A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain

Journal of
Sensor and Actuator Networks

MDPI

Review

A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain

Wendong Chen [1], Haiqin Wu [2,*], Xiao Chen [3,*] and Jinfu Chen [1]

[1] School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China
[2] School of Software Engineering, East China Normal University, Shanghai 200062, China
[3] School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, UK
* Correspondence: hqwu@sei.ecnu.edu.cn (H.W.); xiao.chen@ed.ac.uk (X.C.)

Abstract: Numerous academic and industrial fields, such as healthcare, banking, and supply chain management, are rapidly adopting and relying on blockchain technology. It has also been suggested for application in the internet of vehicles (IoV) ecosystem as a way to improve service availability and reliability. Blockchain offers decentralized, distributed and tamper-proof solutions that bring innovation to data sharing and management, but do not themselves protect privacy and data confidentiality. Therefore, solutions using blockchain technology must take user privacy concerns into account. This article reviews the proposed solutions that use blockchain technology to provide different vehicle services while overcoming the privacy leakage problem which inherently exists in blockchain and vehicle services. We analyze the key features and attributes of prior schemes and identify their contributions to provide a comprehensive and critical overview. In addition, we highlight prospective future research topics and present research problems.

Keywords: blockchain; internet of vehicles (IoV); vehicular ad hoc networks (VANETs); privacy preservation

Citation: Chen, W.; Wu, H.; Chen, X.; Chen, J. A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain. *J. Sens. Actuator Netw.* **2022**, *11*, 86. https://doi.org/10.3390/jsan11040086

Academic Editor: Mohamed Benbouzid, Leandros Maglaras and Mohamed Amine Ferrag

Received: 17 October 2022
Accepted: 14 December 2022
Published: 19 December 2022

1. Introduction

In recent years, the internet of vehicles (IoV), a new networking paradigm, has been growing rapidly and has a promising future. IoV cars are commonly equipped with radar, navigation and positioning, vision sensors, etc. They can collect road environment data and real-time traffic conditions and submit them to the cloud so that other users can plan their routes in advance by accessing these data. Therefore, the IoV has brought great convenience to users. The term vehicular ad hoc network (VANET) was developed from mobile ad hoc network (MANET) to describe a complex and special network of vehicles or other devices in an area in a real traffic environment. VANET combines the global position system (GPS) and wireless communication network to provide a fast data access network for high-speed moving vehicles. In addition, it can provide drivers and passengers with weather information, music, infotainment, etc. [1]. VANET provides a powerful solution for roads and vehicles and greatly improves the traffic environment [2].

The IoV system is a complex system composed of multiple network participants, such as vehicles, road side units (RSUs), and people, communicating through wireless networks. With the increasing maturity of autonomous driving technology, VANET will progressively manage large-volume vehicle information and user data in the future. Users who share information may face severe security and privacy risks, such as leakage of driver identity, current location, and navigation information. At the same time, because of high liquidity and volatility, in-vehicle networks are susceptible to a variety of threats [3]. Common attacks include bogus information, Sybil attack, and denial of service (DoS). Suppose that attackers tamper with data and maliciously upload traffic information; in that case, it will bring great trouble to the urban transportation network and even violate the

passengers' safety (e.g., traffic accidents and casualties). Therefore, ensuring secure data sharing without compromising user-side privacy in VANET is essential.

In recent years, a substantial amount of study has been undertaken on the security and privacy concerns in VANETs. Garg et al. [4] reviewed existing VANET security protocols and algorithms and discussed the challenges of realizing a secure IoV architecture. The authors of [5] presented a basic view of VANET applications, various forms of assaults, security needs, and the current status of security and privacy protection concerns. Finally, they discussed the numerous authentication schemes and challenges in VANETs. The authors of [6] presented a complete literature review on security and privacy solutions for 5G vehicular networks, where communication utilizes multiple communication models and technologies that are vulnerable to eavesdropping, interference, Sybil attacks, distributed denial of service (DDoS), and DoS.

In contrast, some work focused on specific security and privacy threats in VANETs. Mathew et al. [7] compared different approaches to protect the identity of the IoV. Lu et al. [8] discussed anonymous authentication schemes for protecting the identity privacy of each vehicle and summarized three types of trust models and important properties for establishing effective trust management in VANETs. Location privacy is also a crucial aspect of privacy protection in VANETs. The attacker may use the communication to steal the user's confidential information, such as itinerary, destination, etc. Recognizing these location privacy threats, Reference [9] surveyed some recently launched location privacy protection solutions for VANET and evaluated these techniques critically concerning various operational and security parameters. On the other side, the authors of [10] comprehensively discussed trust-management models in VANETs, compared cryptography and trust models against different types of attacks, and discussed security and privacy issues in vehicular cloud computing (VCC).

However, the solutions assessed in the aforementioned research still rely on a trusted authority (TA) to accomplish the desired functionality and security features. As the number of connected vehicles increases, TAs will be tasked with a large amount of computation and storage, leading to single-point-of-failure problems. The emergence of blockchain brings opportunities for the IoV to solve such problems, attributed to the invariance and controllability of data access and the support of smart contracts in blockchain. Reference [11] focused on the integration of blockchain with vehicular networks. The article detailed prior blockchain-empowered schemes for the IoV. They also analyzed the different requirements in the application of blockchain-based IoV and introduced the research challenges in the corresponding domain. Reference [12] analyzed the main features and performance of existing solutions for privacy protection from the perspective of the practical application of blockchain in IoV, and classified and compared the solutions.

Although there have been many studies on the privacy protection of the IoV, the exploration of using blockchain technology to integrate the privacy protection of the IoV still requires in-depth research. The two aforementioned reviews [11,12] mainly categorize and discuss from the perspective of connected vehicle applications (e.g., advertisement and in-vehicle entertainment) in blockchain environments, while our paper summarizes and categorizes the existing blockchain-based privacy protection schemes for connected vehicles according to different privacy types (identity privacy, location privacy, and data privacy) and summarizes the privacy protection schemes used in them. The following are the key contributions made in this paper:

- We classify the most recent study on blockchain-based privacy protection in the IoV according to the types of privacy to be safeguarded.
- A categorization of the mentioned blockchain-based privacy protection schemes for IoV is provided, considering the type of blockchain adopted by the scheme and the blockchain framework used at the bottom.
- We summarize the shortcomings and research challenges in prior solutions and envision potential research directions for future work.

2. Research Methodology

The approach for studying blockchain-based privacy solutions for the IoV can be divided into two parts as follows: the research methods and analysis of results.

2.1. The Research Method

In this work, we perform a comprehensive assessment of IoV blockchain-related privacy-preserving methods. For paper selection and filtering, we follow the three steps below.

First, we searched the Scopus database (www.scopus.com, retrieved on 4 July 2022) for papers on blockchain-based solutions in the IoV. The search aimed to find papers most similar to the research topic "Blockchain-based privacy protection schemes proposed in IoV". Therefore, we utilized phrases such as "IoV", "blockchain", "privacy", "smart vehicle", "vehicular networks", and "Cooperative and Intelligent Transport Systems" in our literature search. The search terms are as follows:

TITLE-ABS-KEY ((vanet OR "smart vehicle" OR "IoV" OR "vehicular networks" OR "Cooperative and Intelligent Transport Systems" AND blockchain AND privacy) AND(LIMIT-TO(SUBJAREA, "COMP"))

Then, we filtered the articles according to the category partition of the journals or conferences in which they were published, and discarded some articles published in journals/conferences that ranked relatively low, while we also fully considered the impact factor of the journals.

Our research focuses on privacy protection for the IoV based on blockchain. The blockchain consists of several decentralized nodes that lack mutual trust. Each node keeps a replica of the blockchain database and manages the on-chain data collectively. When a majority of nodes in the blockchain system confirm a new block (the number depends on the consensus process), miners add it to the blockchain. The distributed consensus and cryptographic techniques, such as hash chain and digital signature mechanisms, ensure the on-chain data consistency, integrity, and immutability. This article examines what specific technologies blockchain can incorporate to improve VANET, especially for security and privacy enhancement. This review aims to explore the existing applications or proposals for applying blockchain technology to the IoV field. We further organize, summarize, and point the way for future research directions.

2.2. Analysis of Results

In this subsection, we analyze the paper according to the method in Section 2.1. We searched for related keywords on Scopus on 5 July 2022, and returned a total of 181 articles. We repeatedly selected 41 papers that were most relevant to our research. These papers are all related to privacy protection in blockchain-based IoV, including identity privacy, location privacy, and data privacy. Figure 1 displays the year of publication for the selected publications. The included articles were published between 2018 and 2022, with a steady rise between 2018 and 2020. The number in 2021 is the same as that in 2019, and the lower number in 2022 is because the retrieval result only involves papers published before August. We expect more papers to be accepted and published in the next couple of months.

Considering the forms of privacy protection offered by the blockchain technology for the IoV, most of the papers (73.17%) we surveyed focus on protecting vehicle identities, called identity privacy. Location privacy (36.59%) and data privacy (34.15%) were roughly equal in volume. The vertical diagram of the three privacy types is shown in Figure 2. However, most of these documents do not offer a solitary type of security for the user's privacy. As shown in Figure 3, the Venn diagram reveals that 8 (19.51%) of the papers provide privacy for both identity and location, 4 (9.76%) provide privacy for both identity and location, and 3 (7.32%) provide all types of privacy.

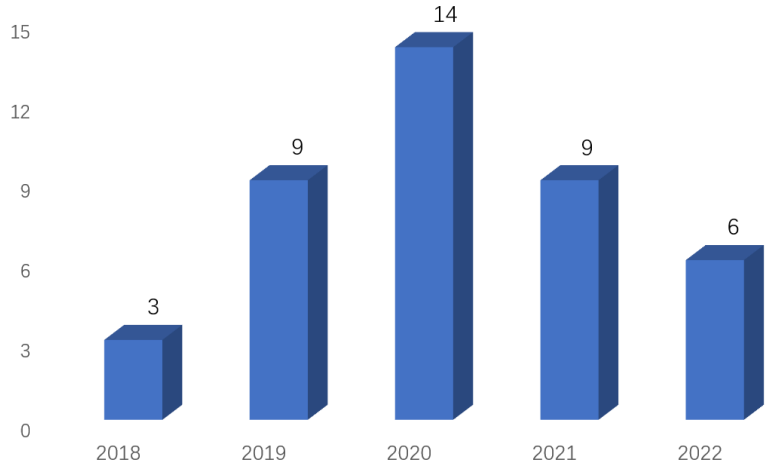

Figure 1. Year distribution map of selected papers.

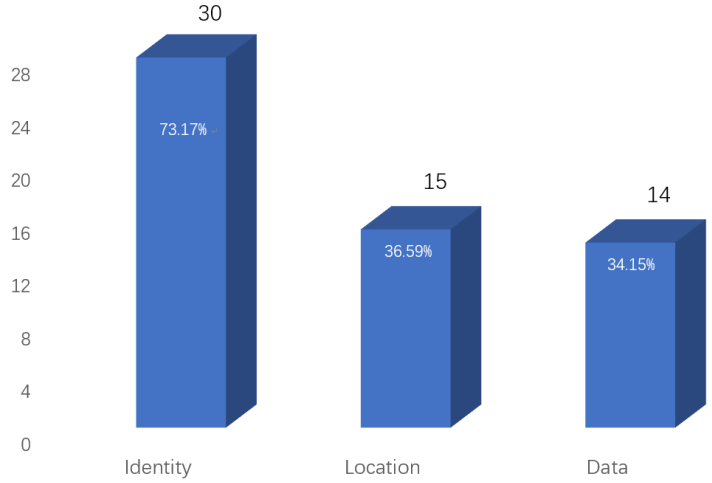

Figure 2. The sorts of privacy that appear in the papers.

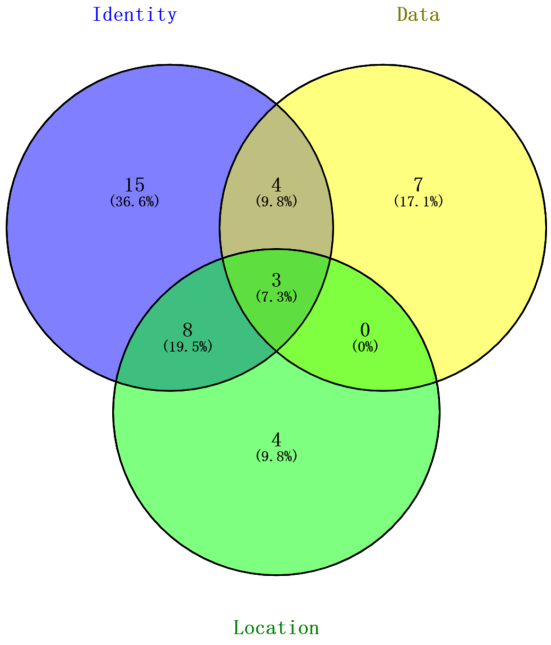

Figure 3. The forms of privacy covered in the papers.

Classifying the different categories of blockchains [13], 25 solutions (60.98%) proposed schemes based on the permissioned blockchains, 8 papers (19.51%) use permissionless blockchain, and 4 studies (9.76%) use both permissioned and permissionless (i.e., hybrid) blockchains. As seen in Figure 4, 4 (9.76%) articles do not specify the type of blockchain employed in their solution.

Among the selected papers, Hyperledger Fabric (21.95%) and Ethereum (17.07%) are the most commonly used blockchain platforms in the proposed schemes (see Figure 5). In comparison, most papers (60.98%) do not mention a specific blockchain platform.

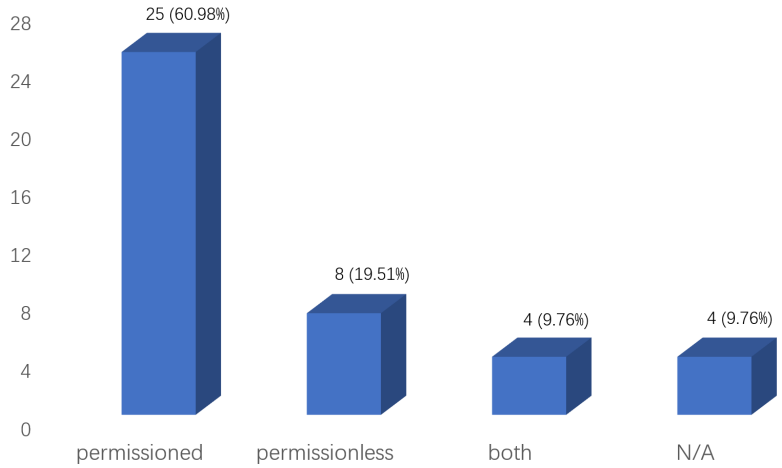

Figure 4. Types of blockchains presented in the papers.

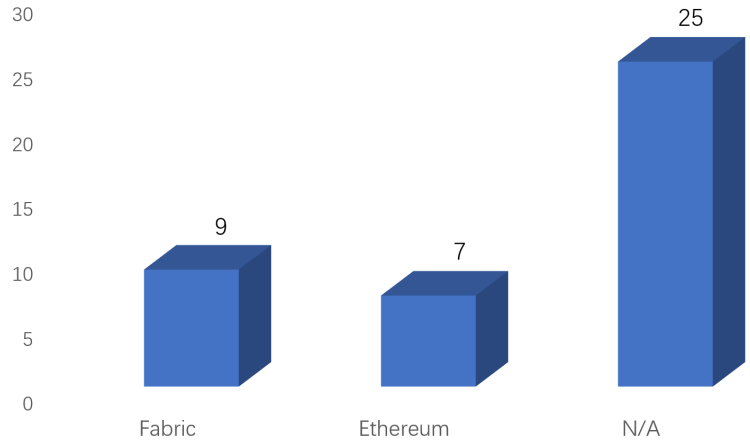

Figure 5. The blockchain framework covered in the papers.

As shown in Figure 6, we categorize the representative privacy protection techniques employed in the paper according to different privacy concerns. Since many papers may use multiple techniques, we do not label the specific number with respect to each method. However, pseudonyms are still the most often adopted technique.

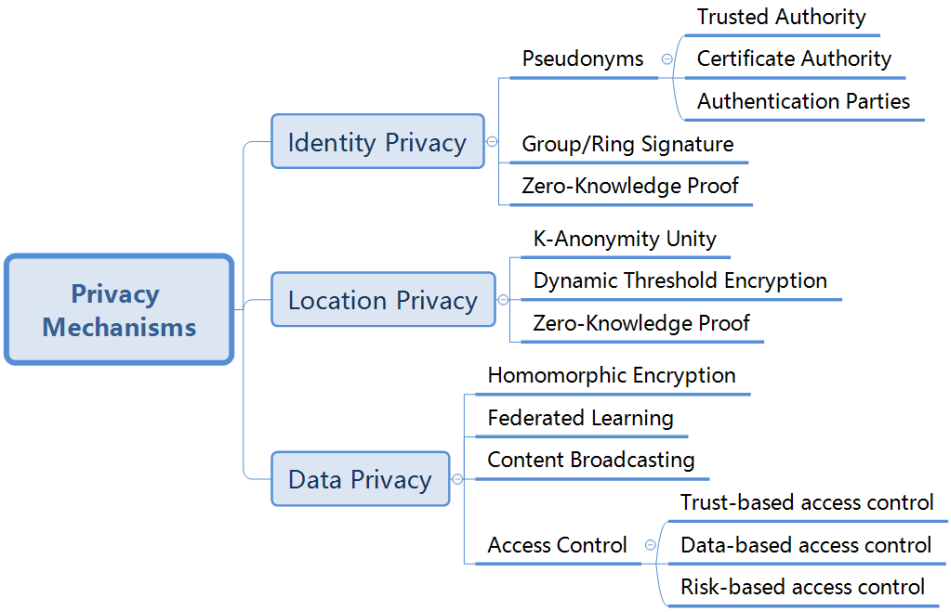

Figure 6. Typical privacy protection techniques adopted in the papers.

3. Background

This section presents some background knowledge. We briefly introduce the IoV, including its basic system architectures. Then, we elaborate on blockchain technology and its significant characteristics.

3.1. Internet of Vehicles

The IoV is a new paradigm, an integrated platform that combines IoV technologies with intelligent transportation systems. It targets to solve the primary limitations of in-vehicle Ad Hoc networks [14], such as scalability, interoperability, quality of service, and data processing. The IoV can provide numerous benefits, such as traffic management, safe driving, autonomous driving, road safety (intersection coordination, dynamic regulation of traffic lights), and infotainment.

Various architectures for IoV were discussed in articles [15,16]. Overall, IoV comprises three entities: central server, edge devices, and vehicles. Edge devices are responsible for transmitting communications between vehicles or to a central server. In addition, they feature specialized management capabilities, such as message aggregation and data extraction. A centralized server collects and processes data from all cars and the internet. It stores all information and offers a variety of vehicle and user functions. Figure 7 shows a standard blockchain-based model of an IoV vehicle authentication system with four entities.

- Trusted authority (TA): The city's vehicle registration and management center is a trusted third party. It is responsible for vehicle registration and the revocation of malicious vehicles, such as those reported by certain vehicles after being identified, to send false information about roads, traffic, or the environment. Additionally, it provides deployment and maintenance of smart contracts for vehicle registration and cancellation. TA is an entity with strong computational and communication capabilities and is totally trusted by the system. It is the sole entity that knows the true identity of the vehicle.
- RSU: RSUs can communicate directly with vehicles in radio range and transmit messages to TAs or central servers. The RSU is responsible for verifying the legitimacy of the vehicle and assigning regional secrets to verified vehicles. The RSU is semi-trustworthy, meaning that it would follow the specified interaction protocol, but may want to know the private information about the vehicles due to curiosity or being attacked (e.g., once an adversary attacks the RSU, it can access the vehicle's authentication information).

- Vehicle: The vehicle's on-board unit (OBU) is installed, which also has a communication and computing unit. In IoV, vehicles must be authenticated before communicating with other vehicles or posting messages. Otherwise, the messages sent are regarded as invalid and discarded.
- Blockchain: The blockchain is a decentralized and trustworthy platform that ensures the integrity of data. Registration data will be uploaded on the blockchain so that users and RSUs can quickly search the recorded data. Transaction information is connected to secure the authenticity, validity, and immutability of shared multimedia material.

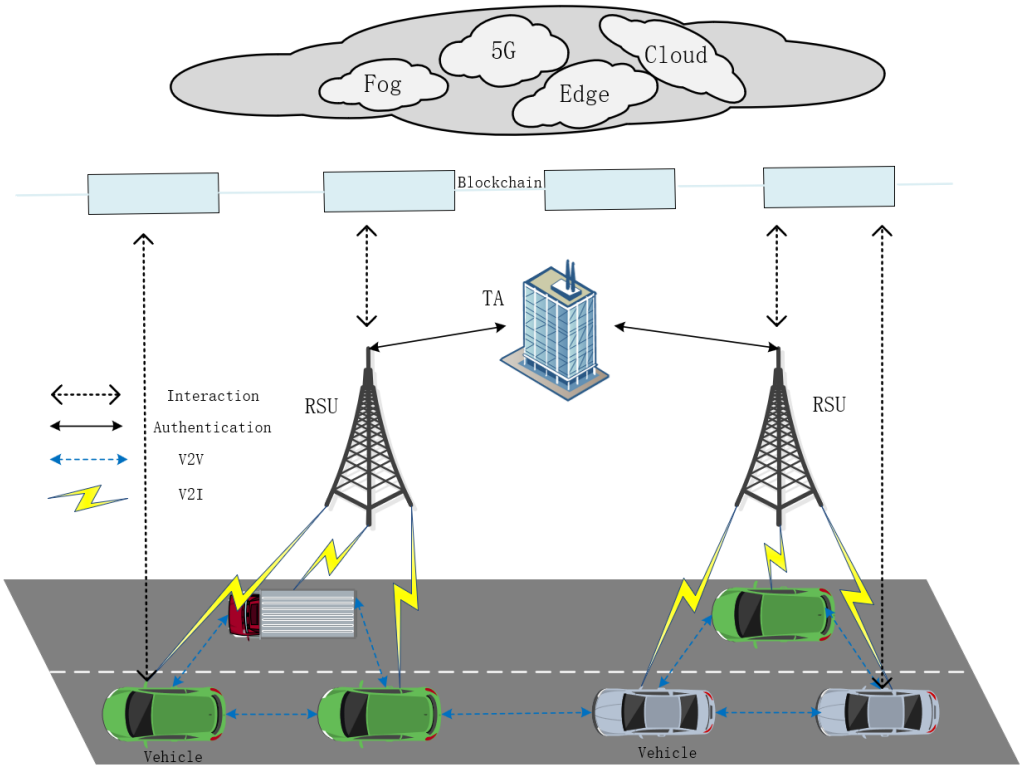

Figure 7. Authentication model for the IoV based on blockchain technology.

3.2. Blockchain

3.2.1. Introduction to Blockchain

Blockchain is a distributed and shared ledger. It is constructed using a peer-to-peer (P2P) network. The network intends to maintain a connected database amongst all blockchain network participants who reach consensus using a particular consensus technique, e.g., proof of work (PoW) [17]. The blockchain ledger maintains an ordered list of chain blocks that contain transactions, currencies, data, and certificates. All records of trades between members of multiple blockchains (BCs) are stored in this distributed ledger, whose replica is jointly maintained by the network peers. Cryptographic techniques and distributed consensus ensure that all on-chain transactions cannot be tampered with. PoW assumes that a group of miners cannot control more than 50% of the network computation power. Otherwise, we consider it vulnerable to a 51% attack. Other consensus algorithms work for different blockchains, such as proof of stake (PoS), proof of authority, and practical byzantine fault tolerance (PBFT). Overall, BCs can create a transparent, safe, and unchangeable environment.

The smart contract is an integral part of the blockchain [17]. Smart contracts are computer programs based on blockchain and are designed to run automatically whenever certain conditions are met. They are frequently used to conduct automated procedures so that all parties can quickly ascertain the result without needing an intermediary, saving time. They can also automate workflows by triggering operations when conditions are met.

Three types of blockchains [18,19] have been developed to fulfill the demands of various users: public chain, private chain, and consortium chain.

- Public chain: No complex requirements exist for the participation authority of the public chain, and any individual or organization can join and leave freely. All data records on the public chain are open and transparent, and anybody may participate in the consensus procedure. The public chain is an institution-free blockchain that is entirely decentralized. The most typical representative of the public chain is the Bitcoin system. The system is open to everyone, and the information in the Bitcoin system is completely open and transparent.
- Private chain: Also known as an internal chain, it is a non-public "chain" that usually requires authorization to join the nodes and has a shallow degree of openness. Access to write and modify data is only in the hands of insiders, and it is a single central network of private organizations. Many large groups of companies are currently developing their private chains, which can be used for corporate management, financial auditing, bank clearing, settlement, etc.
- Consortium chain: It is jointly participated by multiple organizations and has an excellent cooperative relationship with each other. The degree of openness of the consortium chain is between the public and private chains, and the writing and modification rights are still in the hands of multiple organizations. It is regarded as a partially decentralized blockchain. The participants of the consortium chain have a high degree of mutual trust, where the verification efficiency is fast, the transaction cost is significantly reduced compared with the public chain, and part of the data privacy can be well-protected. Consortium members can only share the information and resources on the consortium chain. The well-known consortium chain includes the R3 blockchain [20] and Hyperledger Fabric [21]. In a blockchain, a consensus result is reached between multiple nodes for a particular state mainly through a consensus algorithm.

3.2.2. The Reason Why Blockchain Can Be Combined with the IoV

As in [22], some of the major security requirements in IoV are as follows:

- Data integrity—guaranteeing that messages exchanged are protected from alteration or modification by attackers;
- Vehicle authentication—recognizing valid vehicles and making sure they are what they claim to be;
- Vehicle privacy and anonymity—guaranteeing that the vehicle's private information is not leaked and cannot be traced by attackers;
- Access control—granting access to data and services of various entities in the network.

With the following characteristics, blockchain is a promising technology that can effectively satisfy the aforementioned IoV security requirements:

- Decentralization: BC is a distributed system without a centralized authority that is able to offer a secure solution.
- Cryptocurrency: Many BC ledgers offer cryptocurrency exchange services. Vehicle cooperation can be effectively facilitated by developing efficient, secure, and automated incentives.
- Transparency: All nodes in the BC network have access to the contents of the BC ledger.
- Pseudonymity: Each BC user is associated with an anonymous address. This method enables the deployment of privacy protection services.
- Availability: As a result of the BC decentralization, there is no single failure point. This significantly increases the system's availability and dependability.

4. Privacy Protection Scheme for IoV on Blockchain

Privacy protection has recently become a hot topic in IoV research [23,24]. Privacy is a security property that an individual or a group can protect his confidential information

from unauthorized use [25]. Protecting user privacy is very important for the IoV, as it is a system of many mutually distrustful participants. In addition, with the increase in the types of services provided by the IoV [26], the data on vehicle interaction are also increasingly growing. We may divide privacy protection into three categories based on the information to be protected: identity privacy protection [27–41], location privacy protection [42–53], and data privacy protection [54–68].

- Identity privacy: It protects the user's true identity from disclosure, mainly through using pseudonyms during in-vehicle system communications.
- Location privacy: It safeguards the user's location information, often using camouflage and clustering techniques.
- Data privacy: It secures personal user data, such as vehicle trajectories, speeds, and temporary messages among vehicles. For data privacy, encryption techniques, such as homomorphic encryption, are utilized.

4.1. Identity Privacy

With the massive use of IoV, more and more users enjoy convenience, while the privacy of users' identities has been threatened and challenged. The literature [27–30] addressed this issue and proposed various privacy-preserving authentication schemes in combination with blockchain technology.

As vehicle ad hoc networks have evolved, network security and privacy have received more attention, especially as attackers have more and more resources. In response to these problems, Liu et al. [27] proposed a dynamic anonymous authentication scheme (DAIA) based on blockchain and the elliptic curve discrete logarithm problem. The scheme guarantees offline updates, pseudonym tracking, and anonymous authentication while improving the efficiency of keys in the face of dynamic changes. The system model has three main actors: the certification authority (CA), the RSU, and the vehicle. When a vehicle roams in different RSU communication ranges, it uses a tamper-proof device (TPD) to generate dynamic pseudonym keys for anonymous and offline authentication. Even in the worst case, such as when all RSUs are compromised, the vehicle's identity remains private. Simulation results show that although the scheme is slow compared to other schemes, it is more suitable for real-world VANET environments by virtue of its good security and privacy protection.

To ensure secure dissemination of road traffic information in VANET, Guehguih et al. [28] proposed a geo-blockchain-based scheme. The scheme seeks to ensure the confidentiality of authentication and message distribution, containing two different blockchains. They use private blockchains for authentication and public blockchains to manage event messages. A trusted authority (TA) is in charge of conducting transactions in a private blockchain within the borders of the country. The transaction contains the identifying information necessary to authenticate the vehicle upon its initial network connection. Other vehicles have the right to read and check the authenticity of the new cars from the private blockchain. The public blockchain is used to store event messages within the boundaries of predefined areas to ensure the security of message propagation. The text refers to it as the roadside unit blockchain (RSU-BC) because it is in a VANET. In this way, the need to deploy RSUs in VANET is eliminated, and the reliance on TA is reduced. Analysis of performance reveals that the system has lower computational and communication overheads, making it more appropriate for VANET implementation.

Shi et al. [29] presented a blockchain-based privacy protection strategy for the sharing of multimedia data in vehicular social networks (VSN). Using cryptographic primitives, it conceals the true identities of users, cars, and RSUs. Moreover, blockchain ensures the integrity of data sources and prohibits the manipulation or falsification of multimedia data by attackers. Using blockchain, Yang et al. [30] proposed an authentication system. The method supports anonymous authentication by storing the mapping of pseudonyms and public keys through blockchain, thus enabling the protection of vehicle privacy. Simultaneously, malevolent cars can be revoked with minimal expense. In addition, neither the

vehicle nor the trusted authority needs to keep a significant number of pseudonyms. With the installation of a regional management entity, the number of cars impacted by malicious vehicles during revocation is considerably reduced, and a compromise is reached between the frequency of vehicle authentication and the number of affected vehicles.

Among the methods of IoV privacy protection, public keys and anonymous certificates are common. At the same time, many new technologies are gradually incorporated into IoV protection. While new technologies bring convenience, they also raise new problems, and scholars have explored new approaches [31–38] for this purpose.

The success of the IoV depends mainly on its robustness of IoV, as data rights disputes or any form of security breach between service providers can completely disrupt transportation services. Sharma et al. [31] proposed an efficient in-vehicle information system called BlockAPP (Blockchain for Authentication and Privacy Protection), which utilizes blockchain for privacy-preserving authentication. With its decentralized, robust, and scalable nature, blockchain can be used to enable seamless access control and vehicle authentication services, providing a new solution for all service providers. The proposed architect is decentralized, robust, and scalable. The system has four primary components: the registration server, the service provider, the blockchain, and the vehicle. The authors constructed the system on the Ethernet platform and deployed Solidity smart contracts on the Remix platform. The results demonstrate that blockchain ensures data integrity and consensus across distributed service providers.

Moussaoui et al. [32] presented a blockchain-based public key infrastructure (PKI) scheme to enhance identity privacy in VANET. The central authority (CA) grants the first pseudonym (initial pseudonym), and the vehicle produces a pseudonym and creates a blockchain transaction to request registration in the blockchain. Two blockchains were proposed: the pseudonym blockchain (PBC) and the pseudonym revocation blockchain (PRBC). The PBC saves pseudonyms, and its neighbors generate a signature-based revocation request when a rogue node is discovered. If the transaction is confirmed and authenticated, the PRBC will record the pseudonym of the malicious node.

Pseudonymous certificates are a common approach to addressing automotive privacy issues, and a certificate management solution can administer the system and maintain the certificate lifecycle. Bao et al. [33] proposed an effective pseudonym certificate management scheme. Blockchain was developed to ease network architecture and distributed certificate revocation list management (CRLs). This method cuts down on the communication overhead and the time it takes by putting some of the certificate revocation functionality into the programs dealing with security and privacy. The solution's effectiveness is proven through simulation and analysis, and blockchain provides a more economical solution to combat cyber attacks while consuming fewer network resources.

According to existing studies, the cluster-based media access control (CB-MAC) protocol has reasonable control and management performance in VANET. However, it still needs improvement in security and privacy protection. For this purpose, Akhter et al. [34] presented a blockchain-based authentication model for cluster-based VANET systems. Vehicles and authentication centers are included in the architecture. In the article, they describe the construction of the authentication center, the registration of vehicles, and the generation of keys. The storage of all vehicle information in the architecture is handled by the global authentication center (GAC). Meanwhile, the local certification center (LAC) is responsible for keeping the blockchain for fast switching between vehicle clusters. All blockchains communicate with each other using a 5G network, and the RSA-1024 digital signature algorithm is used to transmit encrypted information, thus increasing security and confidentiality. Therefore, there is no need to use RSU. Experiments demonstrate that the approach performs well in terms of time and storage. The numerical analysis demonstrates that the proposed transmission protocol surpasses the conventional medium access control (MAC) and benchmark approaches in terms of throughput, latency, and packet loss.

Edge computing offloads computing tasks locally with low latency, which can reduce the burden of vehicular computing and storage in IoV. However, there are still concerns

about data integrity and privacy. In order to tackle these issues, using blockchain-enabled IoV and edge computing, Qian et al. [35] presented an efficient privacy-preserving authentication technique to address these issues. In detail, edge computing and federated blockchain combine to perform efficient computing and storage capabilities while providing low communication latency and data auditability. In addition, conditional identity privacy protection and vehicle message authentication are achieved using pseudonym mechanisms and identity-based signatures, respectively. Then, a clustering selection and critical update algorithm based on the Chinese residual theorem is proposed to ensure the transmitted information's forward and reverse security according to the vehicles' dynamic changes. Finally, the security analysis demonstrates that the proposed approach fulfills the vehicle communication security criteria. Both numerical and performance analysis show that the method is valuable and feasible in the IoV.

For privacy-preserving authentication in IoV, Akhter et al. [36] proposed a blockchain-based scheme. With its distributed and decentralized nature, blockchain can be used to store and manage authentication messages. The scheme is developed on Ethernet using digital signature algorithms, thus guaranteeing the confidentiality, non-repudiation and integrity of IoV. The suggested cooperative protocol is subjected to quantitative analysis, which reveals that it successfully increases system throughput while simultaneously reducing both latency and packet dropping rate (PDR).

In-vehicle broadcast networks are among the most promising utilities in smart vehicle communication and intelligent transportation systems. However, there are currently two main problems with building an effective in-vehicle broadcast network. Firstly, it is challenging to forward trustworthy notifications without disclosing the sender's identity. Second, users lack incentives to post announcements. Li et al. [37] aimed to overcome both issues by developing CreditCoin, a privacy-protecting announcement network based on blockchain technology. On the one hand, CreditCoin enables a large number of untrustworthy individuals to produce signatures and make announcements anonymously in an environment that is not totally trusted. CreditCoin, on the other hand, encourages people to contribute the information it obtains via blockchain. In addition, CreditCoin enables conditional privacy by virtue of its trace manager, which allows the identity of malicious users to be tracked in announcements through relevant transactions. Tests have shown that CreditCoin is functional and efficient in smart vehicle simulation.

Lee et al. [38] developed a distributed reward solution based on blockchain for driver privacy in terms of the security of driver-provided information in IoV. By using pseudonyms instead of unique identifiers, drivers can protect their location privacy from potential attackers. In this solution, a key role is played by the embedded tamper-proof black box, which is loaded on each vehicle and has been used to design security protocols. The black box supports hardware storage, such as smart cards, which ensures that confidential information is not compromised, even if the vehicle's black box (VBB) is stolen. To prevent associations between old and new pseudonyms, the rest of the information is changed every time a new identity is created. Therefore, the anonymity and privacy of transactions are guaranteed.

Meanwhile, some scholars have adapted the scheme from a framework perspective [39–41] to address the vulnerability of IoV to attacks.

While VANETs bring improvements to road safety and traffic control, they also pose potential risks to traffic safety. For example, only authenticated vehicles can transmit data, and revoked vehicles do not interfere with communications. Besides a high computational cost and communication overhead, the existing centralized VANET is also susceptible to assault. George et al. [39] proposed a permissioned blockchain to provide a secure, lightweight certification framework and manage the identities of vehicles in the network. They use blockchain to construct decentralized and distributed VANET frameworks, thus avoiding a single point of trust. In addition, blockchain ensures data immutability and enhances the system's integrity. Hyperledger Fabric is used in this paper to maintain and

verify the identities of vehicles, and simulations have been carried out on OMNET++ and SUMO, showing that the system can reduce the computing power of the RSU.

Shrivastava et al. [40] explored the possibility of deploying blockchain in self-driving car networks and proposed a blockchain-based security model for IoV systems. The decentralized approach has advantages over traditional centralized structures, such as access control and message authentication. The scheme increases vehicle security and provides new ideas for secure communication between vehicles. The scheme keeps the vehicle data on the server and the associated hash values on the distributed ledger. The suggested methodology performs data integrity checks and demonstrates its security and efficiency advantages.

Zheng et al. [41] proposed a framework for a blockchain-based distributed and traceable connected vehicle system with secure communication authentication between vehicles and RSU. This solution offers intelligent vehicles a secure communication environment and conceals users' true identities to achieve anonymity. In addition to preventing internal cars from forging messages for propagation, a distributed blockchain transaction storage method is meant to safeguard their transaction information from attackers while simultaneously tracking bad vehicles.

In summary, identity privacy is an essential component of IoV, and we must verify the identity of a vehicle before it enters the network. Existing identity privacy protection schemes focus on pseudonyms, which are digital certificates with a short life cycle. In the future, we should further optimize the pseudonym update cycle issue to reduce computational consumption.

At the same time, since most schemes do not specify the type of blockchain they use (public, consortium, or private), we distinguish blockchain types in the table with permissioned and permissionless chains. As shown in Table 1, we can find that most of the blockchain types used in the schemes are permissioned chains. Permissioned chains sacrifice some of their decentralization nature in exchange for faster processing speed, which is crucial for IoV.

Table 1. Comparison of identity privacy.

Literature	Underlying Privacy Protection Mechanism	Blockchain Characteristic
[27]	Dynamic Pseudonyms (using TPD)	Permissioned
[28]	Pseudonyms (using Certificate Authority)	Permissioned, Permissionless
[29]	Pseudonyms (using Trusted Authority)	Permissionless
[30]	Anonymous Authentication	Permissioned
[31]	Pseudonyms	Permissioned
[32]	Pseudonyms (using Certificate Authority)	Permissionless
[33]	Pseudonyms Shuffling	Permissioned
[34]	Cluster-based Medium Access Control, Pseudonyms	Permissioned
[35]	Multiple One-Time Pseudonyms	Permissioned
[36]	Digital Signature Algorithm	Permissioned
[37]	Threshold Ring Signature, Combined-Public Keys	Permissioned
[38]	Access Control	Permissioned
[39]	Pseudonyms (using Certificate Authority)	Permissioned
[40]	Access Control	Permissioned
[41]	Pseudonyms (using Service Provider)	Permissionless

4.2. Location Privacy

Because of the high real-time requirements of the IoV, vehicles are required to upload data more frequently, which undoubtedly increases the possibility of vehicle privacy leakage; scholars have proposed their solutions to this problem [42–49].

Under the explosive rise of IoV, vehicle-based spatial crowdsourcing (SC) applications have been presented and swiftly implemented in several domains. However, since workers involved in crowdsourcing tasks in SC need to upload their locations, this may lead to

serious location privacy leakage problems. To address this problem, Zhang et al. [42] proposed a scheme called PriSC, centered on decentralized location privacy protection, by introducing the blockchain. It allows requesters and workers to crowdsource without a third-party platform, guarantees the location policy privacy of tasks, and provides multiple layers of privacy protection for workers' whereabouts. Any requester in the system can verify the evidence of location to prevent workers from faking their whereabouts and unlawfully collecting incentives. Finally, the effectiveness and feasibility of the approach are experimentally verified.

Due to the time-sensitive nature of connected car services, vehicles need to report their location frequently. Su et al. [43] implemented a distributed management mechanism for vehicle public key information, which ensures the storage of the information by virtue of the blockchain's non-tampering feature. The information kept on-chain cannot be tampered with unlawfully. In addition, the connection between the car and the location service provider is anonymized to prevent the service provider from violating the privacy of the vehicle. The system is superior to conventional alternatives regarding communication security and efficiency.

As VANET requires high timeliness and frequent reporting of vehicle information, we enjoy the convenience of location-based services (LBS), while security issues need to be addressed. Bohan Li et al. [44] suggested a trust management approach based on blockchain to constrain and regulate vehicle behavior. The scheme uses certificates as pseudonyms to avoid direct communication between vehicles, reducing the possibility of some privacy leakages. Using anonymous pseudonym areas can also make vehicles immune to location service provider (LSP) attacks. Instead of using the traditional PoX (proof of transfer) algorithm in this scheme, a hot-stack consistency consensus mechanism is used, improving efficiency and reducing resource consumption. Finally, it is shown experimentally that the system runs well in the face of trust model attacks and outperforms its counterparts in vehicle privacy protection.

To mitigate the adverse effects of the VANET centralized design and absence of privacy protection mechanisms, Chaudhary [45] proposed a blockchain-enabled strategy for protecting location privacy called BELP. BELP utilizes joint blockchain technology to implement a decentralized and fast computing environment. The system comprises a registration authority (RA), a user (vehicle), and an RSU. When a vehicle reaches the RSU region, it first sends a registration request to the closest RSU, then to the RA. After that, the RA will forward the request to the intelligent contracts, checking its authenticity through predefined authentication rules. If the vehicle complies with the regulations, the RA uses a pseudonym to index the vehicle. RA will register all data in the federal blockchain. Additionally, vehicles are replaced with pseudonyms in random cycles to prevent pseudonym leakage. Compared to the current centralized structure, the simulations demonstrate that the proposed system provides superior protection for individuals' location privacy.

Similarly, in the design of Liang et al. [46], the issue of ensuring location privacy is addressed. The system comprises four parts: RA, RSU, vehicle, and LSP (location-based service provider). The paper uses digital certificates to replace the pseudonyms in the K-anonymity algorithm. Digital certificates ensure the legitimacy of the user's identity and increase privacy. Additionally, the paper abandons direct communication between vehicles and uses RSU-dominated construction of anonymous cloaking regions, which significantly protects the privacy and reduces the computational burden. Compared with the traditional solution using PoX alone, they use the dual consensus mechanism of PoW + HotStuff to maintain the blockchain. They not only improve computational efficiency, but also reduce resource consumption. Experiments show that the scheme protects user privacy and is immune to classical trust attacks.

Li et al. [47] designed a blockchain-based VANET system model based on blockchain. The model contains the blockchain setup, vehicle registration, SBM (secure beacon message) upload, and blockchain record. The usage of blockchain can successfully address the inherent VANET issues of distrust and centralization. To safeguard identity and location

security, they proposed UGG (undirected graph generation), IPP (identity privacy protection) and LPP (location privacy protection) algorithms. In order to evaluate the availability of *k*-anonymous unification, they additionally introduced two metrics: connectedness and average distance. Simulation experiments involving system time, connectivity and other aspects show that the structure is superior in processing time compared to existing structures, and maintains identity information and guards location privacy.

VANET provides location-based services (LBS) when the vehicle communicates with the environment. The Space–Air–Ground Integrated Network (SAGIN), an integrated product of terrestrial communications and satellite systems, ensures the reliability of LBS, but it does not meet the privacy protection needs of LBS. For this reason, Bohan Li et al. [48] used blockchain to design a trust model for LBS security protection. Instead of choosing the traditional Proof-of-X (PoX: such as PoW and PoS), we adopt the Conflux mechanism, which ensures security and speeds up information processing. The authors also connected the vehicle to SAGIN through RSU to reduce the user communication effort and the danger of communication leakage. Finally, they used trust management to address trust among users in distributed *k*-anonymity algorithms, in which the RSUs construct *k*-anonymous regions. Numerous experiments have shown the high feasibility of the scheme.

One of the most common ways to protect privacy is called *K*-anonymity. In this method, a remote region can hide the real location of the requesting vehicle (RV). However, we assume that all collaborating vehicles (CVs) are always honest, and this aspect allows dishonest CVs to exploit it. For this reason, Feng et al. [49] developed a trusted stealth region construction (TCAC) approach. The scheme employs edge computing to handle a large amount of trust demand from LBS requests. The scheme also proposes a redundant block deletion strategy, which helps preserve the blockchain's timing structure. Security analysis demonstrates that the scheme may prevent the transfer of the requested content of RV and the service result of LSP.

In addition, some practical applications of IoV [50,51] involve the risk of privacy leakage, and scholars have designed schemes for this purpose.

Because of the limited range that electric vehicles can travel after each charge, the charging process becomes frequent. During vehicle charging, the location and charging mode of the electric vehicle may be exposed to the service provider, triggering user privacy issues. In response to these issues, Gabay et al. [50] proposed a framework to protect the privacy of electric vehicles during charging by using smart contracts and zero-knowledge proofs. Initially, the authors offered a method based on smart contracts and tokens that enables authentication, scheduling, and billing independent of other parties. Then, improvements were implemented using the Pederson promise instead of a token mechanism. The authors can use one smart contract to serve all electric vehicles in both cases to improve efficiency. Security analysis shows that the approach does not expose any information to interested parties, such as electric vehicle charging service providers (EVSPs) and public entities within charging stations. Zokrates has also been used to implement two implementation frameworks. The results indicate that the entire process's duration and cost are appropriate for real applications.

With the rapid development of the IoV, there has been a surge in advertising dissemination in the IoV, allowing advertisers to promote their products. However, deploying IoVs faces issues such as vehicle location privacy. In particular, vehicles may defraud advertisers and receive rewards for not spreading their ads. In addition, concerns about privacy invasion may prevent vehicles from participating in the advertising dissemination process. To solve these problems, Ming Li et al. [51] proposed an anonymous advertisement dissemination scheme based on blockchain and aims to enable vehicles to accomplish advertisement dissemination honestly. To ensure fairness, the paper utilizes Merkle hash trees and smart contracts to implement the "ad receipt proof" property (checking whether the vehicle received the ad without cheating or introducing a lot of storage costs) to mitigate "free-rider" attacks. In addition, smart contracts allow for the detection and punishment of ad recipients who repeatedly receive rewards. Anonymity is achieved by applying

zero-knowledge proof technology, which protects vehicle privacy. Finally, the solution is shown to be feasible and efficient through a large number of security implementations.

Some scholars [52,53] have also designed incentive mechanisms to address the problem of users' fear of privacy leakage and rejection of data upload in IoV.

The problem of user-side insufficient participation in connected vehicle spectrum data sharing can be attributed to users' fear of their location privacy leakage. For this reason, Li et al. [52] proposed an incentive mechanism based on location privacy protection (IMLPP). First, a K-anonymity location protection scheme that enables multi-user cooperation is constructed. Then, an incentive system is created to encourage people to share. Each user has a baseline honesty level, which varies in real time based on their actions. The simulation demonstrates that the technique may boost user participation in IoV spectrum sharing while maintaining location security.

Wang et al. [53] introduced credit values for this purpose, utilizing a multi-attribute decision making (MADM) algorithm to convert the user's data into credit values, in response to the problem that many location privacy-preserving algorithms are typically based on theoretical data and lack actual user data. In addition, the bills of anonymous zones are recorded on the blockchain using a credit value reward and punishment mechanism based on the blockchain. Lastly, the method analysis and simulation demonstrate that the method successfully restricts unwanted user behavior while generating anonymous zones and protects the confidentiality of user location data.

As shown in Table 2, we compared the literature on location privacy protection. It is easy to see that K-anonymity is an important technology used today to protect location privacy. We can find that permissioned chains still dominate the majority. This is because permissioned blockchains achieve a higher level of security because they provide access control compared to permissionless blockchains. In the future, on the one hand, we need to incentivize more users to upload their data. On the other hand, we can combine existing advanced technologies (e.g., differential privacy technology) to design better solutions to address the problem of location privacy leakage and fully consider the possibility of its practical application.

Table 2. Comparison of location privacy.

Literature	Underlying Privacy Protection Mechanism	Blockchain Characteristic
[42]	Additively Homomorphic Encryption	Permissioned
[43]	Pseudonyms (using Public Keys)	Permissionless
[44]	Anonymous Cloaking Regions, Pseudonyms	Permissionless
[45]	Pseudonyms, Random Encryption Period	Permissioned
[46]	Pseudonym update	Permissioned
[47]	K-anonymous	Permissioned
[48]	Digital Certificate	Permissioned
[49]	Dynamic threshold encryption	Permissioned
[50]	K-anonymous	Permissionless
[51]	Zero-Knowledge Proof of Knowledge	Permissioned
[52]	Edge calculation	Permissioned
[53]	Multiple-attribute decision making	Permissioned

4.3. Data Privacy

With the increasing number of vehicles connected to IoV, the data in the vehicle network have risen dramatically. However, the traditional centralized IoV data-management system is subject to a significant increase in the possibility of single point of failure and privacy leakage. For this reason, scholars have actively conducted numerous studies [54–66] aimed at protecting data.

In the IoV, data transmission between vehicles can be easily forged due to the untrustworthy environment. In the meantime, the information transmission may leak the data of vehicles. Yao and Chen et al. [54,55] presented a blockchain-based privacy protection scheme for vehicle trust management. The scheme utilizes a federated blockchain to

build a two-tier in-vehicle network architecture with a federated layer and a vehicle layer. The federated layer consists of those that maintain the federated blockchain and manage operations related to homomorphic computation, pseudonym updates, and consensus processes. The main components of the vehicle layer are vehicles that first submit identity information to a law enforcement agency (LEA) before entering the system for registration and authentication. In addition, the vehicles can operate as message senders, trust assessors, or verifiers based on their system involvement. Homomorphic confidentiality techniques and pseudonym update strategies are used to secure data and identity privacy, respectively. PEPA is then utilized to simulate the system and do performance analysis.

Assisted traffic control, as one of the more mature applications in IoV, has high requirements for the traffic information provided by vehicles. In work [56], a semi-centralized model of attribute-based blockchain in IoV is proposed that balances availability and privacy protection. The group's temporary protocols and messages of the protocol wheel are stored on an attribute-based blockchain, and the contents of the protocols and messages are not accessible to other users or groups. The decision on signal timing modifications is nonetheless visible and verifiable by the traffic signal controller and all users. In addition, the authentication center and monitoring manager pre-verify the true identity of users to track fraudulent individuals and hold them accountable. A significant number of trials demonstrate that the strategy is applicable to real-world situations and is highly practical.

In recent years, the internet combined with IoV has realized intelligent operation and management. However, traditional IoV data management inevitably encounters data security problems due to the centralized approach, and users' privacy is threatened. As a significant subset of the IoT, the IoV has also garnered considerable interest. For this reason, Ma et al. [57] presented a blockchain-based secure data-sharing strategy for IoV (IoVChain) that classifies data as either public or private. To maintain user privacy and security, smart contracts employ homomorphic encryption and zero-knowledge proof processing on sensitive data. The study also uses the PBFT consensus technique to assure consistency, and all IoV data-processing and -consumption procedures are kept in immutable blocks of Merkle trees. The authors would also like access to data sources, such as insurance firms and 4S retailers, to record the entire vehicle process data. The analysis proves that the proposed scheme is feasible in terms of secure data sharing.

With the further popularity and use of VANET, more and more data are generated, and the increase in data poses more significant challenges to security and privacy. Combining blockchain and ciphertext-based attribute encryption (CP-ABE) approaches, Li et al. [58] designed a blockchain-based fine-grained access control mechanism (FADB) for VANET data. FADB realizes distributed storage and fine-grained access to VANET data through CP-ABE encryption technology in the encryption section and distributed IPFS in the storage section, therefore achieving distributed storage and fine-grained access to VANET data. In addition, the research presents a new efficient encryption method, HECP-ABE, which is based on the CP-ABE algorithm and uses blockchain technology to enable distributed encryption and decryption processes. Through simulation experiments and security research, it is demonstrated that FADB can provide data security with minimal performance overhead.

Modern traffic-management systems rely on data for decision making, but the lack of data privacy in traffic networks makes it more difficult to centralize data from connected vehicles to the traffic management system. For this reason, Li et al. [59] proposed a decentralized management architecture. The structure is based on blockchain design, which transforms the traditional centralized traffic data management into decentralized management. The paper also proposes the concept of a gateway, which is mainly responsible for verifying the identity information of vehicles. Finally, latency and throughput are analyzed using Hyperledger Caliper to demonstrate the feasibility of the scheme.

Ma et al. [60] proposed a lightweight blockchain-based framework for IoV that optimizes resource consumption through a layered structure and enabled flexible access control. Different blockchains are used for the inter-vehicular and intra-vehicular networks, and both blockchains are refactored to reduce the pressure of computation and storage. The

paper also designs a new reputation-based consensus method by drawing on the core ideas of the delegated proof of stake (DPoS) consensus algorithm, which employs multi-weight reputation evaluation which can curb network nodes from engaging in internal collaboration. The simulation experiments show that the scheme can guarantee the precision and safety of reputation evaluation in-vehicle networks.

Arkil et al. [61] proposed a protocol for intelligent transportation named "VehicleChain" to provide secure communication between cars and vehicles and infrastructure. The protocol uses blockchain technology and elliptic curve cryptography (ECC) to enhance system security while preserving the original processing burden. Additionally, the protocol protects against a range of security threats. The proposed protocol is theoretically proven to be secure and effective and can be implemented on the road.

Wang et al. [62] presented a unique blockchain-based system for protecting the privacy of vehicle data sharing. The research employs zero-knowledge proof (ZKP) technology to build an anonymous and auditable data exchange mechanism, which not only protects the privacy of cars but also retains the audibility of data for TA. Additionally, to achieve the goal of low communication complexity and high scalability, a multi-partition blockchain protocol is designed in the paper, where consensus nodes handle multiple partitions instead of one compared to other existing partitioning protocols. Experiments show that the proposed framework can improve the security of the system.

Liu et al. [63] presented a novel heterogeneous aggregated signature termed CPHAS, which has the benefit of requiring less time. In addition, they suggest a blockchain-based mechanism for exchanging traffic statistics that protects user privacy. Through simulation, it is shown that the proposed protocol can better protect data anonymity. Zhao et al. [64] developed a privacy-preserving announcement system that ensures the efficacy of announcement forwarding while maintaining privacy. The study also builds a blockchain-based trust management (BBTM) system, in which the authors employ a hybrid PoW and an improved PBFT consensus mechanism to increase verification efficiency. Finally, it is shown through simulation that the BBTM system outperforms other similar methods.

Qureshi et al. [65] proposed a blockchain-based conditional privacy protection and authentication mechanism for IoV networks. The scheme provides conditional privacy for vehicles by allowing vehicle nodes to be anonymous during communication and voting to protect the communication content of the IoV endpoint communication process.

Zhang et al. [66] proposed a blockchain-based asymmetric group key scheme (B-AGKA). This protocol can demand members to authenticate themselves before negotiating group keys, preventing unauthorized individuals' admission. At the same time, the protocol differs from existing group key protocols (GKA) in that the protocol can be verified by a formula right during the computation process without additional rounds to obtain verifiability. The performance analysis shows that the protocol can provide security for group message dissemination among IoV terminals.

In addition to the conventional techniques of access control, zero-knowledge proof and CP-ABE mentioned above, scholars are actively integrating new techniques into data privacy protection [67,68].

By introducing an awareness engine into the traditional IoVs, a cognitive internet of vehicles (CIoV) is formed, which enables some intelligent functions such as vehicle deployment and quota. Regarding content caching, CIoV shines with its ability to sense users' needs and then match them with content. However, users are concerned that their data may be leaked. To solve this problem, Qian et al. [67] added blockchain technology to CIoV and proposed a privacy-aware content caching architecture. Three layers make up the architecture. The first layer is the car, which primarily collects data through sensors and uploads them to the cloud for cognitive engine data processing. Each RSU covers a different area and sends information to the cars around it. The third layer is a cloud-based remote provider and cognitive engine that senses and analyzes the vehicle's needs to deliver content. Finally, a large number of experiments prove that the policy is more effective in content caching.

Accurate and accurate traffic data is essential for traffic management; hence, traffic flow forecasting has become an integral component of IoV. However, existing centralized machine learning approaches for prediction suffer from serious privacy leakage risks. For this reason, Qi et al. [68] proposed a consortium blockchain-based federated learning framework, which enables decentralized and reliable federated learning. In this scheme, participating cars do not send data directly; instead, they train local models and distribute model updates to ensure privacy. Using a consortium blockchain enables a collection of trustworthy nodes to oversee all local model changes in place of the central server. Additionally, differential privacy techniques are used in the scheme to protect privacy. The framework has more significant implications for traffic management, but there is still more room for improvement due to the significant communication overhead of federated learning.

As indicated in Table 3, we compared the literature on data privacy protection. Homomorphic encryption and zero-knowledge proofs are the most used data-protection approaches. Despite the assurance of data privacy, these two kinds of cryptographic techniques are of lower efficiency. In the future, scholars are expected to integrate lightweight privacy-aware techniques technologies that work effectively with blockchain and provide efficient IoV service without data disclosure.

Meanwhile, from all the tables above, we can find that most of the blockchain types used in the schemes are permissioned chains. The biggest problem with permissionless chains is the consensus problem. In the case of Bitcoin, a transaction takes several minutes, which is intolerable for connected car systems that require low latency. Permissioned chains, on the other hand, are more cost-saving than permissionless chains because they are open to a specific group of people, which reduces network stress and thus speeds up transactions and improves the overall performance.

Table 3. Comparison of data privacy.

Literature	Underlying Privacy Protection Mechanism	Blockchain Characteristic
[54,55]	Homomorphic encryption, Pseudonym update	Permissioned
[56]	Ciphertext-policy attribute-based encryption	Permissioned
[57]	Homomorphic Encryption, Zero-Knowledge Proof	Permissioned
[58]	CP-ABE	Permissioned
[59]	Zero-knowledge proof	Permissioned
[60]	Access control	Permissioned
[61]	Elliptic-curve cryptography	Permissioned
[62]	Zero-knowledge proof	Permissioned
[63]	Aggregation signature	Permissioned
[64]	Group signature	Permissioned
[65]	Anonymous Authentication	Permissioned
[66]	Group key	Permissioned
[67]	Deep learning	Permissioned
[68]	Federated learning	Permissioned

5. Research Challenges

By studying the above papers, we find that user privacy and security issues are of top priority in IoV applications. Scholars have relied on blockchain to achieve decentralized privacy protection by combining the latest research results in identity authentication, trust management and privacy protection. However, some issues still need to be solved. We highlight the primary obstacles and probable future research directions below.

1. Many of the above proposed solutions are still based on simulations and simple experiments and rely on limited hardware equipment, which makes it difficult to apply the existing solutions in practice. In addition, it is a question of how to better integrate blockchain technology into the existing infrastructure while considering the cost. To do this, we need to further optimize the hardware and software requirements.

2. Blockchain is effective in decentralization and security, but its system throughput is very limited and throughput is a quantitative indicator of the scalability of blockchain systems, which is one of the difficulties to be overcome by current blockchain technology. For this reason, we need to improve the scalability of blockchain, for example, by improving the read performance of blockchain, using more efficient sharing techniques, designing secure directed acyclic graphs (DAGs), and reducing the storage volume by employing the coding theories. Moreover, there is a need for developing a scalable blockchain-based approach for authentication and access control for new IoV architectures, such as the software-defined vehicular networks.
3. As the number of vehicles increases, data transmission becomes more widespread and the amount of data becomes more massive. It is a great challenge to provide low-latency IoV services in such a large volume. In the future, we have to develop higher speed communication networks to reduce the transmission latency between data and optimize the communication architecture.
4. The one-wayness of cryptographic hashing provides blockchain immutability as its core advantage. With the emergence of quantum computing, the immutability may be compromised. However, it also offers opportunity. In the future years, quantum computing will have widespread application sources [69], for which we can combine quantum computing with new technologies. Additionally, edge computing can be applied in blockchain to enhance data analysis performance, which can be incorporated with anti-quantum security protocols to improve the security of vehicle nodes. Moreover, deep learning and reinforcement learning may be integrated with blockchain technology to enhance system security.

6. Conclusions

As a promising research field, IoV has also attracted much attention for its security and privacy issues. Blockchain can guarantee the completeness and immutability of the IoV data, but it cannot protect data privacy. Therefore, the IoV solutions utilizing blockchain technology must consider using privacy protection schemes to protect user privacy.

This paper reviews proposed solutions that use blockchain to provide different vehicle services while protecting privacy using pseudonym techniques, permission control, ring signature techniques, etc. We categorize and present the literature with three privacy concerns: identity, location, and data privacy. We also sort them according to the blockchain platform and framework they employ. Through classification, it is found that there are relatively mature privacy protection technologies in each specific privacy protection field. In addition, several blockchain-based privacy-preserving solutions for IoV have begun to integrate other new technologies to meet the low latency and low computation requirements of IoV. Finally, we highlight the primary problems and future research directions in this field with which we expect to motivate and inspire more researchers interested in this line of work to conduct further investigations.

Author Contributions: Conceptualization, W.C. and X.C.; methodology, W.C.; validation, W.C., H.W. and X.C.; formal analysis, W.C. and H.W.; investigation, W.C.; data curation, W.C.; writing—original draft preparation, W.C.; writing—review and editing, W.C. and H.W.; visualization, W.C.; supervision, X.C. and J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This project has also received funding from National Natural Science Foundation of China (No. 62202167) and State Key Laboratory of Software Development Environment (No. SKLSDE-2017KF-03).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
2. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. [CrossRef]
3. Tangade, S.S.; Manvi, S.S. A survey on attacks, security and trust management solutions in VANETs. In Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–6. [CrossRef]
4. Garg, T.; Kagalwalla, N.; Churi, P.; Pawar, A.; Deshmukh, S. A survey on security and privacy issues in IoV. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 5409–5419. [CrossRef]
5. Luckshetty, A.; Dontal, S.; Tangade, S.; Manvi, S.S. A survey: Comparative study of applications, attacks, security and privacy in VANETs. In Proceedings of the 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 6–8 April 2016; pp. 1594–1598. [CrossRef]
6. Sağlam, E.T.; Bahtiyar, S. A Survey: Security and Privacy in 5G Vehicular Networks. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 108–112. [CrossRef]
7. Mathew, D.; Roy, H.A. A survey on different privacy-preserving authentication schemes in VANET. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *396*, 012033. [CrossRef]
8. Lu, Z.; Qu, G.; Liu, Z. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 760–776. [CrossRef]
9. Talat, H.; Nomani, T.; Mohsin, M.; Sattar, S. A Survey on Location Privacy Techniques Deployed in Vehicular Networks. In Proceedings of the 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 8–12 January 2019; pp. 604–613. [CrossRef]
10. Sheikh, M.S.; Liang, J.; Wang, W. Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 5129620. [CrossRef]
11. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in internet of vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]
12. Kaltakis, K.; Polyzi, P.; Drosatos, G.; Rantos, K. Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 9792. [CrossRef]
13. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
14. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.T.; Liu, X. Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. *IEEE Access* **2016**, *4*, 5356–5373. [CrossRef]
15. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
16. Mundhe, P.; Verma, S.; Venkatesan, S. A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Comput. Sci. Rev.* **2021**, *41*, 100411. [CrossRef]
17. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System; Decentralized Business Review. 2008. p. 21260. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 16 October 2022).
18. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
19. Buterin. On Public and Private Blockchains. 2015. Available online: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains (accessed on 16 October 2022).
20. Brown, R.G. The corda platform: An introduction. *Retrieved* **2018**, *27*, 2018.
21. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
22. Abassi, R. VANET security and forensics: Challenges and opportunities. *Wiley Interdiscip. Rev. Forensic Sci.* **2019**, *1*, e1324. [CrossRef]
23. Sun, G.; Chang, V.; Ramachandran, M.; Sun, Z.; Li, G.; Yu, H.; Liao, D. Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *J. Netw. Comput. Appl.* **2017**, *89*, 3–13. [CrossRef]
24. Sun, G.; Xie, Y.; Liao, D.; Yu, H.; Chang, V. User-defined privacy location-sharing system in mobile online social networks. *J. Netw. Comput. Appl.* **2017**, *86*, 34–45. [CrossRef]
25. Kalaiarasy, C.; Sreenath, N.; Amuthan, A. Location privacy preservation in VANET using mix zones—A survey. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2019; pp. 1–5.
26. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2018**, *5*, 3701–3709. [CrossRef]
27. Liu, Y.N.; Lv, S.Z.; Xie, M.; Chen, Z.B.; Wang, P. Dynamic anonymous identity authentication (DAIA) scheme for VANET. *Int. J. Commun. Syst.* **2019**, *32*, e3892. [CrossRef]

28. Guehguih, B.; Lu, H. Blockchain-based privacy-preserving authentication and message dissemination scheme for vanet. In Proceedings of the 2019 5th International Conference on Systems, Control and Communications, Wuhan, China, 21–23 December 2019; pp. 16–21.
29. Shi, K.; Zhu, L.; Zhang, C.; Xu, L.; Gao, F. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. *Multimed. Tools Appl.* **2020**, *79*, 8085–8105. [CrossRef]
30. Yang, H.; Li, Y. A Blockchain-Based Anonymous Authentication Scheme for Internet of Vehicles. *Procedia Comput. Sci.* **2022**, *201*, 413–420. [CrossRef]
31. Sharma, R.; Chakraborty, S. BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
32. Moussaoui, D.; Kadri, B.; Feham, M.; Ammar Bensaber, B. A Distributed Blockchain Based PKI (BCPKI) architecture to enhance privacy in VANET. In Proceedings of the 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH), Boumerdes, Algeria, 9–10 February 2021; pp. 75–79. [CrossRef]
33. Bao, S.; Lei, A.; Cruickshank, H.; Sun, Z.; Asuquo, P.; Hathal, W. A Pseudonym Certificate Management Scheme Based on Blockchain for Internet of Vehicles. In Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019; pp. 28–35. [CrossRef]
34. Akhter, A.S.; Ahmed, M.; Shah, A.S.; Anwar, A.; Zengin, A. A secured privacy-preserving multi-level blockchain framework for cluster based VANET. *Sustainability* **2021**, *13*, 400. [CrossRef]
35. Mei, Q.; Xiong, H.; Zhao, Y.; Yeh, K.H. Toward Blockchain-Enabled IoV with Edge Computing: Efficient and Privacy-Preserving Vehicular Communication and Dynamic Updating. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Japan, 30 January–2 February 2021; pp. 1–8. [CrossRef]
36. Akhter, A.S.; Ahmed, M.; Shah, A.S.; Anwar, A.; Kayes, A.; Zengin, A. A blockchain-based authentication protocol for cooperative vehicular ad hoc network. *Sensors* **2021**, *21*, 1273. [CrossRef] [PubMed]
37. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220. [CrossRef]
38. Lee, J.; Lee, J.; Park, H. A Privacy Preserving Blockchain-based Reward Solution for Vehicular Networks. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020; pp. 1–4. [CrossRef]
39. George, S.A.; Jaekel, A.; Saini, I. Secure Identity Management Framework for Vehicular Ad-hoc Network using Blockchain. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–6. [CrossRef]
40. Shrivastava, A.L.; Dwivedi, R.K. A Secure Design of the Smart Vehicular IoT System using Blockchain Technology. In Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 23–25 March 2022; pp. 616–620.
41. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. *IEEE Access* **2019**, *7*, 117716–117726. [CrossRef]
42. Zhang, J.; Yang, F.; Ma, Z.; Wang, Z.; Liu, X.; Ma, J. A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 2299–2313. [CrossRef]
43. Su, T.; Shao, S.; Guo, S.; Lei, M. Blockchain-based internet of vehicles privacy protection system. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8870438. [CrossRef]
44. Li, B.; Liang, R.; Zhu, D.; Chen, W.; Lin, Q. Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3765–3775. [CrossRef]
45. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3198–3212. [CrossRef]
46. Liang, R.; Li, B.; Song, X. Blockchain-based privacy preserving trust management model in VANET. In Proceedings of the International Conference on Advanced Data Mining and Applications, Foshan, China, 12–14 November 2020; pp. 465–479.
47. Li, H.; Pei, L.; Liao, D.; Sun, G.; Xu, D. Blockchain meets VANET: An architecture for identity and location privacy protection in VANET. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1178–1193. [CrossRef]
48. Li, B.; Liang, R.; Zhou, W.; Yin, H.; Gao, H.; Cai, K. LBS meets blockchain: An efficient method with security preserving trust in SAGIN. *IEEE Internet Things J.* **2021**, *9*, 5932–5942. [CrossRef]
49. Feng, J.; Wang, Y.; Wang, J.; Ren, F. Blockchain-Based Data Management and Edge-Assisted Trusted Cloaking Area Construction for Location Privacy Protection in Vehicular Networks. *IEEE Internet Things J.* **2021**, *8*, 2087–2101. [CrossRef]
50. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5760–5772. [CrossRef]
51. Li, M.; Weng, J.; Yang, A.; Liu, J.N.; Lin, X. Toward blockchain-based fair and anonymous ad dissemination in vehicular networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11248–11259. [CrossRef]
52. Li, H.; Li, J.; Zhao, H.; He, S.; Hu, T. Blockchain-Based Incentive Mechanism for Spectrum Sharing in IoV. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6807257. [CrossRef]
53. Wang, H.; Wang, C.; Shen, Z.; Liu, K.; Liu, P.; Lin, D. A MADM Location Privacy Protection Method Based on Blockchain. *IEEE Access* **2021**, *9*, 27802–27812. [CrossRef]

54. Chen, X.; Ding, J.; Lu, Z. A Decentralized Trust Management System for Intelligent Transportation Environments. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 558–571. [CrossRef]
55. Yao, Y.; Chen, W.; Chen, X.; Ding, J.; Pan, S. A Blockchain-based Privacy Preserving Scheme for Vehicular Trust Management Systems. In Proceedings of the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), Zhenjiang, China, 27–29 November 2020; pp. 1–5. [CrossRef]
56. Cheng, L.; Liu, J.; Xu, G.; Zhang, Z.; Wang, H.; Dai, H.N.; Wu, Y.; Wang, W. SCTSC: A Semicentralized Traffic Signal Control Mode With Attribute-Based Blockchain in IoVs. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1373–1385. [CrossRef]
57. Ma, Z.; Wang, L.; Zhao, W. Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network. *IEEE Sens. J.* **2021**, *21*, 25472–25479. [CrossRef]
58. Li, H.; Pei, L.; Liao, D.; Chen, S.; Zhang, M.; Xu, D. FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain. *IEEE Access* **2020**, *8*, 85190–85203. [CrossRef]
59. Li, W.; Guo, H.; Nejad, M.; Shen, C.C. Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. *IEEE Access* **2020**, *8*, 181733–181743. [CrossRef]
60. Ma, X.; Ge, C.; Liu, Z. Blockchain-enabled privacy-preserving Internet of vehicles: decentralized and reputation-based network architecture. In Proceedings of the International Conference on Network and System Security, Sapporo, Japan, 15–18 December 2019; pp. 336–351.
61. Patel, A.; Shah, N.; Limbasiya, T.; Das, D. Vehiclechain: Blockchain-based vehicular data transmission scheme for smart city. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 661–667.
62. Wang, J.; Huang, J.; Kong, L.; Chen, G.; Zhou, D.; Rodrigues, J.J.C. A Privacy-Preserving Vehicular Data Sharing Framework atop Multi-Sharding Blockchain. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6. [CrossRef]
63. Liu, J.; Zhang, G.; Sun, R.; Du, X.; Guizani, M. A Blockchain-based Conditional Privacy-Preserving Traffic Data Sharing in Cloud. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
64. Zhao, Y.; Wang, Y.; Wang, P.; Yu, H. PBTM: A Privacy-Preserving Announcement Protocol With Blockchain-Based Trust Management for IoV. *IEEE Syst. J.* **2022**, *16*, 3422–3432. [CrossRef]
65. Qureshi, K.N.; Shahzad, L.; Abdelmaboud, A.; Elfadil Eisa, T.A.; Alamri, B.; Javed, I.T.; Al-Dhaqm, A.; Crespi, N. A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles. *Appl. Sci.* **2022**, *12*, 476. [CrossRef]
66. Zhang, Q.; Li, Y.; Wang, R.; Li, J.; Gan, Y.; Zhang, Y.; Yu, X. Blockchain-based asymmetric group key agreement protocol for internet of vehicles. *Comput. Electr. Eng.* **2020**, *86*, 106713. [CrossRef]
67. 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]
68. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Gener. Comput. Syst.* **2021**, *117*, 328–337. [CrossRef]
69. Hassija, V.; Chamola, V.; Goyal, A.; Kanhere, S.S.; Guizani, N. Forthcoming applications of quantum computing: Peeking into the future. *IET Quantum Commun.* **2020**, *1*, 35–41. [CrossRef]