy, and dependability [5,15,16]. IoV built on blockchain has the potential to establish a new ecosystem for the transportation and car industries in which value can be transferred and maintained in a safe, transparent, immutable, and efficient manner. Moreover, the adoption of blockchain to the existing IoV can result in substantial improvements in terms of safety, efficiency and information delivery.

1.3. Contributions

While there have been numerous studies of blockchain technology in smart grids and P2P energy trading, the authors contend that the state-of-the-art of blockchain-enabled applications in the IoV has received little attention. The approach proposed in [17] does not address the entire scope and applicability of blockchain opportunities in the IoV. Instead,

the security aspects of the IoV systems and the issues of integrating blockchain within the IoV were given emphasis. Other studies focus on the specific function of blockchain, such as the creation of decentralized and data-intensive smart grids [14,18], and the integration of blockchain with IoT [19,20], while some of them are focused on the energy sector, providing a holistic view of the blockchain capabilities in this sector [21–23]. Conclusively, there is an absence of a concrete and comprehensive evaluation of existing blockchain related state-of-the-art analysis, relevant to the current opportunities and limitations in the IoV domain. The latter was the major driver for undertaking this research. Our study adds to a comprehensive understanding of blockchain capabilities and gives a picture of existing blockchain-enabled applications across the IoV domain and, specifically, the IoV-assisted smart grids. Even though smart grid is a well-known term, which refers to an electricity network/grid enabling a two-way flow of electricity and data, an IoV-assisted smart grid may be a little ambiguous. In the context of this research, an IoV-assisted smart grid refers to a smart grid which is supported by the IoV key functionalities (i.e., as those presented at the beginning of this paper), which could assist it in order to achieve flexible resource demand response (DR).

Based on a systematic literature review methodology, the authors provide the following key contributions:

1. A detailed taxonomy of the range of blockchain application areas in the field of IoV.
2. A discussion of the observed IoV challenges of different segments and scenarios of the smart grid domain with the goal of understanding why blockchain should be used and how it may contribute to solving such challenges.
3. A research agenda around the current limitations of blockchain technology in the field of IoV and future research directions are presented.

1.4. Article Structure

The remainder of this article is organized as follows. Section 2 provides the background of the current work, presenting the blockchain preliminaries and its added value in the IoV domain, as well as elaborating on the concept of IoV. Section 3 presents the method followed to conduct the systematic literature review. The descriptive analysis of the retrieved literature is presented in Section 4, discussing the current challenges of IoV-assisted smart grids and the blockchain opportunities in this field. Section 5 presents the systematic literature review findings, highlighting the limitations of using blockchain in the area of IoV-assisted smart grids, as well as providing open issues, trends, and further research lines. Lastly, Section 6 concludes the paper, summarizes its contributions and limitations, and suggests future work.

2. Background: Blockchain for the IoV

Blockchain technology is one of the most current topics that has piqued the interest of many companies and researchers owing to the numerous advantages it offers over conventional alternatives, such as cryptography techniques and trust management. Blockchain is a distributed database that does not require a central authority and does not require third-party verification. A blockchain is composed of blocks, and each block has a hash of the preceding block, forming a chain of blocks from the genesis block to the present block (i.e., genesis block does not relate to a prior block). Most nodes should register their agreement in order to record a transaction in the distributed ledger. This necessitates the use of a consensus mechanism. Proof of Stake (PoS) and Proof of Work (PoW) are the most frequent and widely used consensus algorithms. Blockchain has the potential to provide significant benefits in a variety of industries and applications, including IoV. This new technology shares some common features that involve decentralization, transparency, immutability, better security, anonymity, cost reduction and autonomy.

It is evident within the literature that blockchain is widely used for addressing the privacy and security concerns of a variety of use cases. However, it is of paramount importance to highlight that blockchain is complementing existing techniques such as cryp-

tography (e.g., elliptic curve cryptography) and identity management (e.g., self-sovereign identity management and the K-Anonymity algorithm).

As briefly stated in the Introduction, the Internet of Vehicles is regarded as being among the most active research domains in ITS, integrating VANET and IoT. The IoV combines two scientific visions: (a) vehicle connectivity and (b) vehicle intelligence, focusing on the integration of objects such as persons, cars, things, networks and surroundings [24]. Because of the combination of communication and information technology in the IoV, it is advantageous in addressing numerous traffic and driving difficulties, which contributes to the safety of passengers and the overall driving experience [25]. Therefore, based on the existence of multiple technologies in the IoV ecosystem, researchers proposed an architecture consisting mostly of four layers [26,27].

1. The first layer (i.e., the sensing layer) comprises all the sensors within the vehicles, which collect data and identify particular events of interest such as driving patterns, vehicle circumstances, weather conditions, etc.
2. The second piece (i.e., the communication layer) enables various wireless communication modes (e.g., V2V and V2I). The communication layer ensures that existing and future networks are always connected (such as GSM, Wi-Fi, LTE and Bluetooth, among others).
3. The third layer (i.e., computing) is in charge of storing, analyzing, processing and making decisions regarding various circumstances in the IoV network. This layer also provides data computing services.
4. Finally, the application layer is the highest level of the IoV and may provide consumers with a range of vehicle services.

Figure 1 displays an example of a hybrid blockchain and IoV architecture in light of the preceding discussion. The blockchain acts as a governance layer and may be viewed as a bridge between the communication and application layers [24,27–29]. In such an expanded IoV architecture, blockchain may supply blockchain-based solutions and bundle data into new blocks. Furthermore, it may leverage incentive mechanisms to incentivize users to share information resources by rewarding a certain number of tokens, allowing users to actively contribute transaction information to the system.

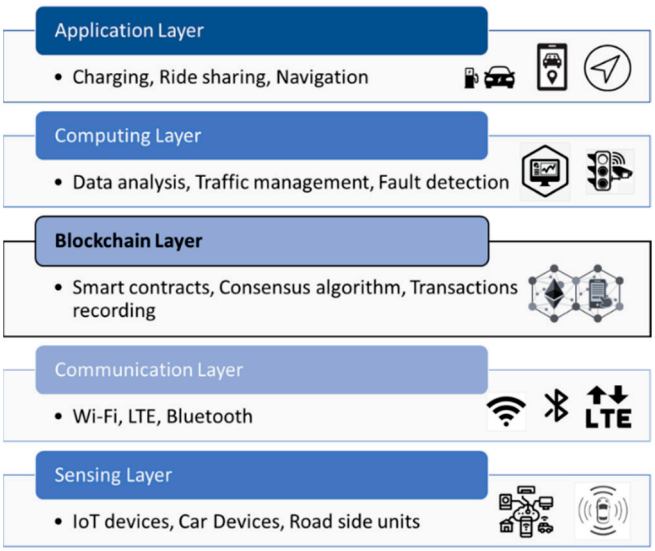

Figure 1. Blockchain and IoV architecture.

3. Review Method

The current study was carried out utilizing one of the most effective and commonly used Systematic Literature Review (SLR) approaches in the world of software engineering, namely Kitchenham's approach [30]. This technique presents rigorous steps for analyzing

research knowledge while adhering to a reliable and auditable methodology. However, several authors have questioned Kitchenham's technique and/or offered modifications to it [31]. Kitchenham released a revised version of her approach in [32] in response to these critiques and recommendations for improvement. This SLR adheres to the most recent version of Kitchenham's technique, as mentioned above. It outlines three stages for carrying out a systematic review:

- Planning, which defines aspects such as the need for the research, the review protocol and research questions;
- Conducting, during which the previously established protocol is carried out;
- Reporting, which presents the final analysis to answer each research question.

Figure 2 shows these phases and their tasks on a timeline to achieve the research objective of this article.

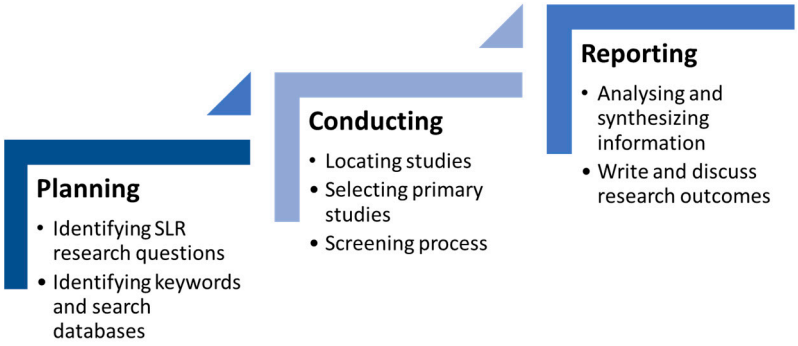

Figure 2. Systematic literature review phases.

3.1. Planning the Review

This section explains the planning approach that was used in this SLR. The goal for the review was determined throughout this process, as were the research questions (RQs) and the review protocol.

3.1.1. Study Goal and Systematic Literature Review Questions

The aim of this stage was to investigate the adoption of blockchain in the IoV, identify current issues and provide future research directions. The goals that concerned the outcome of this research were extracted based on taxonomy characteristics for the review [33], and are the following:

- Identify the main problems in the IoV where blockchain technology is applied, considering current challenges in the IoV landscape, opportunities for blockchain application and current limitations;
- Discuss findings and provide future research directions.

A systematic review is based on pre-defined questions [30,32]. Thus, the identified SLR questions (SLR.Q) guided many aspects of the review process, including determining eligibility criteria, searching for studies, collecting data from included studies and discussing the findings. The questions that guided the current SLR were the following:

- SLR.Q1: How can blockchain be applied in smart grids and especially in the IoV concept?
- SLR.Q2: What are the current challenges in the IoV?
- SLR.Q3: What are the opportunities of blockchain in the area of IoV?
- SLR.Q4: What are the limitations of the current research?

3.1.2. Review Protocol

Another essential procedure of the literature review is the definition of the search process (i.e., the review protocol). The research protocol was described in a documented definition of the review process, based the approach given in [34], to categorize literature

reviews. Specifically, the authors of the current review considered the following aspects during the definition of their review protocol:

- Search strategy for identification of studies: databases and sources to be searched, included time periods, search terms and keywords, search queries, language restrictions;
- Screening: inclusion/exclusion criteria for studies;
- Validation: pattern recognition and taxonomy creation;
- Data extraction and Synthesis: type of synthesis to be used, representation of data to address review questions.

3.1.3. Search Strategy

During the planning phase, the authors identified a set of search keywords and databases. Since the research questions (RQ1–RQ4) are related to the combination of blockchain technology with the IoV—two emerging concepts that have drawn scientific attention in recent years—the systematic literature search was conducted from 2017 onwards. The selected database sources for the search were Google Scholar (i.e., since it includes a broad field of publications), IEEEXplore, ScienceDirect, SpringerLink and ACM Digital Library. As this particular study is focused on scientific information about blockchain applicability in relation to the IoV concept, the authors focused on literature published in academic journals, conference proceedings and book chapters, which helped ensure quality. Afterwards, the authors decided on the keywords to be used in the study (i.e., the "*" sign was used at the end/beginning of some keywords to expand the range of possible studies, since many papers use slightly different keywords for the same concept, e.g., "connected vehicles" instead of "electric vehicles"). Initially, the authors attempted to extract all relevant publications based on the submitted keywords (a) blockchain and (b) energy. The results from the previous queries were referring to a specific keyword, which led to the identification of more relevant keywords around the domain of interest. The knowledge gained by the previous results guided the researchers in the construction of new keyword queries submitted in the researched databases. Table 1 presents the selected databases as well as the search queries used to identify the relevant studies for the review.

Table 1. Selected databases, keywords and queries.

Databases	Keywords	Search Queries
Google Scholar	blockchain, energy	"blockchain AND energy"
	renewable energy	"blockchain AND "renewable energy""
IEEEXplore	blockchain, microgrid	"blockchain AND microgrid"
	blockchain, energy trading	"blockchain AND "energy trading""
ScienceDirect	blockchain, V2V	blockchain AND ("* vehicle" OR V2G OR V2V OR IoV)
SpringerLink	blockchain, V2G	
ACM Digital Library	blockchain, IoV	
	blockchain, * vehicle	

3.2. Conducting the Review

3.2.1. Study Locations

The submission of the search queries in the electronic databases returned thousands of results in one database (e.g., IEEEXplore), while fewer results were returned from others (e.g., ACM). However, the authors were unable to apply the same set of search queries to each database due to the various database models. To extract relevant information from the research databases, the authors created various queries based on the goal of the study. The submitted queries for the different selected databases are presented in Appendix A. The location process resulted in an initial number of 5688 publications. Before moving to the screening process, the authors checked for possible duplicates within the union of the results of all databases. The results assessed in the screening, after removing the duplicates, totaled 5412, as depicted in Figure 3.

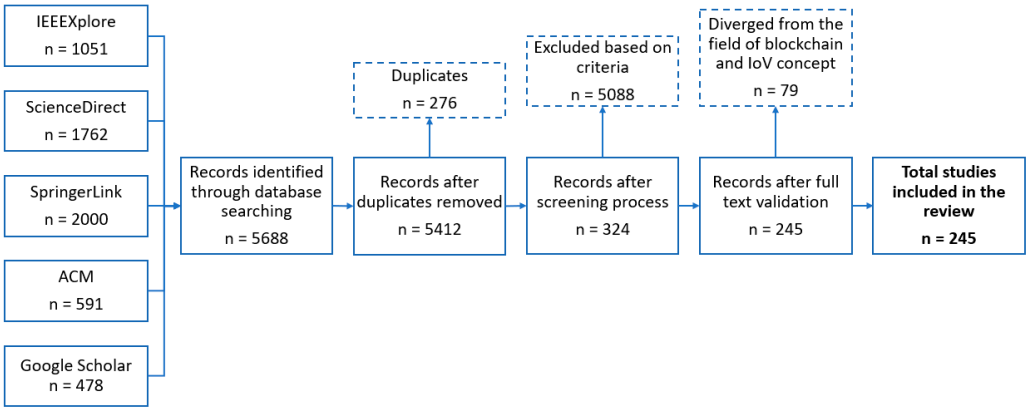

Figure 3. Procedure for identifying selected studies.

3.2.2. Screening

The authors evaluated the eligibility and quality of the selected literature based on a set of specified quality criteria for exclusion and inclusion, as presented in Table 2. Some exclusion criteria were used before introducing the literature in the bibliographic manager (i.e., we used Mendeley in the current review), such as language, publication year and document type restrictions. Initially, the titles, keywords and abstracts of all research papers were assessed. Publications that met one of the exclusion parameters were omitted and sorted by exclusion.

Table 2. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Peer-reviewed studies	Grey literature
Academic theoretical and empirical research	White papers and material from non-academic sources
Full-text available	Full-text not available
Written in English language	Written in non-English language
Published in 2017 onwards	Published before 2017
Relevant to blockchain and IoV concept	Diverged from the field of blockchain and IoV concept
Concept addressed by means of a valid methodology	

3.2.3. Validation

After the location of the initial set of studies and the definition of the inclusion and exclusion criteria, the authors carefully read the abstract, keywords and titles of the initial 5412 papers, with the goal of identifying the primary research studies. In order for a study to be considered as eligible for the review, it needed to meet all the inclusion criteria. Then, the authors focused on two eligibility criteria during the reading of abstracts: "Is the paper relevant to blockchain and/or DLT?" and "Does the paper describe a concept/framework/study relevant to smart grids, electric vehicles or IoV in general?". Papers had to meet both criteria in order to be considered. Using this procedure, the authors were left with 324 papers. After the screening process, the authors proceeded to the full-text validation of the selected studies. The authors excluded 79 studies that were not relevant to the goal of the review, resulting in 245 studies remaining. These were the papers that the authors studied in order to reach the goals of the current systematic literature review and answer the research questions. The primary studies are provided in Appendix B.

3.3. Reporting the Review

Based on [30,32], the goal of this process was to utilize data extraction forms to properly record the information gathered by the authors from the primary study selection.

For the data extraction process, a framework was formed by the authors using Microsoft Excel. The data extracted from each study were the following:

- Study details including authorship, year, type of paper, publication location and digital object identifier;
- Summary of the study and description of the observed thematic area;
- Main application area;
- Evaluation of the study in terms of research knowledge including the identified problems;
- Proposed solutions/opportunities, study outcomes and study limitations and/or research directions;
- Evaluation of the study in terms of technological knowledge, including concept validation and blockchain network used.

From the considered-studies cluster of 245, the most interesting ones once were selected (excluding the documents in the form of surveys or literature reviews, which were also considered separately), to highlight the main current research trends and the gaps that have yet to be filled. The selection was based on the Interest Tag (i.e., low, medium, high). The authors selected only the studies tagged as "high" that were of the highest importance. At this point, it should be stated that the decisions determining whether studies were considered to be of high importance were based on two factors:

- The study should be sufficiently evaluated in terms of research knowledge;
- The study should be evaluated in terms of technological knowledge.

The selected studies are presented in Appendix B, and they are grouped by application area. The following features are highlighted: (a) authors and publication year, (b) application area, (c) identified problems, (d) study outcomes and (e) study limitations and/or research directions. The majority of the studies were high quality conference proceedings and journal articles, although some book chapters were also analyzed. In 2021, the published articles had the highest rank. A clear depiction of the types of publications identified is presented in Figure 4, while the distribution of them within the time range of the review is presented in Figure 5.

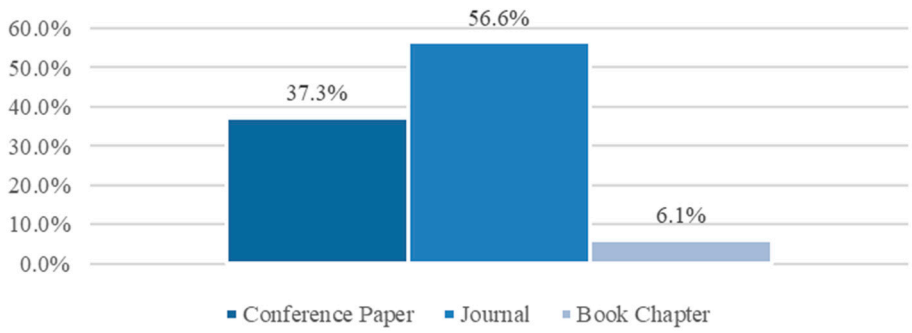

Figure 4. Study types as percentages.

During the analysis process, the authors classified blockchain applications within the IoV into eight main categories according to their purpose and field of activity:

- Privacy and security;
- Data protection and management;
- P2P energy trading;
- Microgrid management;
- IoV management;
- AI/Machine Learning (ML) and IoV;
- Blockchain performance in the IoV;
- General-purpose studies (e.g., reviews, surveys, etc.).

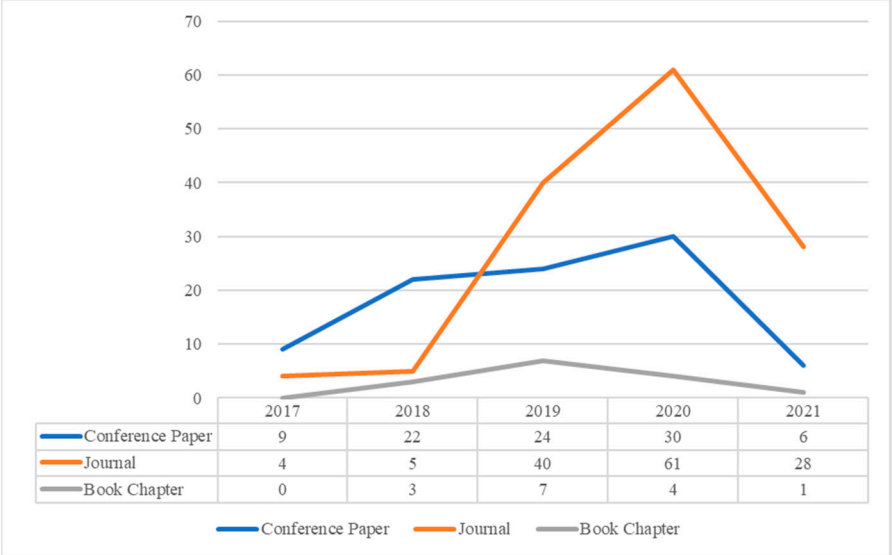

Figure 5. Distribution of studies from 2017 to 2021.

The taxonomy of the identified application areas is depicted in Figure 6. The authors found that approximately one in three applications were about Privacy & Security (27%), which included authentication, Vehicle to Everything (V2X) and identity management initiatives. The second most popular category was IoV Management (25.8%). This was followed by P2P Energy Trading and general-purpose studies, accounting for 12.7% and 12.3% of total studies, respectively. Other application areas made up around 22% of the total, as presented in Figure 7.

From the abovementioned facts, it is obvious that the impact of blockchain in smart grids and especially in the car industry has been widely assessed. Blockchain is now receiving more attention in the IoV sector, where its transformative potential also appears impressive, as will be presented in Section 4. This led the authors to further investigate the blockchain adoption in each one of the identified IoV application areas. The authors gathered this kind of information following an algorithmic approach, leveraging an algorithmic model, based on web-harvested information for assessing the blockchain's correlation with different applications (e.g., charging management, pricing schemes, etc.), as initially described in [35]. In this model, the basic idea is to apply web mining techniques to estimate the strength of association between two words/terms. This approach has been widely used in areas such as information retrieval and natural language processing, which deal with (mostly) textual data, while the world wide web (www) is regarded as the largest possible source of data. Based on the latter hypothesis (i.e., www as the largest source), the use of appropriate tools, both for indexing and querying, is needed. For this purpose, the employment of standard search engines—through their respective APIs—constitutes a common practice. Motivated by the above considerations, we used the Google web search engine. For every application (Table 3), an association score was computed between this application and the term "internet of vehicles". For example, for the "pricing scheme" application, the association score was computed by calculating the Pointwise Mutual Information (PMI) between "pricing scheme" and "internet of vehicles", taking into account the number of hits (i.e., the number of search results) as returned by the used web search engine. More details about PMI can be found in the indicative works of [36,37], where in the latter, PMI is applied over www data. The results are shown in Table 3. It appears that higher positive scores indicate a stronger association, while scores that lie closer to 0, as well as negative scores, suggest weaker associations.

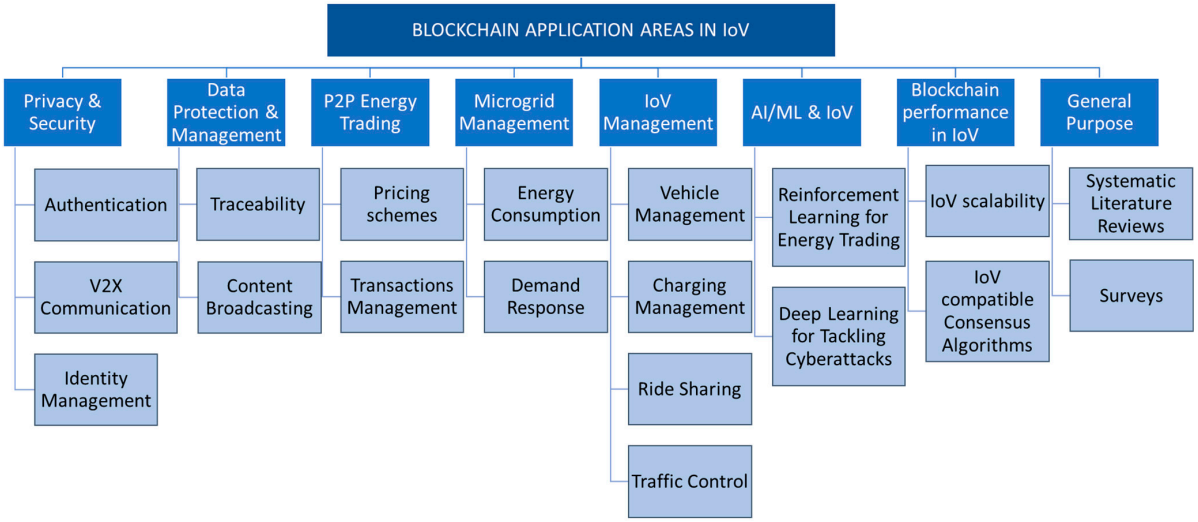

Figure 6. Blockchain application areas in the IoV.

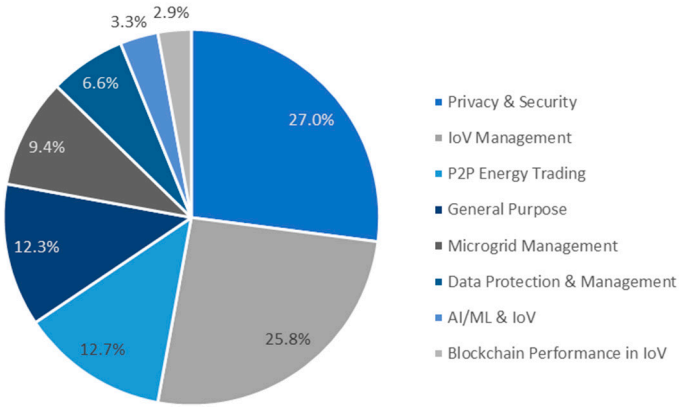

Figure 7. Blockchain applications in the IoV—classification according to their application areas.

Table 3. Association of blockchain in different IoV application areas: results.

Application Area	Correlation Result
Ride sharing	1.499
Energy consumption	1.121
Pricing schemes	1.049
Data protection	0.491
Charging management	0.468
Traffic control	0.415
V2X communication	0.300
Demand response	0.095
Machine learning	0.047
Incentive mechanisms	−0.032
Identity management	−0.157
Network performance	−0.369
Regulation	−0.398

In terms of the results, as also depicted in Figure 7, blockchain technology is currently widely adopted in the areas of ride sharing, studies on energy consumption and pricing schemes that are related with different IoV participants. It is also observed that there is a significant correlation of blockchain in the areas of charging management, V2X communications, traffic control and data protection. The correctness of the aforementioned scores and observations is also justified by the literature, considering that they are included in the top

three categories, as depicted in Figure 7. On the other hand, for the areas that had a negative score or a score close to zero (e.g., demand response, incentive mechanisms, network performance, etc.), it is believed and justified—both from the web mining process and from the literature—that they do not have a high blockchain adoption rate yet. This is justified by their weak association rate with blockchain. However, as will be further discussed in Section 4, there are some application areas that are currently rising and need further investigation. Thus, areas such as demand response management, incentive mechanisms and network performance are considered to be limitations of the blockchain integration in the area of IoV. The association result is justified by the fact that, at present, there is minimal work conducted (i.e., either academic or industrial) in this field of study.

Additionally, blockchain activities, according to the platform used, were also classified wherever information was made available. As depicted in Figure 8, 53.4% of the research work developed solutions based on Ethereum, while 19.2% used Hyperledger Fabric. In addition, IOTA is gaining ground, with 8.2% of researchers selecting this platform for evaluation purposes. Other blockchain platforms include Hashgraph, Corda, Hyperledger Indy, Hyperledger Sawtooth, Interchain, Cosmos and Binance. At this point, the authors choose to disclaim that the fourth most used platform is Hyperledger. However, the corresponding studies did not highlight which frameworks were used in particular (i.e., comparing with author studies that mention the framework used, as depicted in Table 4 and Figure 9).

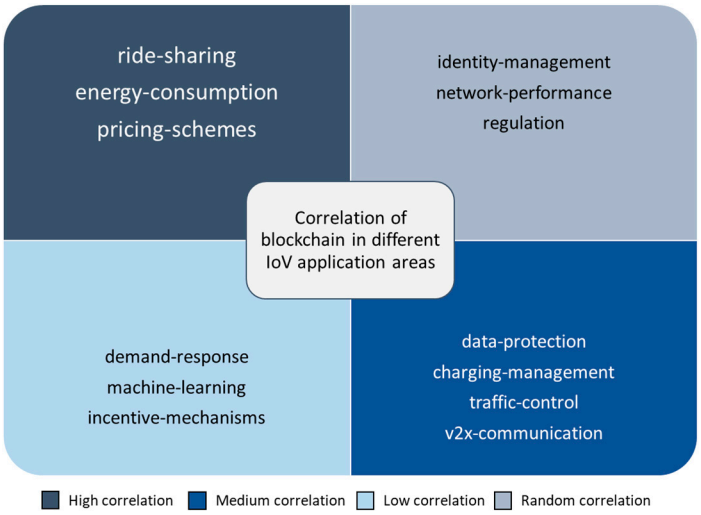

Figure 8. Matrix of blockchain in different IoV-associated areas.

Table 4. Association of blockchain in different IoV application areas: results.

Blockchain Platforms Used in IoV	Platform Adoption Percentage
Ethereum	53.4%
Hyperledger Fabric	19.2%
IOTA	8.2%
Hyperledger	4.1%
Hashgraph	2.7%
Binance	1.4%
Bitcoin	1.4%
Ganache	1.4%
Corda	1.4%
Exonum	1.4%
Hyperledger Indy	1.4%
Hyperledger Sawtooth	1.4%
InterChain	1.4%
Cosmos	1.4%

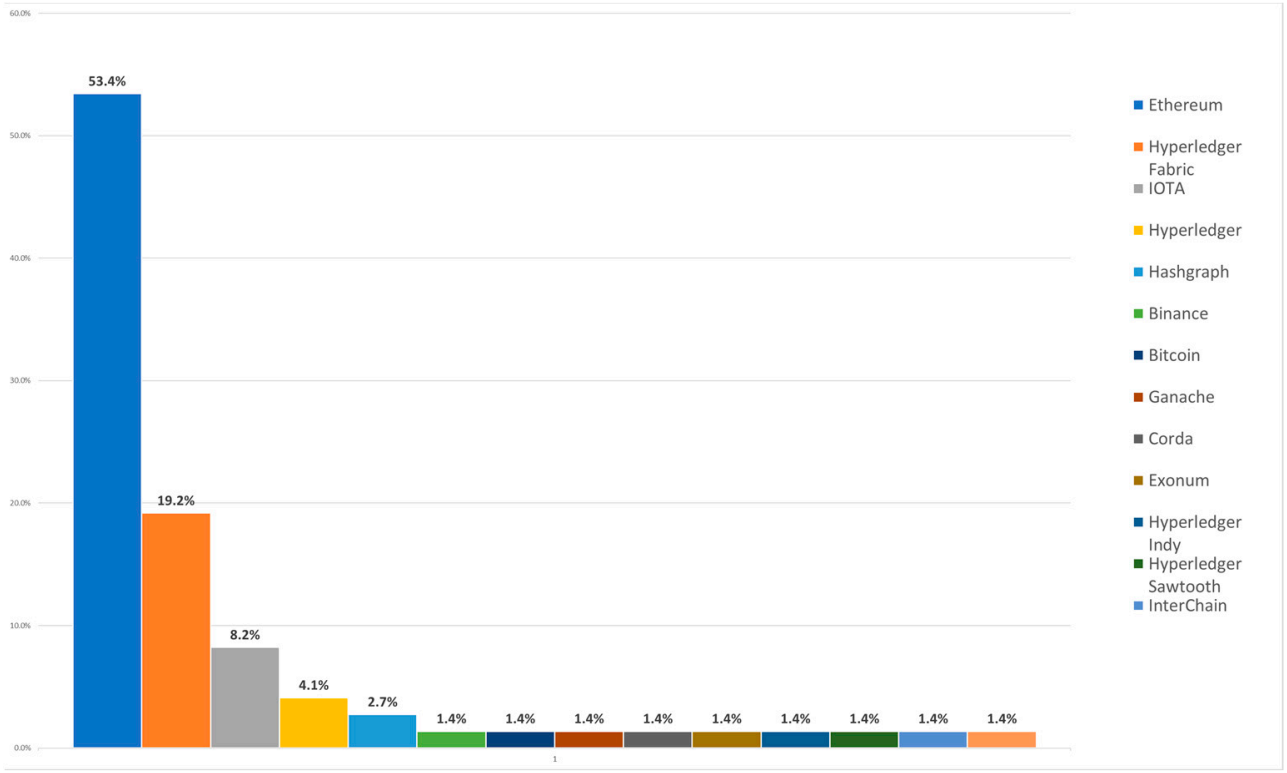

Figure 9. Blockchain application in the IoV—classification according to blockchain platform.

4. Discussion

This section presents the findings of the systematic literature review. Based on the conducted analysis, the authors provide a detailed presentation regarding the following: (a) the identified challenges of IoV-assisted smart grids, (b) the blockchain contributions and advantages in this field and (c) the limitations of blockchain adoption in smart grids. This section concludes by providing an overview of open research problems that need further investigation.

4.1. Challenges of IoV-Assisted Smart Grid

Internet of Vehicles is an emerging concept that is believed to help realize the vision of ITS within smart grids. Within this paradigm, the vehicles will be able to communicate with each other and with their environment: pedestrians, devices, traffic signs, etc. Thus, efficient road safety and global traffic efficiency applications will be developed and deployed, reducing traffic causalities [25]. Moreover, a massive amount of data will be introduced and outsourced to the cloud and edge storage from the vehicles as well as vehicular services that will be innovated for IoV.

However, the integration with existing internet technologies to support the IoV paradigm opens up many challenges [3,25] including security, privacy, trust, transparency, connectivity and performance. It is important to state, however, that the aforementioned challenges are common issues with the IoT paradigm and have been extensively researched [38–41]. IoV, on the other hand, incorporates some unique characteristics compared to IoT, such as mobility and energy demand-response [17]. Thus, the IoV ecosystem might bring a number of novel challenges within smart grids. Such unique challenges of the IoV-assisted smart grids are presented in Figure 10 and described below:

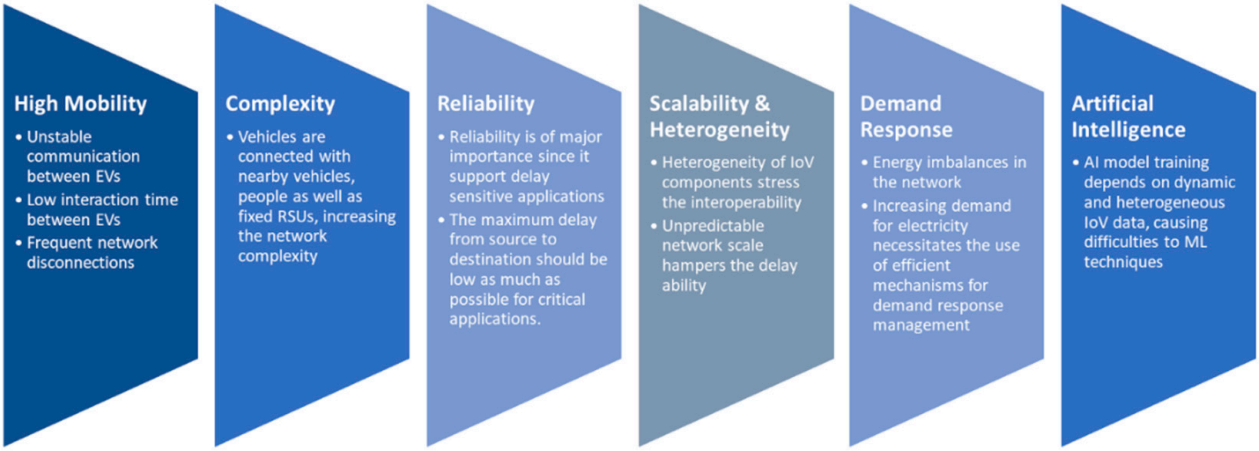

Figure 10. Challenges of IoV-assisted smart grids.

Challenge 1—High mobility: Within IoV applications, all types of EVs are seen as fast-moving objects that often operate along roadways. Likewise, the operating speeds of the vehicles may differ, creating different mobility patterns, especially for manually driven vehicles [42]. As a result of the mobility of nodes in the IoV, it is difficult to correctly analyze the number of nodes that engage in the network. Furthermore, even if vehicles have the appropriate energy to utilize computational and communication resources when they connect with nearby objects, vehicles will struggle to maintain consistent connection due mainly to their variety and rapid mobility characteristics [17,43], which would possibly bring additional challenges. One example is the difficulty of transmitting vehicles' critical data due to restricted transaction times, which are caused by the aforementioned mobility issues of the vehicles [44].

Challenge 2—Complexity: The IoV environment is built on a wireless communication network that supports a variety of wireless technologies. In this environment, vehicles communicate wirelessly with surrounding vehicles, humans and RSUs [45,46]. Bluetooth and DSRC are examples of typical technologies that provide a variety of wireless network-related services (e.g., communication, message exchanges) in the IoV. Furthermore, the cars' network topologies vary due to their mobility, as discussed previously. As a result, the effects of network complexity on IoV scenarios are considerable.

Challenge 3—Reliability in critical applications: In order to support mission-critical applications in the IoV (e.g., first responder communication and transportation systems), services with low communication latency and high reliability are required [47–49]. These latency-sensitive applications have propagation lengths that range from short to medium. As a result, the maximum time between the source and destination should be as short as possible for them. For instance, in emergency and safety-related applications, communication must be completed within a specific time frame in order to avoid potentially hazardous circumstances such as accidents [50]. Nonetheless, satisfying the service demand is difficult owing to the specific characteristics of the IoV, such as restricted wireless connection bandwidth, rapid vehicle mobility, quick data transfer and computing overhead.

Challenge 4—Scalability and Heterogeneity: Considering the diverse nature of the IoV components, which include heterogeneous devices, protocols and platforms, smooth integration with cutting-edge information and communication technologies is required. The variety of IoV components may pose another obstacle to interoperability [51]. Interoperability describes the capacity of IoV components to interact in terms of information consumption and sharing throughout different sectors, systems, devices and applications, considering both software and hardware. As stated within the literature [52], it may be challenging to create an efficient and interoperable solution that meets all of the IoV restrictions and the criteria required for IoV deployment.

Challenge 5—Demand Response: In recent years, demand response has played an active part in the energy ecosystem (e.g., providers offer time-of-use pricing to their cus-

tomers). Traditionally, balancing electrical supply and demand was very straightforward, thanks to large and controlled power facilities on the one hand and reasonably predictable demand on the other [53,54]. However, in recent years, smaller, more variable and less predictable renewable energy sources have emerged (i.e., the rise of the smart grid). Thus, as the traditional energy grid is switching towards the smart grid, it is becoming increasingly vital to address the demand response problem. Expanding demand for electricity in smart grids requires the adoption of effective Demand Response Management (DRM) [55]. Balancing supply and demand is becoming increasingly difficult as the energy grid needs greater flexibility. Smart meters, interconnected appliances and in-home monitors bring up new opportunities for demand-side innovation. For example, empowered customers may progressively engage by changing their consumption patterns [56].

Challenge 6—Artificial Intelligence: Intelligent transportation incorporates complicated applications that need intelligent decision-making. As a result, the progress of AI and ML found its way into IoV, resulting in the explosion of smart vehicles. This emergence led several businesses to invest in AI for IoV applications such as autonomous driving, real-time navigation, traffic monitoring and more [57]. Despite the advantages of AI for IoV, its application may be limited by a lack of computing resources and the processing of untrustworthy data. Because the IoV infrastructure is tightly connected with the Edge (i.e., Edge computing takes place near the source of the data rather than depending on the cloud at data centers to handle all of the work), the available resources are restricted, making AI task allocation a difficult process. As a result, another issue is managing the IoV network's resources and scheduling its traffic [58]. Moreover, since many AI algorithms rely heavily on vehicle data to train the corresponding models, the dynamic and diverse characteristics of the IoV environment complicate the implementation of such approaches [59].

Challenge 7—Privacy and Security: Although privacy and security are well-known considerations in the IoT space, they are relevant enough to be highlighted, since they are also among the most critical in the IoV ecosystem. The IoV needs strong security and privacy solutions to reduce misleading and malicious information exchanges between vehicles. Such occurrences can result in a variety of accidents that endanger drivers, passengers and pedestrians [60]. IoV security risks may be classified further into the physical, communication and application levels. At the physical level, the different IoV components (for example, EVs, RSUs and so on) are vulnerable to unauthorized access and illegal behavior, resulting in a threat of data security and reliability [39,61]. Furthermore, malicious EVs may initiate Sybil attacks by posing as several non-exiting EVs. Malicious EVs might use a Denial of Service (DoS) attack (i.e., an attack meant to shut down a machine or network, making it inaccessible to its intended users) to submit repeated offers without committing to them, preventing other EVs from charging, and thus, making the IoV trading system unstable and unreliable [62,63]. At the communication level, there are serious issues regarding the creation of safe and fast payments and interactions throughout the IoV ecosystem [64]. Furthermore, due to the mobility and topological unpredictability of the IoV, maintained privacy is not ensured during the resource-sharing process [65]. Lastly, at the application level, the IoV is subject to cloud service issues, which may result in data loss or inadequate storage capacity [66].

4.2. Blockchain Contributions in IoV-Assisted Smart Grid

As stated in Section 4.1, the IoV ecosystem faces several issues, including heterogeneity of IoV systems, poor interoperability, privacy and security risks, network complexity, high vehicle mobility and the smart grid's demand response problem. The application of blockchain within IoV-assisted smart grids can provide several benefits to the present and future intelligent transportation systems [18]. This Section goes through the contributions in the field of smart grids and the IoV environment that are especially related to the features and functioning principles of blockchain, as derived from the current literature.

Over the past few years, blockchain has emerged as a transformative technology in the context of the smart energy grids [67], enabling secure and reliable P2P energy trading between DERs [68]. Due to blockchain's nature, a stable, open and decentralized ledger could be established for all data and transactions, related to energy production and consumption [12]. In addition, smart contracts facilitated through blockchain can enable transparent and immutable transactions on the energy grid and promote interconnections between energy producers and energy consumers (i.e., prosumers) in a decentralized and fault-tolerant environment [69]. Thus, a technology such as blockchain, which does not have a centralized trust body, becomes necessary to ensure efficient and reliable energy trading within the smart grid [13].

Furthermore, blockchain has the ability to deliver a significant number of novel solutions in most IoV applications. The majority of such applications are real-time and mobile, generating and exchanging a huge quantity of data. Incorporating blockchain into IoV enhances system efficiency and automation while also increasing security, privacy and dependability. As a result, researchers have begun to build blockchain-based IoV [5,15,16]. IoV built on blockchain has the potential to establish a new ecosystem for the transportation and car industries in which value can be transferred and maintained in a safe, transparent, immutable and efficient manner. Moreover, the adoption of blockchain to the existing internet of vehicles can result in substantial improvements in terms of safety, efficiency and information delivery. The most compelling reasons for implementing blockchain in IoV-assisted smart grids are presented in Figure 11 and described below:

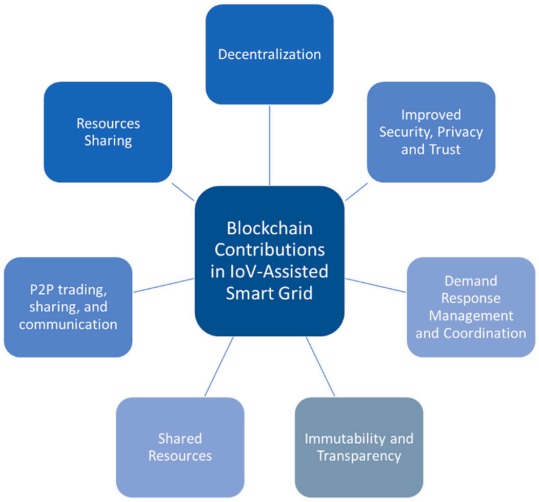

Figure 11. Blockchain contributions in IoV-assisted smart grids.

Contribution 1—Decentralization: A growing number of consumers, producers and prosumers are projected to be accommodated in distributed energy trading scenarios via smart grids. As a result, they should be able to exchange their local generation or excess energy from DERs, such as microgrids, EVs and RSUs, with one another in order to attain benefits such as the lowering of load peaks and the balancing of energy supply and demand. The inherent features of blockchain make it a great option for designing a more decentralized and open energy market and trading system [70], since it is built on a decentralized structure that eliminates centralized entities and third-parties. Blockchain enables the creation of decentralized IoV networks, which comprise more dispersed entities such as RSUs, cars and people [71]. Simultaneously, these distributed entities can autonomously manage their own activities. Current IoV operating principles, which are mostly dependent on central decision-making, will be moved to a decentralized architecture and possibly simplified. Additionally, decentralization will improve the user experience of automotive services.

Contribution 2—Improved Security, Privacy and Trust: As described in Section 4.1, one of the main IoV challenges is related to the privacy and security of the network and the involved parties. The adoption of blockchain in the IoV presents an opportunity

to overcome security risks such as interruption, single-point-of-failure and availability issues [72,73]. This is because of the possibility of blockchain synchronization and replication between all involved peer nodes to the network. As a result, even if one or more nodes fail, the IoV services can continue to operate normally. Blockchain technology is based on advanced cryptographic algorithms to ensure common security and privacy features [74]. In particular, blockchain promotes the greater security and privacy within IoV networks through encryption. Specifically, numerous studies have used blockchain as a privacy-preserving mechanism for privacy protection and energy storage [75], trusted data sharing [76], identity management [77], prevention of malicious attacks, secure tariff decision [78], protected V2G payment mechanisms [79,80], as well as authentication [81] and encrypted vehicular communication [82,83]. Moreover, the decentralized nature of blockchain storage provides safe recording of transactions that occur within a car, and from a car to its surroundings (e.g., other cars or the infrastructure). Transactions within a car are considered (a) any communications transmitted between the various components of a car and (b) information related to the cars' state. Whenever a state is recorded on the blockchain, every component in the IoV network may analyze prior states and messages to determine if the new state constitutes a valid and secure state change.

Contribution 3—Immutability: The integration of blockchain allows increased security for the IoV. The applied cryptographic techniques combined with the consensus mechanism provide data immutability. Once an energy transaction has been included in the blockchain network, it would be very hard to alter this transaction for illegitimate purposes or to delete the transaction, resulting in a very secure and robust system for IoV services and applications [84,85]. Blockchain's immutability characteristic may assist in avoiding data tampering and manipulation, as well as enabling reliable auditing.

Contribution 4—Transparency: Public blockchain is permission-less and is typically open to all entities. Thus, the use of public blockchain potentially opens the door to full access to the data stored in the blockchain and enhances the transparency of the IoV ecosystem. One of the most significant promises of blockchain technology, which provides a completely auditable and legitimate record of transactions, is the ability to provide information transparency. Blockchain ensures transparency by storing data in such a way that it cannot be modified without recording the alterations [86]. Within the IoV environment, blockchain technology will be used to enhance openness in global EV supply chains for raw materials and parts, allowing for their seamless traceability. Transparency is especially crucial when it comes to the usage of such valuable finite resources, most notably EV batteries. This is where BMW has been trying to improve transparency in raw material extraction [87]. Volvo [88] and Volkswagen [89] have also announced their own initiatives that will allow them to accurately trace the origin of their cobalt using the blockchain.

Contribution 5—P2P trading, sharing, and communication: Blockchain allows peer-to-peer trading, sharing and communication between two entities. Recipients and providers of IoV services can communicate directly in such a network. This functionality is very beneficial in IoV environments, since it allows cars and RSUs to safely share data and resources [90,91]. Since the involved actors in an IoV network do not need to interact with any mediator, the final outcome is low-latency applications and services [91]. Moreover, due to the benefits of security, decentralization and trust, blockchain, in which every transaction is recorded in a verifiable and permanent manner, has proven its ability to safeguard energy trading [92].

Contribution 6—Resource Sharing: The IoV provides the potential to create a cooperative resource-sharing network for both static and moving vehicles. Blockchain can enable a decentralized platform, allowing cars to share resources with others in order to enhance efficiency and performance [65]. Blockchain can handle resource-sharing issues, by promoting trust while also maintaining entity security and privacy. Furthermore, with the support of blockchain, non-moving vehicles may safely and effectively share their idle computing and networking resources when parked [93,94].

Contribution 7—Demand Response Management and Coordination: Since blockchain technologies have the ability to offer cost-effective smart grid solutions, they represent better alternatives for tackling challenges such as traffic congestion and road safety within the IoV. They also efficiently lower the cost of communication between multiple participants (e.g., drivers, vehicles, RSUs, etc.). It is underlined that blockchain might enhance end-consumer, EV and renewable energy engagement in IoV-assisted smart grids. As a result, these users are exposed to the true cost of energy, which leads to more efficient energy usage and makes the demand response price signals more appropriate [92]. This procedure may be achieved by utilizing various aspects of blockchain technology, such as smart contracts. The use of smart contracts in demand response might improve their efficiency and lower their operational costs. Furthermore, they can enhance the confidentiality of demand response communication [95]. Furthermore, one of the recent applications of blockchain is EV charging management and optimization, which is starting to grow quickly [96]. EV drivers may share their private chargers with others thanks to blockchain-based applications. Private owners can make their chargers available to the public while they are not in use by using P2P EV charging systems. In exchange, customers may make some profit from their idle charger by expanding its use [97].

5. Findings and Future Directions

5.1. Review Findings: Limitations of Using Blockchain in IoV-Assisted Smart Grid

As stated in the previous Sections, over the past few years, blockchain has emerged as a transformative technology in the context of the smart energy grids and IoV in particular. Blockchain technology, in combination with consensus algorithms, cryptographic techniques and smart contracts, has enabled end-users to interact without the intervention of a centralized authority or middleman. Despite the fact that no middlemen are present during runtime and operation, blockchain-based systems constantly rely on the validity of the predefined rules [70]. As a result, it is critical to ensure that they are trustworthy, secure and reliable. Moreover, blockchain technology is still in its early stages and is dealing with a variety of issues, such as reduced transaction loads [98]. Furthermore, the complexity of current protocols and solutions continues to be a challenge for academics and industry players. Despite the fact that a lot of work has been conducted, blockchain is still experiencing some limitations, as well as some potential restrictions related to its integration in the smart grid [99]. In this Section, we discuss, in detail, the research limitations of blockchain in IoV-assisted smart grids, which must be addressed before the broad adoption in large scale environments. The authors believe that the presented limitations are worthy of future study efforts towards blockchain integration in IoV-assisted smart grids. The identified limitations in the area of blockchain and IoV-assisted smart grids are depicted in Figure 12 and described below:

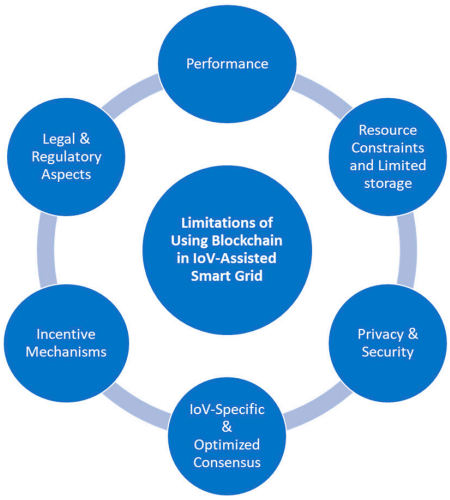

Figure 12. Limitations of using blockchain in IoV-assisted smart grids.

Limitation1—Legal and Regulatory Aspects: Significant limitations to technology adoption arise in both the regulatory and legal spheres. Consumers' active engagement in electricity markets is encouraged by regulators [21]. Furthermore, several policy-makers have developed supporting measures for local or community energy systems [100,101], with the goal of lowering consumer costs, promoting low-carbon technology and eliminating fuel poverty. Nonetheless, when it comes to alterations in the main power grid, the present grid legal system does not enable energy trading from prosumers to consumers and does not encourage the incorporation of blockchain and smart contracts into the energy grid [12]. New forms of contracts, specifically for the P2P trading system and the decentralized interactions between the IoV entities, must be established, since in the present grid system, such issues are strictly regulated. Furthermore, regulatory bodies are in charge of establishing consumer data protection standards.

The new EU regulation on consumer data (i.e., General Data Protection Regulation (GDPR)) is a recent example. Users of blockchain systems should be recognized in order to account for their responsibilities, but consumer information, such as agreed-upon pricing between an energy supplier and a consumer, should be kept private [102]. Towards this direction, further investigation is also needed regarding the legality and regulation of the smart contracts, since they should be incorporated into legal code, in order to guarantee compliance with the law and GDPR [103,104]. Therefore, even if blockchain technology has already shown its value in smart grids and IoV, adopting the technology into the main grid is extremely difficult without revised legal and regulatory mechanisms.

Limitation 2—Performance: Integrating blockchain into IoV-assisted smart grids necessitates the capacity to handle a huge volume of data and transactions in a rapidly changing environment occupied by moving cars. This is one of the current restrictions of blockchain technology in terms of immediately integrating it with IoV [59]. As a consequence of the reliance on enormous data and mobility, the performance levels of the blockchain-enabled IoV network are just as essential as its privacy and security [43,105]. Latency, throughput and scalability are examples of such performance metrics. The scalability of the current blockchain solution further restricts its adoption in large-scale IoV. The scalability of blockchain may be assessed by comparing transaction throughput per second to the number of IoV nodes and simultaneous processes, causing numerous blockchain implementations to suffer from low throughput [27]. Bitcoin, for instance, can only handle seven transactions per second. In comparison, VISA can handle approximately 2000 transactions per second, whereas PayPal can process 170 transactions per second [106,107]. Before blockchain will be widely adopted in the IoV, it must demonstrate that it can provide the needed scalability to support the critical IoV applications and ensure road safety. The blockchain technology has already passed the proof of concept stage, but it must now be scaled up.

Limitation 3—Resource Constraints and Limited storage: The majority of IoV devices have limited resources. Sensors, RSUs, EV batteries, charging points and other devices, for example, have inadequate processing capabilities, limited storage space, insufficient battery power and inadequate network connection capabilities. Yet, the consensus algorithms of blockchains sometimes necessitate a large amount of computer power and energy usage. Proof of Work, for example, was proven to consume a lot of energy [39]. As a result, consensus techniques with high energy consumption may be impractical for low-power IoV devices. On the other hand, the large amount of blockchain data makes it impossible to completely implement blockchains throughout the IoV [38]. As a result, it is difficult to keep the whole blockchain on each IoV device. Furthermore, the enormous data generated in the IoV, in near real time, complicates the issue [108]. Consequently, strategies to restrict the amount of storage resources required by the ledger are needed.

Limitation 4—Privacy and Security: Adopting blockchain in the IoV provides security and prevents data manipulations by ensuring data immutability. Nonetheless, considering that blockchain is built on different techniques, it cannot immediately ensure security and privacy [109]. A few of these techniques that can protect the security of the

information (transactions and/or records) inside the blocks, and also the privacy of the IoV users and devices, include advanced cryptographic techniques, pseudonyms and off-chain storing [65]. Transactions in BTC, for example, are conducted using IP addresses rather than participants' actual identities, thereby maintaining anonymity. Furthermore, one-time accounts in BTC are created to ensure user privacy. These safeguards, however, are not robust. User pseudonyms, on the other hand, may be cracked by recognizing and inferring the transactions connected with a single common user [76]. Furthermore, the entire storing of transaction data on the blockchain may result in possible privacy leaks [110]. In blockchain, any transaction-related information, including senders'/recipients' records and value amounts, are publicly accessible and open. As a result, even if users employ pseudonyms, this may not help them remain fully anonymous, raising security and privacy issues [111]. Moreover, IoV-participants' actions and energy profiles, such as energy consumption, production, energy use patterns, driving profiles and other records, can be monitored and leaked by analyzing the publicly available data in the blockchain. Thus, users' true identities may be disclosed [112]. Last but not least, blockchain in IoV-assisted smart grids grid has the potential to expand across an extended geographical area. In such a scenario, it is realistic to say that multiple chains and off-chains will be used. In such multi-chain environments, it is extremely difficult to ensure privacy and security [64].

Limitation 5—IoV-Specific and Optimized Consensus: As found in the analysis of the studies, several consensus algorithms have been used for the demonstration of IoV scenarios, which resulted in the following issues. Because it requires a significant amount of energy to confirm a transaction, PoW is a computationally costly consensus algorithm [113]. In addition, the PoS algorithm faces a problem with rich rules [114]. In addition, BFT-related algorithms are unsuitable for large public blockchain networks with large numbers of players [115,116]. As a result, several consensus mechanisms have been developed to address the limitations and enhance the performance of currently popular mechanisms. One drawback shared by most of the consensus algorithms is their single-purpose use, such as their use in cryptocurrencies exclusively. However, due to the distinctive nature of IoV, there are several challenges associated with implementing these algorithms in the IoV, such as block validation, security, reward schemes and energy usage. Thus, IoV-specific and optimized consensus algorithms have the potential to expand the usefulness of incorporating blockchain into IoV [59]. Even though there are some preliminary studies and implementations of IoV-specific consensus algorithms [108,117,118], they still lack reliability, since they need to be further tested and evaluated.

Limitation 6—Incentive Mechanisms: In a common public blockchain network, a miner or validator is generally rewarded for successfully generating a block. This incentive is distributed to the participants in the case of a group of miners or validators who work together. For instance, a miner who accomplishes the computationally demanding work first will be paid with a number of BTCs. Meanwhile, an Ethereum transaction will be charged a gas-fee to compensate miners for contract execution. However, the lack of smart grid-centric incentive mechanisms continues to be a challenge, since there are limited incentivization schemes available in the literature [119–121]. Providing incentives, such as bitcoin, money, carbon credits and reputation value, through the blockchain eventually helps increase the consumption of clean and renewable energy, as well as promoting participation in smart grids. As a result, one important future research direction is to create effective and beneficial incentive mechanisms with equal distribution to incentivize all stakeholders, including producers, consumers and miners/validators, to participate in the blockchain network toward clean and renewable energy consumption. Furthermore, penalty systems are required to prohibit harmful acts by any party.

5.2. Observations and Future Directions

Real-time monitoring and management are critical in the organization and management of smart energy grids. Recently, due to the fast expansion of distributed energy prosumers (e.g., EV drivers), smart grid management challenges can no longer be solved

efficiently through centralized procedures. As a result, there is a widespread recognition of the necessity for innovative decentralized designs and mechanisms. Variability in energy production, whether excess or deficit, may jeopardize energy supply security, resulting in energy overload and, eventually, power outages or service interruptions. The aforementioned concerns are also applied in the IoV scenarios, as presented in detail in the previous sections, resulting in a highly distributed and constantly changing IoV-assisted smart grid. Future research analysis of this study will emphasize the anticipated peak of energy generation and consumption in such IoV-assisted smart grids. A potential solution to these previously described issues is efficient demand response (DR) management, which aims to balance energy demand with production by incentivizing the smart grid participants to reduce or move their energy use to deal with peak load hours and/or peak load geographical areas [122]. Any forthcoming approach should balance requirements, distribute costs and revenues fairly and transparently among all participants in the IoV value chain, and be assisted by proactive initiatives. In order for the IoV-assisted smart grid to function properly, EV energy trading and charging procedures must effectively represent demand–supply balance and potential shortages. In this sense, blockchain seems to have the potential to be an innovative paradigm to DR programs, laying the groundwork for a decentralized, transparent and privacy-preserving charging coordination mechanism and optimal demand response management to address the aforementioned limitations in IoV-assisted smart grids. The described future directions are based on the review findings discussed in Section 5.1 and on the observations presented in Section 5.2, as shown in Table 5.

Table 5. Observations derived from the systematic literature review findings.

Observation	Description
OB.1	IoV needs decentralization in terms of energy management
OB.2	Real-time monitoring of the connected objects in the IoV is critical
OB.3	Energy generation and consumption in the IoV may affect the demand and response in smart grids
OB.4	EV energy trading and charging procedures must effectively represent demand–supply balance
OB.5	Private information of the EVs are exposed resulting in privacy and security issues
OB.6	EVs with surplus energy are not motivated to participate as energy sellers due to the lack of incentive mechanisms
OB.7	Blockchain can be used for fair payments during energy trading without relying in untrustied third-parties
OB.8	Blockchain can provide security and privacy through EV identity management and data encryption

6. Conclusions

This article explored challenges and opportunities in the blockchain-enabled IoV domain, extracted from papers between 2017 and 2021. The authors acquired a number of articles by utilizing a rigorous search filtration method; however, some were deemed to be irrelevant. Initially, the authors investigated the current challenges in the area of IoV-assisted smart grids, concluding that the major concerns are related to high mobility, the complexity of the interconnected EVs and other IoV objects (e.g., RSUs), and demand response. Then, the authors explored the blockchain applications in IoV-assisted smart grids in various fields including, among others, P2P energy trading among EVs, IoV management, data protection and blockchain performance. In addition to reviewing diverse blockchain contributions in the IoV, the authors suggested several potential avenues for beginner researchers to pursue. Those directions mainly include blockchain performance and scalability, resource constraints, privacy and security issues, IoV-specific consensus algorithms, incentive mechanisms, legal and regulatory aspects, as well as efficient demand response management. The current review revealed that blockchain provides disinterme-

diation, confidentiality and tamper-proof transfers, and it also provides innovative ways for EV drivers to participate more actively in the IoV concept and to benefit from their properties.

Based on the findings of the conducted systematic literature review, the authors highlighted a set of observations as the basis for further research. Based on the authors' observations, the main limitation that needs to be addressed is the centralized management of the IoV, and the need for real-time monitoring of all the connected objects (i.e., vehicles, charging stations, road-side units, parking lots, etc.) in the network. Moreover, it was observed that energy generation and consumption in the IoV may affect the demand and response in smart grids. Therefore, EVs' energy trading and charging procedures should effectively represent demand–supply balance in the grid, and consequently in all parts of a smart city. As derived from the current review, there are several research studies that provide solutions to manage demand by trading energy in a V2V and/or V2G manner. However, it was noticed that objects in the IoV (i.e., especially EV and charging stations) face various limitations, such as security and privacy issues and a lack of incentives. Finally, it was confirmed by all the studies included in this review that blockchain technology has a great potential in the area of IoV. Specifically, the findings of the current review stated that blockchain can be used, among other applications, for fair payments during energy trading without relying on untrusted third-parties, as well as to provide security and privacy through EV identity management and data encryption.

According to the current review of the existing literature, the majority of countries in the IoV industry use a centralized system, which is frequently controlled by the country's laws and regulations. As a result, future studies should consider the potential applicability of blockchain in this domain, as well as the obstacles associated with its adoption, from a national or regional perspective. Moreover, blockchain should be studied in the context of the country or region in question, as well as its present issues.

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

Funding: This work was supported by PARITY project funded by the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement No. 864319.

Data Availability Statement: Not Applicable, the study does not report any data.

Acknowledgments: This work was also supported by the Institute for the Future, University of Nicosia, as part of the corresponding author's Ph.D. Studies.

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

Appendix A. Search Queries Submitted in Different Databases

The authors were unable to apply the same set of search queries to each database due to the various database models. To extract relevant information from the research databases, the authors created various queries based on the goal of the study. The tables below present the submitted queries for the different selected databases.

IEEEXplore Database Queries		
Query 1	("All Metadata":blockchain) AND ("All Metadata":energy)	686 results
Query 2	("All Metadata":blockchain) AND ("All Metadata":renewable energy)	132 results
Query 3	("All Metadata":blockchain) AND ("All Metadata":microgrid)	123 results
Query 4	("All Metadata":blockchain) AND ("All Metadata":energy trading)	132 results
Query 5	("All Metadata":blockchain AND ("All Metadata":"vehicle to grid" OR "vehicle-to-grid" OR "Vehicle-to-Grid" OR V2G))	71 results
Query 6	("All Metadata":blockchain AND ("All Metadata":"vehicle to vehicle" OR "vehicle-to-vehicle" OR "Vehicle-to-Vehicle" OR V2V OR * vehicle OR IoV))	64 results

ScienceDirect Database Queries		
Query 1	blockchain AND energy—in all parts of the document excluding references	1763 results
Query 2	blockchain AND "renewable energy"—in all parts of the document excluding references	445 results
Query 3	blockchain AND microgrid—in all parts of the document excluding references	230 results
Query 4	blockchain AND "energy trading"—in all parts of the document excluding references	223 results
Query 5	blockchain AND ("vehicle to grid" OR "vehicle-to-grid" OR "Vehicle-to-Grid" OR V2G)—in all parts of the document excluding references	172 results
Query 6	blockchain AND ("vehicle to vehicle" OR "vehicle-to-vehicle" OR "Vehicle-to-Vehicle" OR V2V OR * vehicle OR IoV)—in all parts of the document excluding references	170 results
SpringerLink Database Queries		
Query 1	with all of the words: blockchain AND energy	2464 results
Query 2	with all of the words: blockchain AND "renewable energy"	386 results
Query 3	with all of the words: blockchain AND microgrid	102 results
Query 4	with all of the words: blockchain AND "energy trading"	186 results
Query 5	with the exact phrase: blockchain AND ("vehicle to vehicle" OR "vehicle-to-vehicle" OR "Vehicle-to-Vehicle" OR V2V)	37 results
Query 6	with the exact phrase: blockchain AND ("vehicle to vehicle" OR "vehicle-to-vehicle" OR "Vehicle-to-Vehicle" OR V2V OR * vehicle OR IoV)	84 results
ACM Database Queries		
Query 1	[All: blockchain] AND [All: energy]	473 results
Query 2	[All: blockchain] AND [All: "renewable energy"]	34 results
Query 3	[All: blockchain] AND [All: microgrid]	24 results
Query 4	[All: blockchain] AND [All: "energy trading"]	30 results
Query 5	[All: blockchain] AND [[All: "vehicle to grid"] OR [All: "vehicle-to-grid"] OR [All: "vehicle-to-grid"] OR [All: V2G]]	8 results
Query 6	[All: blockchain] AND [[All: "vehicle to vehicle"] OR [All: "vehicle-to- vehicle"] OR [All: "vehicle-to- vehicle"] OR [All: V2V] OR [All: * vehicle] OR [All: IoV]]	22 results
Google Scholar Database Query		
Query	blockchain AND ("* vehicle" OR V2V OR V2G OR IoV OR microgrid)—anywhere in the searched documents	503 results

Appendix B. Primary Studies

The following tables show the analysis of the primary studies, grouped by application area. The following features are highlighted: (a) authors and publication year, (b) title, (c) identified problems, (d) study outcomes and (e) study limitations and/or research directions.

IoV Management				
(a) Author	**(b) Title**	**(c) Identified Problems**	**(d) Study Outcomes**	**(e) Limitations**
[123]	A review of strategic charging–discharging control of grid-connected electric vehicles	System performance (e.g., overloading, deteriorating power quality, power loss)	A review on key challenges for the V2G charging-discharging	Lack of simulation models, security, EV aggregation methods, regulation, communication protocols and standards, charging profiles
[124]	Integrating IoT and blockchain for ensuring road safety: an unconventional approach	Road accidents caused by parameters such as speed, security, stability and fairness.	Integration of IoT with DLTs through Hashgraph to create a communication network between the different vehicles and other relevant parameters. Scheduling the requests according to the priorities for ensuring better QoS	Large amounts of time and resources for validation, limited storage, authentication and user revocation

IoV Management				
(a) Author	**(b) Title**	**(c) Identified Problems**	**(d) Study Outcomes**	**(e) Limitations**
[15]	Blockchain based trading platform for electric vehicle charging in smart cities	High storage footprint, computation and communication overhead	A smart-contract-based trading platform that runs on top of Ethereum	Limited computational power, network throughput and latency
[125]	BlockEV: Efficient and Secure Charging Station Selection for Electric Vehicles	Untrusted EV charging infrastructures result in privacy and security threats to EV user's private information	A blockchain-based efficient CSs selection protocol for EVs to ensure security and privacy, availability of the reserved time slots, high QoS and enhanced EV user comfort	Dynamic pricing, integration of EVs and renewable energy in smart grid
Smart Grid Management				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[126]	A Secured and Trusted Demand Response system based on Blockchain technologies	Interoperability issues, security and privacy issues in aggregator-prosumer transactions	A multi-agent decision making system and self-learning algorithms to enable aggregation, segmentation and coordination of several diverse clusters. In addition, a blockchain-based smart contract for securing the aggregator–prosumer transactions.	Optimizing the security-efficiency trade-offs
[127]	Blockchain and smart metering towards sustainable prosumers	Imbalances in the energy network due to the arrival of prosumers, security concerns related to the communication between prosumers	A load-balancing network incorporating smart meters, and adopting blockchain for securing the communication between prosumers	Optimal control of energy flows, optimal scheduling in non-standard prosumers, incentive mechanism
[128]	Research on the Blockchain-based Integrated Demand Response Resources Transaction Scheme	Centralized trading of electricity market model is unable to meet the trading needs of distributed resources, difficulties in real-time scheduling of demand response	The blockchain-based demand response transaction platform which supports the credible transaction and settlement between the distributed resources and promote the development of DERs.	Smart contracts execution fees, Real-time scheduling
[129]	Enabling New Technologies for Demand Response Decentralized Validation Using Blockchain	Improper management of the energy supply and demand can threaten the stability of the grid, Variations of the energy production and consumption can lead to overloading the network, Technological scalability problems it may also generate higher fees in energy prices	A demand response framework for near-real time autonomous demand response management combined with a democratic market driven pricing scheme.	Technological scalability problems, higher fees, higher energy prices

Smart Grid Management				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[92]	Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles	Lack of incentive mechanism, privacy leakage and security threats	A distributed, privacy-preserved, and incentive-compatible demand response mechanism for secure energy trading between EVs, with moderate cost	Tremendous costs for decrypting the encrypted data, increased computation resources
[95]	An Introduction to Blockchain-based Concepts for Demand Response Considering of Electric Vehicles and Renewable Energies	Weak data security and privacy, low speed of financial transactions	Proposition of a blockchain-based concept for demand response programs by efficient use of electric vehicles and renewable energies in the electricity markets	Lack of participation of end-consumer, EVs and DERs in local electricity markets, lack of incentive mechanisms
[130]	Sustainable microgrid design considering blockchain technology for real-time price-based demand response programs	Unsustainable microgrid design, energy demand uncertainty	A fuzzy multi-objective optimization approach to determine the optimal number, location, and capacity of renewable distributed generation units as well as the equilibrium supply and dynamic pricing decisions under uncertain demand, capacity, and economic, environmental, and social parameters.	Increased computational time, requirement for historical data to analyse the probability distributions of the uncertainty parameters
P2P Energy Trading				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[131]	Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains	Transactions security and privacy protection issues	A localized P2P electricity trading model for locally buying and selling electricity among PHEVs in smart grids.	Lack of large-scale evaluation
[66]	Blockchain based Data and Energy Trading in Internet of Electric Vehicles	Trust-less IoV environment, trading disputes and conflicting interests among trading parties, lack of privacy while ensuring EVs' anonymity.	A consortium blockchain to maintain transparency and trust in trading activities within the IoV	Limited storage capacity
[132]	Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing	Power fluctuation, lack of a distributed security mechanism for V2G energy trading, single point of failure, denial of service attacks, privacy leakage, lack of an efficient incentive mechanism for V2G energy trading.	A secure and efficient V2G energy trading framework by exploring blockchain, contract theory, and edge computing.	Selection of the initial point to increase the convergence speed

AI/ML in IoV				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[51]	Deep reinforcement learning based performance optimization in blockchain-enabled Internet of vehicle	Scalability and performance issues to handle huge amounts of data coming from the IoV, low data security and privacy, poor interoperability and compatibility among different nodes, high storage and transaction costs	A novel deep reinforcement learning based performance optimization framework for blockchain-enabled IoV	Computation power
[57]	AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions	Lack of recourses in the IoV stress the infrastructure	An overview that discusses the AI and blockchain approaches and models for IoV and proposes a new Vehicular Edge Computing-based architecture embedding both technologies	Collecting IoV data might be costly, Cost optimization in terms of network, storage and computation recoursesData are generated on the user level, and are forwarded to the Cloud/Fog for analysis. Edge resembles the man-in-the-middle for such a process to help the Cloud/Fog pre-processing the data according to the vehicle profile
[133]	Deep Reinforcement Learning for Optimal Resource Allocation in Blockchain-based IoV Secure Systems	Privacy and security of vehicular data, poor interoperability, compatibility among different nodes, high storage and transaction costs	A framework that combines DRL and blockchain to address the high cost and security problems. The proposed learning-based algorithm smartly learns to allocate the computing resource to each miner of the blockchain, in which the data are securely shared and stored for the IoV network.	Privacy-preserving concerns, Lack of large-scale evaluation
Privacy & Security				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[134]	Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities	Single point failure, data immutability	A framework for the VANET system with blockchain technology that provides the reliability of the critical messages	Block verification time, scalability of blockchain network
[16]	A Lightweight Blockchain-Based Trust Model for Smart Vehicles in VANETs	Untrusted messages, compromised RSU, untrusted Vehicles	Lightweight blockchain-based decentralized trust model for preserving the privacy in VANET	Lack of large-scale evaluation

Privacy & Security				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[73]	Blockchain-based Trust Management for Internet of Vehicles	Complex network structure and high mobility, unreliable messages exchange, malicious vehicles	A trust management system of IoV based on blockchain, which formalizes a complete vehicle reputation value calculation scheme to deal with the problem of calculating the credibility of messages	An IoV-compatible consensus algorithm is necessary to make mining times shorter and reduce the delay of trust management systems
[135]	Secure V2X Environment using Blockchain Technology	Unsecure V2X environment	A hypothetical framework that renders the impact of challenging factors on the implementation of blockchain in V2X paradigm	Scalability issues, processing power and time, data protection, interoperability, limited storage, inappropriate consensus algorithm, legal concerns, anonymity
Data Protection & Management				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[64]	Blockchain for The Internet of Vehicles: How to use Blockchain to secure Vehicle-to-Everything (V2X) Communication and Payment?	V2X infrastructure issues, concern about establishing secure and instant payments and communications within the IoV	A blockchain-based solution for establishing secure payment and communication (PSEV) in order to study the use of blockchain as middle-ware between different participants of intelligent transportation systems	Memory and power consumption
[61]	AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology	Erroneous traffic-related messages, malfunctioning IoT devices, malicious vehicles, sharing of fake traffic alerts	A trust management system that is based on deep learning to evaluate the trust of nodes and data. Blockchain is incorporated to the system so that both the identity of vehicles and RSUs and the authenticity of messages sent in the vehicular networks could be validated	Effective evaluation of trust in vehicular networks while maintaining the privacy of vehicles
Blockchain Performance in IoV				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[43]	Impacts of Mobility on Performance of Blockchain in VANET	Grid imbalances due to EV mobility and dynamicity in the connectivity of the nodes	A comprehensive analysis framework that encompasses from modelling of nodes' mobility to analysis of the impacts of mobility on a blockchain system's performance	The grid stability is determined by the nodes' velocities, the number of full nodes, and the radius of the full nodes' communication range. The number of blocks that can be exchanged during a rendezvous can be inferred from the stability

Blockchain Performance in IoV				
Author	**Title**	**Identified Problems**	**Study Outcomes**	**Limitations**
[105]	Performance Analysis of Blockchain-Based Internet of Vehicles Under the DSRC Architecture	Lack of suitable consensus algorithm for IoV applications, mobility of the IoV nodes bring fluctuations and reliability problems to the consensus of the blockchain network	A two-layer wireless architecture to avoid the impact of mobility on the blockchain network, and analyses the blockchain transaction delivery model based on the Carrier Sense Multiple Access (CSMA/CA) mechanism.	Increased confirmation delay

References

1. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 731–736. [CrossRef]
2. Xiong, G.; Zhu, F.; Liu, X.; Dong, X.; Huang, W.; Chen, S.; Zhao, K. Cyber-physical-social system in intelligent transportation. *IEEE/CAA J. Autom. Sin.* **2015**, *2*, 320–333. [CrossRef]
3. Lone, F.R.; Verma, H.K.; Sharma, K.P. Evolution of VANETS to IoV. *Teh. Glas.* **2021**, *15*, 143–149. [CrossRef]
4. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in internet of vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]
5. Hatim, S.M.; Elias, S.J.; Ali, R.M.; Jasmis, J.; Aziz, A.A.; Mansor, S. Blockchain-based Internet of Vehicles (BIoV): An Approach towards Smart Cities Development. In Proceedings of the 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE 2020), Jaipur, India, 1–3 December 2020. [CrossRef]
6. Sadique, K.M.; Rahmani, R.; Johannesson, P. Towards Security on Internet of Things: Applications and Challenges in Technology. *Procedia Comput. Sci.* **2018**, *141*, 199–206. [CrossRef]
7. Samuel, O.; Javaid, N.; Shehzad, F.; Iftikhar, M.S.; Iftikhar, M.Z.; Farooq, H.; Ramzan, M. Electric Vehicles Privacy Preserving Using Blockchain in Smart Community. In *Lecture Notes in Networks and Systems*; Barolli, L., Hellinckx, P., Enokido, T., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 97, pp. 67–80.
8. Zabaleta, K.; Casado-Mansilla, D.; Kapassa, E.; Borges, C.E.; Presmair, G.; Themistocleous, M.; Lopez-De-Ipina, D. Barriers to Widespread the Adoption of Electric Flexibility Markets: A Triangulation Approach. In Proceedings of the 2020 5th International Conference on Smart and Sustainable Technologies (SpliTech), Split, Croatia, 1–4 July 2020. [CrossRef]
9. Corti, F.; Reatti, A.; Piccirilli, M.C.; Grasso, F.; Paolucci, L.; Kazimierczuk, M.K. Simultaneous wireless power and data transfer: Overview and application to electric vehicles. In Proceedings of the IEEE International Symposium on Circuits and Systems, Sevilla, Spain, 10–21 October 2020. [CrossRef]
10. ElGhanam, E.; Ahmed, I.; Hassan, M.; Osman, A. Authentication and billing for dynamic wireless EV charging in an internet of electric vehicles. *Futur. Internet* **2021**, *13*, 257. [CrossRef]
11. Dong, C.; Akram, A.; Andersson, D.; Arnäs, P.O.; Stefansson, G. The impact of emerging and disruptive technologies on freight transportation in the digital era: Current state and future trends. *Int. J. Logist. Manag.* **2021**, *32*, 386–412. [CrossRef]
12. Themistocleous, M.; Stefanou, K.; Megapanos, C.; Iosif, E. To chain or not to chain? A case from energy sector. In *Lecture Notes in Business Information Processing*; Themistocleous, M., da Cunha, P., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 341, pp. 31–37.
13. Kapassa, E.; Themistocleous, M.; Quintanilla, J.R.; Touloupos, M.; Papadaki, M. Blockchain in Smart Energy Grids: A Market Analysis. In *Lecture Notes in Business Information Processing*; Springer: Cham, Switzerland, 2020; Volume 402, pp. 113–124. Available online: https://link.springer.com/chapter/10.1007/978-3-030-63396-7_8 (accessed on 7 December 2021).
14. Alladi, T.; Chamola, V.; Rodrigues, J.J.P.C.; Kozlov, S.A. Blockchain in smart grids: A review on different use cases. *Sensors* **2019**, *19*, 4862. [CrossRef]
15. Lasla, N.; Al-Ammari, M.; Abdallah, M.; Younis, M. Blockchain Based Trading Platform for Electric Vehicle Charging in Smart Cities. *IEEE Open J. Intell. Transp. Syst.* **2020**, *1*, 80–92. [CrossRef]
16. Ayobi, S.; Wang, Y.; Rabbani, M.; Dorri, A.; Jelodar, H.; Huang, H.; Yarmohammadi, S. A Lightweight Blockchain-Based Trust Model for Smart Vehicles in VANETs. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Wang, G., Chen, B., Li, W., di Pietro, R., Yan, X., Han, H., Eds.; Springer International Publishing: Cham, Switzerland, 2021; Volume 12382, pp. 276–289.
17. Tripathi, G.; Ahad, M.A.; Sathiyanarayanan, M. The Role of Blockchain in Internet of Vehicles (IoV): Issues, Challenges and Opportunities. In Proceedings of the 4th International Conference on Contemporary Computing and Informatics (IC3I 2019), Bengaluru, India, 20–21 December 2019; pp. 26–31. [CrossRef]
18. Musleh, A.S.; Yao, G.; Muyeen, S.M. Blockchain Applications in Smart Grid-Review and Frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]

19. Tseng, L.; Yao, X.; Otoum, S.; Aloqaily, M.; Jararweh, Y. Blockchain-based database in an IoT environment: Challenges, opportunities, and analysis. *Clust. Comput.* **2020**, *23*, 2151–2165. [CrossRef]
20. Thakore, R.; Vaghashiya, R.; Patel, C.; Doshi, N. Blockchain-based IoT: A Survey. *Procedia Comput. Sci.* **2019**, *155*, 704–709. [CrossRef]
21. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
22. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy management: Review, solutions, and challenges. *Comput. Commun.* **2020**, *151*, 395–418. [CrossRef]
23. Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C. Digitalization and decentralization driving transactive energy Internet: Key technologies and infrastructures. *Int. J. Electr. Power Energy Syst.* **2021**, *126*, 106593. [CrossRef]
24. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibanez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2018**, *5*, 3701–3709. [CrossRef]
25. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. *Veh. Commun.* **2019**, *20*, 100182. [CrossRef]
26. Golestan, K.; Soua, R.; Karray, F.; Kamel, M.S. Situation awareness within the context of connected cars: A comprehensive review and recent trends. *Inf. Fusion* **2016**, *29*, 68–83. [CrossRef]
27. Huang, P.; Huang, B.; Zhao, Y.; Qiang, Z.; Qing, M. BCoV: A covergence of blockchain and IoV. In Proceedings of the Companion of the 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security (QRS-C 2020), Macau, China, 11–14 December 2020; pp. 636–643. [CrossRef]
28. Jabbar, R.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, A.K. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using Ethereum. *Sensors* **2020**, *20*, 3928. [CrossRef] [PubMed]
29. Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. A survey of trust management in the internet of vehicles. *Electronics* **2021**, *10*, 2223. [CrossRef]
30. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [CrossRef]
31. da Silva, F.Q.B.; Santos, A.L.M.; Soares, S.; Frana, A.C.C.; Monteiro, C.V.F.; MacIel, F.F. Six years of systematic literature reviews in software engineering: An updated tertiary study. *Inf. Softw. Technol.* **2011**, *53*, 899–913. [CrossRef]
32. Kitchenham, B.A.; Brereton, P.; Turner, M.; Niazi, M.K.; Linkman, S.; Pretorius, R.; Budgen, D. Refining the systematic literature review process-two participant-observer case studies. *Empir. Softw. Eng.* **2010**, *15*, 618–653. [CrossRef]
33. Cooper, H.M. Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowl. Soc.* **1988**, *1*, 104–126. Available online: https://link.springer.com/article/10.1007%252FBF03177550 (accessed on 7 December 2021). [CrossRef]
34. Briner, R.B.; Denyer, D. Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool. In *The Oxford Handbook of Evidence-Based Management*; Oxford University Press: Oxford, UK, 2012.
35. Iosif, E.; Christodoulou, K.; Vlachos, A. Web Mining for Estimating Regulatory Blockchain Readiness. *arXiv* **2021**, arXiv:2103.13235.
36. Church, K.W.; Hanks, P. Word association norms, mutual information, and lexicography. *Comput. Linguist.* **1989**, *16*, 76–83. [CrossRef]
37. Iosif, E.; Potamianos, A. Similarity computation using semantic networks created from web-harvested data. *Nat. Lang. Eng.* **2015**, *21*, 49–79. [CrossRef]
38. Viriyasitavat, W.; Anuphaptrirong, T.; Hoonsopon, D. When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *J. Ind. Inf. Integr.* **2019**, *15*, 21–28. [CrossRef]
39. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. *Challenges and opportunities Futur. Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
40. Rakovic, V.; Karamachoski, J.; Atanasovski, V.; Gavrilovska, L. Blockchain Paradigm and Internet of Things. *Wirel. Pers. Commun.* **2019**, *106*, 219–235. [CrossRef]
41. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
42. Kobashi, T.; Jittrapirom, P.; Yoshida, T.; Hirano, Y.; Yamagata, Y. SolarEV City concept: Building the next urban power and mobility systems. *Environ. Res. Lett.* **2021**, *16*, 024042. [CrossRef]
43. Kim, S. Impacts of Mobility on Performance of Blockchain in VANET. *IEEE Access* **2019**, *7*, 68646–68655. [CrossRef]
44. Qian, Y.; Jiang, Y.; Hu, L.; Hossain, M.S.; Alrashoud, M.; Al-Hammadi, M. Blockchain-based privacy-aware content caching in cognitive internet of vehicles. *IEEE Netw.* **2020**, *34*, 46–51. [CrossRef]
45. Mahmood, Z. Connected vehicles in the IoV: Concepts, technologies and architectures. In *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*; Mahmood, Z., Ed.; Springer International Publishing: Cham, Switzerland, 2020; pp. 3–18.
46. Ang, L.M.; Seng, K.P.; Ijemaru, G.K.; Zungeru, A.M. Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges. *IEEE Access* **2019**, *7*, 6473–6492. [CrossRef]
47. Zadobrischi, E.; Dimian, M. Vehicular Communications Utility in Road Safety Applications: A Step toward Self-Aware Intelligent Traffic Systems. *Symmetry* **2021**, *13*, 438. [CrossRef]

48. Sung, H.; Min, J.; Ha, S.; Eom, H. OMBM: Optimized memory bandwidth management for ensuring QoS and high server utilization. *Clust. Comput.* **2019**, *22*, 161–174. [CrossRef]
49. Liu, L.; Chen, C.; Pei, Q.; Maharjan, S.; Zhang, Y. Vehicular Edge Computing and Networking: A Survey. *Mob. Netw. Appl.* **2021**, *26*, 1145–1168. [CrossRef]
50. Liu, C.; Liu, K.; Ren, H.; Zhou, Y.; Feng, L.; Guo, S.; Lee, V. Enabling safety-critical and computation-intensive IoV applications via vehicular fog computing. In Proceedings of the 2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN 2019), Shenzhen, China, 11–13 December 2019; pp. 378–383. [CrossRef]
51. Liu, M.; Teng, Y.; Yu, F.R.; Leung, V.C.M.; Song, M. Deep Reinforcement Learning Based Performance Optimization in Blockchain-Enabled Internet of Vehicle. In Proceedings of the IEEE International Conference on Communications, Shanghai, China, 20–24 May 2019; Volume 2019, pp. 1–6. [CrossRef]
52. Sherazi, H.H.R.; Khan, Z.A.; Iqbal, R.; Rizwan, S.; Imran, M.A.; Awan, K. A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication. *Mob. Inf. Syst.* **2019**, *2019*, 3101276. [CrossRef]
53. Kirsi, K.; Makinen, S.J.; Pertti, J.; Antti, R.; Joni, M. The role of residential prosumers initiating the energy innovation ecosystem to future flexible energy system. In Proceedings of the 2016 13th International Conference on the European Energy Market (EEM), Porto, Portugal, 6–9 June 2016; pp. 1–5. [CrossRef]
54. Hubert, T.; Grijalva, S. Modeling for residential electricity optimization in dynamic pricing environments. *IEEE Trans. Smart Grid* **2012**, *3*, 2224–2231. [CrossRef]
55. Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When Blockchain Meets Smart Grid: Secure Energy Trading in Demand Response Management. *IEEE Netw.* **2020**, *34*, 299–305. [CrossRef]
56. Lazaroiu, C.; Roscia, M. RESCoin to improve Prosumer Side Management into Smart City. In Proceedings of the 7th International IEEE Conference on Renewable Energy Research and Applications (ICRERA 2018), Paris, France, 14–17 October 2018; pp. 1196–1201.
57. Hammoud, A.; Sami, H.; Mourad, A.; Otrok, H.; Mizouni, R.; Bentahar, J. AI, Blockchain, and Vehicular Edge Computing for Smart and Secure IoV: Challenges and Directions. *IEEE Internet Things Mag.* **2020**, *3*, 68–73. [CrossRef]
58. Ning, Z.; Dong, P.; Wang, X.; Rodrigues, J.J.P.C.; Xia, F. Deep reinforcement learning for vehicular edge computing: An intelligent offloading system. *ACM Trans. Intell. Syst. Technol.* **2019**, *10*, 1–24. [CrossRef]
59. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.-Y.; Koh, L.H. Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey. *IEEE Internet Things J.* **2021**, *8*, 4157–4185. [CrossRef]
60. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5. [CrossRef]
61. Zhang, C.; Li, W.; Luo, Y.; Hu, Y. AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology. *IEEE Internet Things J.* **2021**, *8*, 3157–3169. [CrossRef]
62. Sakiz, F.; Sen, S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad. Hoc. Netw.* **2017**, *61*, 33–50. [CrossRef]
63. Baza, M.; Amer, R.; Rasheed, A.; Srivastava, G.; Mahmoud, M.; Alasmary, W. A blockchain-based energy trading scheme for electric vehicles. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications and Networking Conference (CCNC 2021), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–7. [CrossRef]
64. 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]
65. Chai, H.; Leng, S.; Zhang, K.; Mao, S. Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles. *IEEE Access* **2019**, *7*, 175744–175757. [CrossRef]
66. Sadiq, A.; Javed, M.U.; Khalid, R.; Almogren, A.; Shafiq, M.; Javaid, N. Blockchain Based Data and Energy Trading in Internet of Electric Vehicles. *IEEE Access* **2021**, *9*, 7000–7020. [CrossRef]
67. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W.C. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access* **2020**, *8*, 54371–54401. [CrossRef]
68. Asfia, U.; Kamuni, V.; Sheikh, A.; Wagh, S.; Patel, D. Energy trading of electric vehicles using blockchain and smart contracts, In Proceedings of the 2019 18th European Control. Conference (ECC 2019), Naples, Italy, 25–28 June 2019; pp. 3958–3963. [CrossRef]
69. Liu, C.; Chai, K.K.; Zhang, X.; Chen, Y. Peer-to-peer electricity trading system: Smart contracts based proof-of-benefit consensus protocol. *Wirel. Netw.* **2019**, *27*, 1–12. [CrossRef]
70. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
71. Wang, C.; Cheng, X.; Li, J.; He, Y.; Xiao, K. A survey: Applications of blockchain in the Internet of Vehicles. *EURASIP J. Wirel.* **2021**, *2021*, 1–16. Available online: https:https://link.springer.com/article/10.1186/s13638-021-01958-8 (accessed on 7 December 2021). [CrossRef]
72. Pirker, D.; Fischer, T.; Witschnig, H.; Steger, C. Velink-A Blockchain-based Shared Mobility Platform for Private and Commercial Vehicles utilizing ERC-721 Tokens. In Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP 2021), Zhuhai, China, 8–10 January 2021; pp. 62–67. [CrossRef]

73. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N. Blockchain-based Trust Management for Internet of Vehicles. *IEEE Trans. Emerg. Top. Comput.* **2020**, *1*, 1397–1409. [CrossRef]
74. Malina, L.; Srivastava, G.; Dzurenda, P.; Hajny, J.; Ricci, S. A Privacy-Enhancing Framework for Internet of Things Services. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Liu, J.K., Huang, X., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 11928, pp. 77–97.
75. Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Anwar, A.; Kayes, A.S.M.; Zengin, A. A blockchain-based authentication protocol for cooperative vehicular ad hoc network. *Sensors* **2021**, *21*, 1273. [CrossRef]
76. Zhaofeng, M.; Lingyun, W.; Weizhe, Z. Blockchain-Driven Trusted Data Sharing with Privacy-Protection in IoT Sensor Network. *IEEE Sens. J.* **2020**, *21*, 1273. [CrossRef]
77. Khorasany, M.; Dorri, A.; Razzaghi, R.; Jurdak, R. Lightweight blockchain framework for location-aware peer-to-peer energy trading. *Int. J. Electr. Power Energy Syst.* **2021**, *127*, 106610. [CrossRef]
78. Mihaylov, M.; Razo-Zapata, I.; Nowé, A. NRGcoin-A Blockchain-based Reward Mechanism for Both Production and Consumption of Renewable Energy. In *Transforming Climate Finance and Green Investment with Blockchains*; Marke, A., Ed.; Academic Press: Cambridge, MA, USA, 2018; pp. 111–131.
79. Unterweger, A.; Knirsch, F.; Brunner, C.; Engel, D. Low-risk Privavy-Preserving Electric Vehicle Charging with Payments. *Work. Automot. Auton. Veh. Secur.* **2021**, *2021*, 1–6. Available online: https://www.ndss-symposium.org/wp-content/uploads/autosec2021_23001_paper.pdf (accessed on 7 December 2021).
80. Gawas, M.; Patil, H.; Govekar, S.S. An integrative approach for secure data sharing in vehicular edge computing using Blockchain. *Peer-to-Peer Netw. Appl.* **2019**, 1–19. Available online: https://link.springer.com/article/10.1007/s12083-021-01107-4 (accessed on 9 December 2021). [CrossRef]
81. Ramaguru, R.; Sindhu, M.; Sethumadhavan, M. Blockchain for the internet of vehicles. In *Communications in Computer and Information Science*; Singh, M., Gupta, P.K., Tyagi, V., Flusser, J., Ören, T., Kashyap, R., Eds.; Springer: Singapore, 2019; Volume 1045, pp. 412–423.
82. Tan, H.; Chung, I. Rsu-aided remote v2v message dissemination employing secure group association for uav-assisted vanets. *Electronics* **2021**, *10*, 548. [CrossRef]
83. Sankar, P.P.; Kumar, P.A.; Bharathi, B. Blockchain-Based Incentive Announcement in Vanet Using CreditCoin. *Lect. Notes Electr. Eng.* **2021**, *709*, 567–574. [CrossRef]
84. Liu, J.; Zhang, X.; Li, Y.; Cui, Q.; Tao, X. Blockchain-Empowered Content Cache System for Vehicle Edge Computing Networks. In *Communications in Computer and Information Science*; Zheng, Z., Dai, H.-N., Tang, M., Chen, X., Eds.; Springer: Singapore, 2020; Volume 1156, pp. 410–421.
85. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2020**. Available online: https://www.sciencedirect.com/science/article/pii/S2352864819303827 (accessed on 7 December 2021). [CrossRef]
86. Munsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In Proceedings of the 2017 IEEE Conference on Control Technology and Applications (CCTA), Maui, HI, USA, 27–30 August 2017; pp. 2164–2171. [CrossRef]
87. Hampel, C. BMW Uses Blockchain to Increase Resource Transparency. 2020. Available online: https://www.electrive.com/2020/03/31/bmw-uses-blockchain-for-purchase-transparency/ (accessed on 7 December 2021).
88. Hampel, C. Volvo Sets up Blockchain for Tracing Cobalt Sources. Available online: https://www.electrive.com/2019/11/06/volvo-sets-up-blockchain-system-for-tracing-cobalt-sources/ (accessed on 7 December 2021).
89. Hampel, C. Volkswagen Joins Blockchain for Cobalt Supply. 2019. Available online: https://www.electrive.com/2019/04/23/volkswagen-joins-blockchain-initiative-for-purchasing-cobalt/ (accessed on 7 December 2021).
90. Kadhim, A.J.; Naser, J.I. Toward Electrical Vehicular Ad Hoc Networks: E-VANET. *J. Electr. Eng. Technol.* **2021**, *16*, 1667–1683. [CrossRef]
91. Moeini, A.; Dabbaghjamanesh, M.; Dragičević, T.; Kimball, J.W.; Zhang, J. Machine learning technique for low-frequency modulation techniques in power converters. In *Control of Power Electronic Converters and Systems*; Academic Press: Cambridge, MA, USA, 2021; pp. 149–167.
92. Zhou, Z.; Wang, B.; Guo, Y.; Zhang, Y. Blockchain and Computational Intelligence Inspired Incentive-Compatible Demand Response in Internet of Electric Vehicles. *IEEE Trans. Emerg. Top. Comput. Intell.* **2019**, *3*, 205–216. [CrossRef]
93. Wang, L.; Jiao, S.; Xie, Y.; Mubaarak, S.; Zhang, D.; Liu, J.; Jiang, S.; Zhang, Y.; Li, M. A permissioned blockchain-based energy management system for renewable energy microgrids. *Sustainability* **2021**, *13*, 1317. [CrossRef]
94. Simon, P.; Hola, M. Parameters for modelling of increase EV numbers use. In Proceedings of the 2019 20th International Scientific Conference on Electric Power Engineering (EPE 2019), Kouty nad Desnou, Czech Republic, 15–17 May 2019. [CrossRef]
95. Shekari, M.; Moghaddam, M.P. An introduction to blockchain-based concepts for demand response considering of electric vehicles and renewable energies. In Proceedings of the 2020 28th Iranian Conference on Electrical Engineering (ICEE 2020), Tabriz, Iran, 4–6 August 2020; pp. 1–4. [CrossRef]
96. Hiesl, A.; Ramsebner, J.; Haas, R. Modelling Stochastic Electricity Demand of Electric Vehicles Based on Traffic Surveys—The Case of Austria. *Energies* **2021**, *14*, 1577. [CrossRef]

97. Liu, C.; Chai, K.K.; Zhang, X.; Chen, Y. Proof-of-benefit: A blockchain-enabled ev charging scheme. In Proceedings of the IEEE Vehicular Technology Conference, Kuala Lumpur, Malaysia, 1 May 2019; pp. 1–6. Available online: https://ieeexplore.ieee.org/abstract/document/8891291 (accessed on 7 December 2021). [CrossRef]
98. Thukral, M.K. Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review. *Clean Energy* **2021**, *5*, 104–123. [CrossRef]
99. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]
100. Caramizaru, A.; Uihlein, A. *Energy Communities: An Overview of Energy and Social Innovation*; 2019; Available online: https://publications.jrc.ec.europa.eu/repository/handle/JRC119433 (accessed on 7 December 2021). [CrossRef]
101. Johansson, T.B.; Goldemberg, J. Energy for Sustainable Development: A Policy Agenda. 2002. Available online: https://www.osti.gov/etdeweb/biblio/20340358 (accessed on 7 December 2021).
102. Kapassa, M.T.E.; Touloupou, M. Local Electricity and Flexibility Markets: SWOT Analysis and Recommendations. In Proceedings of the 2021 6th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, 8–11 September 2021; pp. 1–6.
103. Ladleif, J.; Weske, M. A unifying model of legal smart contracts. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Singapore, 2019; Volume 11788, pp. 323–337. [CrossRef]
104. Governatori, G.; Idelberger, F.; Milosevic, Z.; Riveret, R.; Sartor, G.; Xu, X. On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artif. Intell. Law* **2018**, *26*, 377–409. [CrossRef]
105. Liu, Q.; Lin, L.; Li, Y.; Liu, Y. Performance Analysis of Blockchain-Based Internet of Vehicles Under the DSRC Architecture. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (LNICST)*; Gao, H., Fan, P., Wun, J., Xiaoping, X., Yu, J., Wang, Y., Eds.; Springer International Publishing: Cham, Switzerland, 2021; Volume 352, pp. 112–126.
106. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Futur. Gener. Comput. Syst.* **2020**, *105*, 13–26. [CrossRef]
107. Singh, A.; Parizi, R.M.; Han, M.; Dehghantanha, A.; Karimipour, H.; Choo, K.K.R. Public blockchains scalability: An examination of sharding and segregated witness. In *Advances in Information Security*; Choo, K.-K.R., Dehghantanha, A., Parizi, R.M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 79, pp. 203–232.
108. Ashfaq, T.; Younis, M.A.; Rizwan, S.; Iqbal, Z.; Mehmood, S.; Javaid, N. Consensus Based Mechanism Using Blockchain for Intensive Data of Vehicles. In *Lecture Notes in Networks and Systems*; Barolli, L., Hellinckx, P., Enokido, T., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 97, pp. 44–55.
109. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Futur. Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
110. Li, S. Application of blockchain technology in smart city infrastructure. In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things (SmartIoT 2018), Xian, China, 17–19 August 2018; pp. 276–282. [CrossRef]
111. Theodouli, A.; Moschou, K.; Votis, K.; Tzovaras, D.; Lauinger, J.; Steinhorst, S. Towards a Blockchain-based Identity and Trust Management Framework for the IoV Ecosystem. In Proceedings of the GIoTS 2020-Global Internet of Things Summit, Dublin, Ireland, 3–5 June 2020. [CrossRef]
112. Mohsin, A.; Zaidan, A.; Zaidan, B.; Albahri, O.S.; Alsalem, M.; Mohammed, K. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Comput. Stand. Interfaces* **2019**, *64*, 41–60. [CrossRef]
113. Javaid, U.; Aman, M.N.; Sikdar, B. A Scalable Protocol for Driving Trust Management in Internet of Vehicles with Blockchain. *IEEE Internet Things J.* **2020**, *7*, 11815–11829. [CrossRef]
114. Vangulick, D.; Cornelusse, B.; Ernst, D. Blockchain for peer-to-peer energy exchanges: Design and recommendations. In Proceedings of the 20th Power Systems Computation Conference (PSCC 2018), Dublin, Ireland, 11–15 June 2018; pp. 1–7. [CrossRef]
115. Pu, Y.; Xiang, T.; Hu, C.; Alrawais, A.; Yan, H. An efficient blockchain-based privacy preserving scheme for vehicular social networks. *Inf. Sci.* **2020**, *540*, 308–324. [CrossRef]
116. Sun, G.; Dai, M.; Zhang, F.; Yu, H.; Du, X.; Guizani, M. Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles. *IEEE Internet Things J.* **2020**, *7*, 7868–7882. [CrossRef]
117. Han, Q.; Yang, Y.; Ma, Z.; Li, J.; Shi, Y.; Zhang, J.; Yang, S. CMBIoV: Consensus Mechanism for Blockchain on Internet of Vehicles. In *Communications in Computer and Information Science*; Springer: Singapore, 2020; Volume 1267, pp. 347–352.
118. Bhatia, G.B.A. A Fast, Secure and Distributed Consensus Mechanism for Energy Trading Among Vehicles using Hashgraph. In Proceedings of the International Conference on Information Networking, Barcelona, Spain, 7–10 January 2020; Volume 2020, pp. 772–777. [CrossRef]
119. Chen, X.; Zhang, T.; Ye, W.; Wang, Z.; Iu, H.H.C. Blockchain-Based Electric Vehicle Incentive System for Renewable Energy Consumption. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *68*, 396–400. [CrossRef]
120. Lazaroiu, C.; Roscia, M.; Saatmandi, S. Blockchain strategies and policies for sustainable electric mobility into Smart City. In Proceedings of the 2020 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM 2020), Sorrento, Italy, 24–26 June 2020; pp. 363–368. [CrossRef]

121. Dabbaghjamanesh, M.; Wang, B.; Kavousi-Fard, A.; Hatziargyriou, N.; Zhang, J. Blockchain-based Stochastic Energy Management of Interconnected Microgrids Considering Incentive Price. *IEEE Trans. Control. Netw. Syst.* **2021**. Available online: https://ieeexplore.ieee.org/abstract/document/9354986 (accessed on 7 December 2021). [CrossRef]
122. Pressmair, G.; Kapassa, E.; Casado-Mansilla, D.; Borges, C.E.; Themistocleous, M. Overcoming barriers for the adoption of Local Energy and Flexibility Markets: A user-centric and hybrid model. *J. Clean. Prod.* **2021**, *317*, 128323. [CrossRef] [PubMed]
123. Solanke, T.U.; Ramachandaramurthy, V.K.; Yong, J.Y.; Pasupuleti, J.; Kasinathan, P.; Rajagopalan, A. A review of strategic charging–discharging control of grid-connected electric vehicles. *J. Energy Storage* **2020**, *28*, 101193. [CrossRef]
124. Prashar, D.; Jha, N.; Jha, S.; Joshi, G.P.; Seo, C. Integrating IoT and blockchain for ensuring road safety: An unconventional approach. *Sensors* **2020**, *20*, 3296. [CrossRef] [PubMed]
125. Danish, S.M.; Zhang, K.; Jacobsen, H.A.; Ashraf, N.; Qureshi, H.K. BlockEV: Efficient and Secure Charging Station Selection for Electric Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–18. Available online: https://ieeexplore.ieee.org/abstract/document/9310692 (accessed on 7 December 2021). [CrossRef]
126. Tsolakis, A.C.; Moschos, I.; Votis, K.; Ioannidis, D.; Dimitrios, T.; Pandey, P.; Katsikas, S.; Kotsakis, E.; Garcia-Castro, R. A Secured and Trusted Demand Response system based on Blockchain technologies. In Proceedings of the 2018 IEEE (SMC) International Conference on Innovations in Intelligent Systems and Applications (INISTA 2018), Thessaloniki, Greece, 3–5 July 2018; pp. 1–6. [CrossRef]
127. Roscia, G.C.L.M. Blockchain and smart metering towards sustainable prosumers. In Proceedings of the International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM 2018), Amalfi, Italy, 20–22 June 2018; pp. 550–555. [CrossRef]
128. Zhao, S.; Li, Y.; Wang, B.; Su, H. Research on the Blockchain-based Integrated Demand Response Resources Transaction Scheme. In Proceedings of the 2018 International Power Electronics Conference (IPEC-Niigata-ECCE Asia 2018), Niigata, Japan, 20–24 May 2018; pp. 795–802. [CrossRef]
129. Cioara, T.; Anghel, I.; Pop, C.; Bertoncini, M.; Croce, V.; Ioannidis, D.; Votis, K.; Tzovaras, D.; D'Oriano, L. Enabling New Technologies for Demand Response Decentralized Validation Using Blockchain. In Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I and CPS Europe 2018), Palermo, Italy, 12–15 June 2018; pp. 1–4. [CrossRef]
130. Tsao, Y.C.; van Thanh, V.; Wu, Q. Sustainable microgrid design considering blockchain technology for real-time price-based demand response programs. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106418. [CrossRef]
131. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3154–3164. [CrossRef]
132. Zhou, Z.; Wang, B.; Dong, M.; Ota, K. Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 43–57. [CrossRef]
133. Xiao, H.; Qiu, C.; Yang, Q.; Huang, H.; Wang, J.; Su, C. Deep reinforcement learning for optimal resource allocation in blockchain-based IoV secure systems. In Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking (MSN 2020), Tokyo, Japan, 17–19 December 2020; pp. 137–144. [CrossRef]
134. Dwivedi, S.K.; Amin, R.; Vollala, S.; Chaudhry, R. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. *Comput. Electr. Eng.* **2020**, *86*, 106719. [CrossRef]
135. Taiyaba, M.; Akbar, M.A.; Qureshi, B.; Shafiq, M.; Hamza, M.; Riaz, T. Secure V2X Environment using Blockchain Technology. In Proceedings of the PervasiveHealth: Pervasive Computing Technologies for Healthcare, Atlanta, GA, USA, 18–20 May 2020; pp. 469–474. [CrossRef]