



Blockchain-Enabled Internet of Vehicles Applications

Junting Gao ¹, Chunrong Peng ², Tsutomu Yoshinaga ¹, Guorong Han ³, Siri Guleng ⁴ and Celimuge Wu ^{1,*}

¹ Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo 182-8585, Japan; k2141014@edu.cc.uec.ac.jp (J.G.)

² Inner Mongolia University of Finance and Economics Library, Inner Mongolia University of Finance and Economics, Hohhot 010051, China; pengchunrong1978@gmail.com

³ B & S Tech Co., Ltd., Arakawa-ku, Tokyo 116-0014, Japan

⁴ School of Computer Science and Information Engineering, Hohhot Minzu College, Hohhot 010051, China

* Correspondence: celimuge@uec.ac.jp

Abstract: Internet of Vehicles (IoV) is a network that connects vehicles and everything. IoV shares traffic data by connecting vehicles with the surrounding environment, which brings huge potential to people's life. However, a large number of connections and data sharing will seriously consume vehicle resources during the interaction. In addition, how to build a safe and reliable connection to ensure vehicle safety is also an issue to consider. To solve the above problems, researchers introduce blockchains into IoV to build a safe and reliable vehicle network relying on the distributed account structure, immutable, transparent and security features of blockchains. We have investigated the application of blockchains in IoV in recent years, and have summarized and compared these studies according to their purposes. On this basis, we also point out the future trends and opportunities.

Keywords: ITS; IoV; blockchain; consensus; smart contract

1. Introduction

With the development of the Internet of Things (IoT) and communication technology, the era of interconnection of everything has arrived. IoT refers to the connection of a terminal with an intelligent product such as an internal facility (e.g., sensor, mobile device, home intelligence) and an external facility (e.g., a person carrying a wireless terminal, a vehicle, etc.) either wireless or wired [1].

As an application of IoT, IoV has become a proven technology with the development of Smart Vehicle [2–4], Artificial Intelligence (AI) [5,6], Cloud Computing [7,8], 5th generation mobile networks (5G), 6th generation mobile networks (6G) communication technology [9].

1.1. Internet of Vehicles

IoV not only connects Vehicle to Vehicle (V2V), but also connects Vehicle to Pedestrian (V2P), Vehicle to Road (V2R), Vehicle to Infrastructure (V2I), Vehicle to Network (V2N), and Vehicle to Cloud (V2C) to a network seamlessly and efficiently, on which data sharing is based. So IoV can also be called V2X (X stands for everything) [10].

With the connection of IoV, the vehicle can realize remote detection, intelligent control, assisted driving and even automatic driving, which can improve the traffic efficiency. It can also reduce accidents by monitoring the distance between vehicles and reduce traffic congestion by autonomous navigation [11]. At the same time, IoV can also achieve the purpose of saving resources, green travel, economical and environmentally friendly. IoV perfectly intelligently interacts with vehicle and makes full use of resources to achieve effective Human–Vehicle–Road collaboration.

In reality, however, road conditions are complex and variable. Connections between vehicles often require short communication time, stability, high frequency, large bandwidth, and high mobility [12]. At the same time, high-speed moving vehicles make it more difficult



Citation: Gao, J.; Peng, C.; Yoshinaga, T.; Han, G.; Guleng, S.; Wu, C. Blockchain-Enabled Internet of Vehicles Applications. *Electronics* **2023**, *12*, 1335. <https://doi.org/10.3390/electronics12061335>

Academic Editor: Nikolay Hinov

Received: 6 February 2023

Revised: 28 February 2023

Accepted: 8 March 2023

Published: 11 March 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

to achieve IoV. How to establish a dynamic, fast and efficient connection between high-speed moving vehicles and transfer data safely is an urgent problem for IoV. Due to the existing technical challenges such as communication security, network complexity and device heterogeneity, IoV needs a decentralized, distributed, low latency, data security and heterogeneous network construction to enhance the implementation of IoV. Researchers propose to solve the above problems safely and efficiently by introducing blockchains into IoV [13–16] based on the characteristics of the blockchain, such as decentralization, unalterable, high transparency and high heterogeneousness [17–20].

1.2. Blockchain

Blockchain originated from a paper on Bitcoin by Satoshi Nakamoto [21]. The blockchain links the blocks by chain in chronological order to become a decentralized and distributed ledger [22]. Its main purpose is to maintain all Bitcoin transactions for the ledger and prevent the double-spending [22] of currency. However, as a blockchain in the 1.0 era, there are many shortcomings in the blockchain at this time, such as lack of Turing-completeness, value-blindness, lack of state, blockchain-blindness and so on.

To solve the problem of blockchain 1.0, blockchain 2.0 adds smart contracts [23]. The typical application of 2.0 is Ethereum [24]. Vitalik Buterin first proposed the concept of Ethereum [25], in “A Next-Generation Cryptocurrency and Decentralized Application” in 2013. Unlike Bitcoin, Ethereum introduces smart contracts, so the blockchain can be customized according to different needs [26,27]. This feature enables the blockchain to establish trusted connections between untrusted entities. At the same time, the tolerance of blockchain to heterogeneous devices has also been improved. Once deployed, smart contracts cannot be changed, which makes the blockchain difficult to change and cannot be tampered with.

In addition, the core technologies of blockchain include consensus, modern cryptography and peer to peer (P2P) distributed network [28]. Consensus protocol is the process of making all blocks reach consensus in a way without central participation. Consensus brings features such as unity, immutability, transparency, and attack traceability to the blockchain by deciding who has the right to write the block. In modern cryptography, hash algorithms are used to ensure node privacy and transaction data security [29], digital signatures and other methods are used to verify the legitimacy of the identity. Finally, because P2P distributed network in blockchain [30], the transaction and maintenance costs of the blockchain, delay of IoV and probability of single point of failure are reduced.

1.3. Advantages of Blockchain Introducing IoV

According to the above advantages of blockchain, introducing blockchain into IoV can improve the performance of IoV in four aspects.

1. To store the large amount of data transmitted by smart vehicles in IoV, traditional method upload all data to the cloud, which requires building cloud servers with large storage. Since the blockchain is a distributed storage structure, using the blockchain to store IoV data will reduce the storage pressure on the cloud.
2. The correctness of information transmission between vehicles also needs to be considered. Vehicles need to grasp the correct information of the surrounding environment. Once the information is wrong, serious traffic accidents will occur. Therefore, due to the distributed structure and unalterable of the blockchain, the use of the blockchain can ensure the safety of the vehicle information transmission process.
3. The road conditions are complex and there are many heterogeneous devices, which increases the difficulty of IoV construction. Blockchain is a highly heterogeneous ledger structure, which can establish trusted connections between untrusted entities, reducing the time for establishing connections between nodes.

4. For the issues of vehicle privacy and attacks, the distributed storage structure of blockchain can also prevent problems such as single point of failure. In addition, the blockchain also uses cryptography principles to ensure the privacy of nodes and provide a higher ability to resist attacks.

Because of the above advantages of blockchain, many researchers try to introduce blockchain into IoV. At present, there are many articles on the introduction of blockchain into IoV. It is difficult for researchers to classify and summarize the articles and select the relevant research. Therefore, it is meaningful to summarize and classify these articles so that researchers can quickly understand this field. At present, most of such review articles focus on how to integrate blockchain into IoV, without considering the specific role and purpose of blockchain in IoV. Therefore, this article summarizes the opportunities that blockchain brings to the IoV field, analyzes the advantages of introducing blockchain into IoV, and summarizes the research results of the last 3–5 years. The research contributions of this paper are as follows:

1. Before introducing the current research results, this article explains the basic knowledge about IoV and blockchain. For researchers who are new to this field, they can quickly understand blockchain and IoV, so this article is more meaningful to read.
2. We highlight the current performance, trust and security, and privacy protection challenges of IoV. According to the characteristics of the blockchain, the motivation for combining the blockchain with IoV is proposed to show how the blockchain can deal with the above challenges.
3. Different from the classification methods of other articles, we focus on the latest application results of blockchain in IoV in the past 3–5 years. After in-depth investigation, it is divided into 5 categories according to different application purposes: Data Management, Resource Management, Trust Management, Safety Management and Privacy Management. Therefore, the train of thought of this paper is relatively novel and the consideration is more comprehensive. This classification method is easier for researchers to understand and provides clearer research ideas.
4. On the basis of summarizing the current research results, we also proposed some open issues of introducing blockchain into iov, and proposed future research directions for building blockchain-based IoV, providing researchers with a wider range of choices direction.

The paper is structured as follows: In the second part, the background and technology of IoV are briefly introduced, and at the same time, some technical solutions of blockchain are introduced. In the third part, the current problems and challenges of IoV are discussed. In response to these challenges, the necessity of blockchain empowering IoV is emphasized. In Section 4, we survey in depth the recent work on the application of blockchain in IoV. Section 5 indicates some existing problems and future research directions in the combination of blockchain and IoV. The structure of this paper is shown in Figure 1. The abbreviations are shown in the Abbreviations Part.

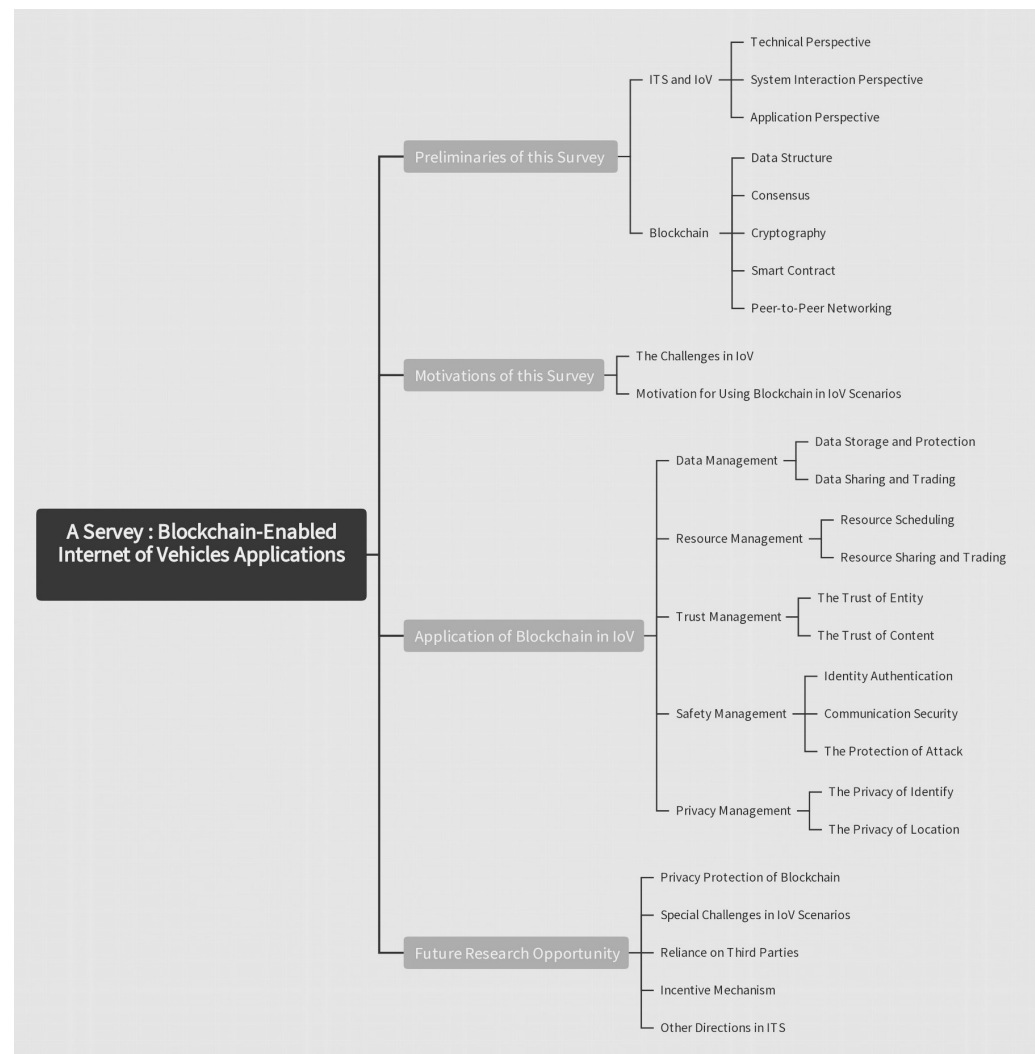


Figure 1. Structure of This Paper.

2. Preliminaries of this Survey

In this section, we briefly introduce the Preliminaries of this survey. Firstly, the basic concepts of ITS and IoV are introduced. Then three aspects of IoV are introduced: technology, system and application. Finally, five key technologies of the blockchain are introduced: data structure, consensus, cryptography, smart contract, and peer-to-peer networking.

2.1. Intelligent Transport System (ITS) and IoV

ITS is a new type of intelligent transportation system based on communication, electronics and other technologies, which connects vehicles (unmanned aerial vehicle (UAV), automobile, railway, aircraft, etc.) to share information [31]. ITS can build high-speed information delivery networks, which make transportation equipment interactive and service-oriented. ITS can also improve traffic efficiency and enhance the QoS in the transportation process. As an important part of ITS, IoV is a network that connects cars, people and the surrounding environment [32]. In recently, smart car and auto-driving technology promote vehicles and everything can be connected in a variety of ways. Vehicles can expand people's perception by collecting environmental information around them. They can also use some intelligent algorithms to make judgments on the environment to assist people's driving behavior and cooperate with their surroundings, so as to optimize the entire transportation system. Therefore, IoV is a highly interactive and dynamically evolving complex system between vehicle, human and environment [33]. During the inter-

action, enormous data is transferred. Therefore, the network is required to have sufficient information processing and transmission capabilities.

IoV is utilized in many aspects, such as Autopilot [34]. Intelligent driving is through vehicle-road coordination. The vehicle collects environmental data through the RSU and it will be transmitted to the vehicle's central processing unit (CPU). The CPU makes judgments to make auxiliary actions for the driver's posture behavior. Secondly, IoV is also applied in emergency rescue [35]. When a major accident occurs to the vehicle, the intelligent system on the vehicle can quickly send a distress signal to nearby rescuers, and transmit the vehicle location to the rescuers through wireless or other means, which can make rescue rapidly. Moreover, the accident information is uploaded to other vehicles, so that other vehicles can avoid danger, which can avoid causing traffic jams or more serious traffic accidents. In addition, IoV also has important applications in traffic management [36]. Vehicles will collect current road conditions and send them to managers to facilitate traffic management and updates. Finally, in-car entertainment is also an application of IoV [37]. IoV can customize entertainment services to make drivers and passengers more comfortable in the car and reduce the incidence of traffic accidents.

IoV is generally divided into in-vehicle Network and inter-vehicle network. As shown in Figure 2, the in-vehicle network refers to various components in the vehicle, such as cameras, user smart devices, bluetooth, etc., which transmit status data to the "central nerve" of the vehicle by installing sensors to achieve monitoring and control purposes. Sensor technology is an important technology in the car network. If there is only an in-vehicle network, the data of the vehicle will become an island of data. At this time, the data of the vehicle needs to be transmitted to the external network, so that the cloud, RSU, and other vehicles can obtain the status information of the vehicle, which is called Inter-vehicle network. Figure 3 is Inter-vehicle network. The technologies of IoV are mainly classified as follows:

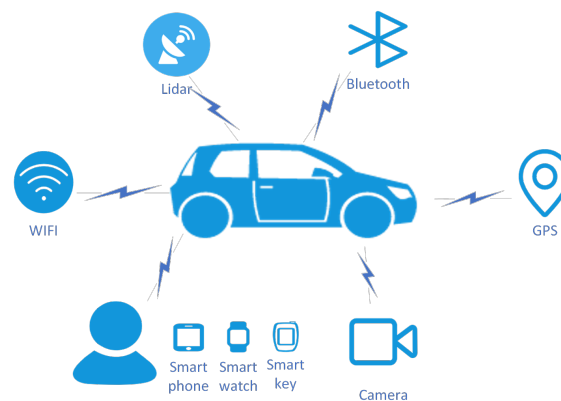


Figure 2. In vehicle network.

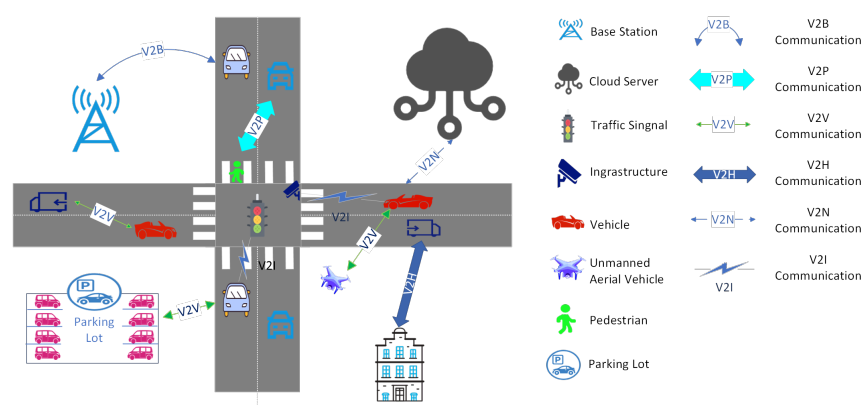


Figure 3. Inter vehicle network.

2.1.1. Technical Perspective

A. Positioning and location Awareness Technology

The most widely used positioning technology in IoV is the Global Navigation Satellite System (GNSS) [38], which is composed of space part (constellation), ground control part (ground monitoring system) and signal receiver (user equipment). It can use satellites to precisely locate vehicles. Three equations can be drawn by using three satellites based on the distance from the satellite to the receiver to calculate the vehicle position. Satellite positioning is affected by orbit, atmosphere, GPS, Glonass, Galileo and Beidou navigation systems belong to global navigation systems. WAAS, EGNOS, MSAS belong to enhancement systems.

In addition, the combination of sensor and high-precision map and the addition of perception technology are called sensor and high-precision map matching positioning technology [39]. This technology can collect the surrounding environment influence through the camera system and extract features for analysis. However, the camera system is vulnerable to weather, angle, distance and other restrictions, resulting in poor effect. In addition, the distance can also be measured through lidar [40] and the time reflected by the laser signal. Although the target position is determined by reflection angle, it is still affected by weather conditions. In addition, the millimeter wave radar is also used for position sensing [41]. The millimeter wave radar can stably and accurately measure the distance and speed of the target. The technology has good robustness, and is not affected by bad weather conditions, and can measure a long distance. However, the technology cannot distinguish multiple targets. Finally, high-precision map sensors can also be used to locate vehicles [42]. After the sensors detect the environmental characteristics, they pre collect and draw high-precision maps to achieve vehicle positioning.

The cellular network positioning and synchronization technology has large bandwidth and high resolution. It has good effect when the measurement distance is less than 200 m. Small pulse signal has strong penetrability and can be free from the influence of complex environment. It has good effect in water, cement and other media [43].

B. Wireless Communication Technology

If the vehicle does not have the communication function, it will not be able to transmit data to the outside world, and also cannot receive the data transmitted from the outside. This means that the vehicle will become a data island. Wireless communication technology can solve the communication problem well. Radio Frequency IDentification (RFID), Wireless-Fidelity (Wi-Fi), etc., are short-range mobile communication technologies, while 5G is a form of long-distance communication technology.

RFID [44] tracks and identifies wireless signals through radio frequency to obtain data. For example, if RFID is placed on the vehicle, vehicle information can be obtained. It can also provide location services for vehicles. In case of vehicle failure, RFID, GPS and other technologies can be combined to quickly obtain accurate vehicle information, so as to quickly rescue. This technology needs to deploy equipment, which is suitable for use with other technologies for precise location awareness. RFID is usually used for the sensing layer of IoV.

ZigBee is a wireless internet protocol [45]. It can be embedded in the equipment, with low complexity, low cost, close distance, low speed and other characteristics, and is mainly used in the automotive automation field. However, when there are more input nodes, multi hop will have higher delay.

As an efficient short distance technology, Dedicated Short-Range Communication (DSRC) [46] connects vehicles and roads and conducts two-way transmission on this basis. The effective range of this protocol is about 3–30 m. It can transmit image, voice and other information. DSRC has high security, fast transmission speed and is not vulnerable to interference. However, DSRC has a small coverage and is suitable for identification management in small areas.

Wi-Fi technology, based on IEEE802.11 protocol, is a standard in wireless local area network (WLAN) [47]. It realizes wireless high-speed connection in the coverage area, with wide range, strong anti-interference, strong signal, fast speed, etc.

Cellular-V2X (C-V2X) [48] is a technology based on cellular network. C-V2X can directly conduct wireless communication between vehicles. This technology includes LTE-V2X and 5G-V2X technologies. LTE-V2X is mainly responsible for traffic safety management, and 5G-V2X is mainly responsible for automatic driving business. C-V2X has two types of interfaces: cellular network vehicle terminal communication interface and short distance direct communication interface. Unlike DSRC, C-V2X features wide coverage, high capacity, strong anti-interference, and does not need to redeploy infrastructure.

Ultrawideband (UWB) [49] is a form of short-distance, low-power and high-speed data transmission technology. UWB has the advantages of high density and speed, low complexity, high security, accurate positioning, and strong anti-interference.

5G [10] communication technology is a new generation global wireless standard. 5G has millimeter wave length, high reliability, low delay, large bandwidth and other characteristics, and can be widely used in IoV. The development of mobile network technology is as follows: 1G can realize analog voice communication, and can only dial a telephone to transmit voice signals; 2G realizes digital voice communication and SMS functions; 3G can transmit multimedia content such as pictures; 4G enables high-speed Internet access, which can quickly transmit video content. In summary, 1–4G focus on the communication between people, while 5G makes it possible to connect people with things and truly realize the interconnection of everything.

2.1.2. System Interaction Perspective

V2V refers to information exchange and communication between vehicles. V2P can enable the vehicle to communicate with the human terminal, which can judge the position of pedestrians and other information to ensure vehicle driving safety. V2N refers to the combination of vehicle and network, which can upload vehicle information to the network and obtain information transmitted by other vehicles at the same time. V2I communicates and shares data between vehicles and roadside infrastructure to determine real-time road traffic conditions.

2.1.3. Application Perspective

A. Monitoring application system

The monitoring system [50] is mainly responsible for collecting vehicle driving conditions, including speed, location and other information. The vehicle will be monitored in real time. Vehicle information is sent to the network for vehicle management. The monitoring system needs to have real-time data collection and transmission functions, and use communication technology to upload information quickly. Besides, the monitoring system should store and analyze data. The data generated during vehicle driving is huge. If all the data are uploaded to the network, it is easy to cause network paralysis. Therefore, the system should have storage and analysis abilities, and only part of the information can be uploaded. Finally, the system should have the ability to display data to the monitoring personnel in real time.

B. Traffic safety system

The driving safety system needs to pay attention to vehicle safety, driving behavior evaluation, cloud data processing and feedback and other issues. The first thing to do is to evaluate the safety of the vehicle. Checking whether the vehicle has faults is the guarantee of safe driving. The second is to evaluate the driver's health and driving behavior. The system should evaluate the driver safety based on judging whether the driver is drunk driving, tired driving, or exhibiting any different driving habit. Finally, the cloud needs to process the data correctly and efficiently and judge whether it meets the current vehicle environment requirements.

C. Dynamic road condition analysis system

Urban road conditions are congested, complex and fast changing. Therefore, the road condition analysis system is required to dynamically analyze the current road conditions and give reasonable suggestions [51]. The vehicle will collect the road condition information first, and upload the surrounding information to the cloud after simple analysis. The cloud combines the information sent by all current vehicles and integrates it into effective information for vehicles and sends it back to vehicles. The vehicle will judge the current road conditions according to the information sent by the cloud, so that the driver can make correct choices.

D. Traffic incident handling system

Road traffic safety is particularly important in IoV [52]. There are two types of traffic incident handling. The first is that when a traffic accident occurs to its own vehicle, the system should quickly send a distress signal, accurately locate it, and send the location information and important accident information to the rescuers close to it, which can speed up the rescue. The second is that when the front vehicle has an emergency traffic accident, the rear vehicle should quickly detect the accident in front and remind the driver. If necessary, it can independently implement emergency braking or diversion to avoid causing a larger traffic accident. At the same time, the rear vehicle should send a distress signal at the same time to increase the rescue ability of the accident vehicle.

As a branch of IoT, IoV is similar to IoT architecture. As shown in the figure, it can be divided into perception layer, transport layer and application layer. Perception layer mainly obtains traffic information of vehicle location, vehicle to vehicle, vehicle to person and other locations and road conditions through sensors, positioning technology, RFID, real-time perception system and other systems. As the relay between the sensing layer and the application layer, the transport layer is responsible for integrating and transmitting the sensing layer data to the application layer. In addition, it also needs to develop network architecture and protocols to coordinate heterogeneous network communication. At the same time, the transport layer should also make full use of network resources by using cloud computing to provide service support for the application layer. Based on the existing network system and protocol, the application layer needs to have strong scalability to realize the embedding of future functions. Vehicles need the application layer to provide safety control, fault warning, traffic management and other functions. On this basis, entertainment services such as broadcasting and subscription should also be provided for vehicles.

The same as IoT, in addition to the architecture, there are two capabilities: security and management. IoV communication needs to be secure. Identity recognition is carried out through key management and other technologies to ensure the legitimacy of connected vehicles. In addition, during the transmission process, IoV needs to ensure the security of the transmission content, the integrity and correctness of the transmission content. At the same time, malicious attacks on vehicles need to be avoided to ensure real-time synchronization of received information with current traffic conditions. Management capability refers to the management of vehicles and roads in the network, and the realization of fast switching between different vehicles, vehicles and infrastructure. At present, the commonly used management system is Quality of Service (QoS), which provides different service priorities according to the conditions of vehicles.

2.2. Blockchain

Blockchain is a distributed ledger technology (DLT). It was first used in Bitcoin and consists of blocks and chains. The block stores information such as transactions. They are connected into chains in chronological order. New blocks are constantly added to the chain. Blockchain is maintained by all peers. When a peer fails, another peer can be used normally, which can effectively avoid overall failure. Besides, the blockchain establishes

trusted connections on entities that do not trust each other. Therefore, trusted transactions can also be executed when the entity does not trust.

The current blockchain is divided into following three categories according to the degree of openness.

Public blockchain [53]: The public blockchain is highly open and transparent. Everyone or organization can join and exit without permission requirements. Each node in a public chain can participate in consensus. The public chain is not controlled by any organization and is completely decentralized. Bitcoin is a typical application of the public chain. Everyone can participate in the Bitcoin system for verification and use.

Private blockchain [54]: Private blockchain is also named internal chain. It is the least open, and only a few nodes have write and modify permissions. Private blockchain is suitable for large companies to create their own blockchain for management, audit and other operations.

Hybrid blockchain [55]: the hybrid blockchain is between the public blockchain and the private chain. Trust organizations form alliances and the trusted organization will be granted permissions. There is full trust among the federations, so it is fast to verify and low in cost. The hybrid blockchain does not fully disclose all information as the public chain does, nor does it have complete privacy as the private blockchain does. The nodes in the alliance chain do not fully disclose information. It is only visible to organizations that form alliances. The hybrid blockchain not only shares data among alliance members, but also hides information from non alliance members, which fully protects data privacy. At the same time, uninterested nodes do not need to store irrelevant data, which greatly reduces the transaction and maintenance costs of the blockchain.

Due to the characteristics of decentralization, eliminating cloud dependence, traceable attacks, privacy protection, high stability, openness and transparency, P2P direct connection and heterogeneity, blockchain is applied in many industries, such as charity, medicine, stock market, identity recognition, insurance industry, IoT industry, etc.

Blockchain usually has five key technologies: data structure, consensus, cryptography, smart contract and point-to-point. Next, we will briefly explain these five key technologies.

2.2.1. Data Structure

Blockchain is a chained storage structure composed of blocks [56]. Block stores data elements, which are divided into block headers and block bodies. The block header is mainly composed of time stamp, version number and other identification information. The block header of the traditional blockchain generally includes the following four parts: (1) The hash value of the block. Hash is a one-way encryption algorithm, which is irreversible and tamper proof; (2) Previous Block Hash (PreHash); (3) Difficulty target, nonce, timestamp and other information. Mining difficulty adjusts mining time according to network computing power. Random number is a counter of workload proof. The timestamp records the generation time of this block; (4) Merkle Tree. Merkle Tree is the unique value obtained by calculating the hash market value of all transactions in the block level by level in pairs. Any change in the hash value will change the final result. Therefore, the finality and uniqueness of Merkle Tree are usually used to judge whether the transaction data have been tampered with.

Block body is the main part, which stores transaction data and hash list of transactions. The schematic diagram of blockchain storage is shown in Figure 4.

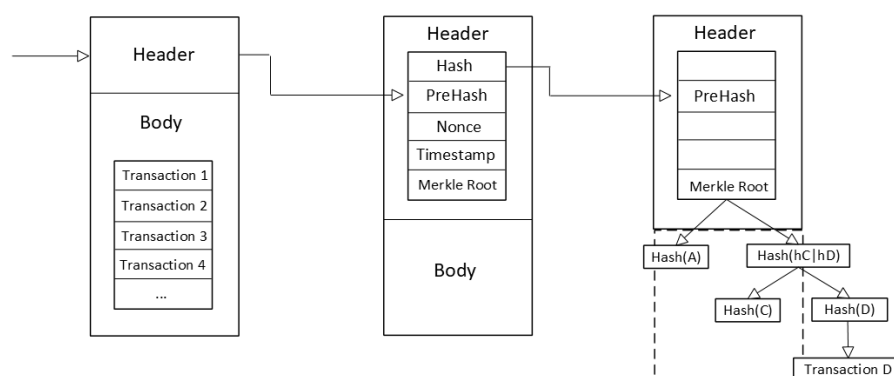


Figure 4. blockchain storage.

2.2.2. Consensus

1. Pow [57]: Pow reached a consensus by measuring computer workload. It is mainly completed by continuously adjusting the random number to calculate the hash value that meets the conditions. In short, the higher the probability of obtaining bookkeeping rights is, the stronger the ability of calculation and the faster the speed. However, this method consumes a lot of resources, and when the computing power of malicious nodes exceeds 51% of the whole system, it can attack the network. The most typical application of Pow is Bitcoin.
2. Pos [58]: Pos is also completed by calculating the hash value that meets the conditions. Different from Pow, the equity proof mechanism uses the time and quantity of currency held by node to judge the equity. The target values calculated by users with different equity sizes are different. The larger the equity, the simpler the calculation, and the easier to obtain the bookkeeping right. This method will damage your own interests if you launch 51% attacks, so it can effectively prevent 51% attacks. However, if a node has too much power, the monopoly of accounting rights will occur, which may lead to a crisis of trust.
3. Delegated Proof of Stake (Dpos) [59]: Dpos votes to select a certain number of representatives through the node holding currency to reach a consensus. The more currencies held by node, the greater the proportion of votes. Representatives elected by voting can take turns to keep accounts, and those who do not comply with the rules will be removed by voting. A new representative shall be elected by a new vote after the end of a term of office.
4. Proof of Capacity (Space)/Proof of Time [60]: Proof of Capacity is an improvement of Pow. Unlike Pow, proof of capacity requires drawing. Drawing refers to storing the pre calculated hash value on its hard disk drive and other memory units before mining, which makes capacity proving faster than Pow and can save a lot of energy.
5. Unique Node List (UNL) [61]: UNL is used in Ripple, Stellar and other blockchains. UNL allows some node to sign transactions, and all nodes can verify the newly written blocks. The UNL is similar to the CA in that it recognizes the uniqueness of node. The possibility of Sybil attack is reduced due to different entity operations. However, UNL makes the blockchain more centralized than other algorithms.
6. Proof of Elapsed Time [62]: Proof of Elapsed Time is used in blockchains such as HyperledgerSawtooth. This method provides a timer for the node at random, and the first end of the timer can be written to the next node. This method can solve the problem of randomly selecting leadership nodes in the PBFT. However, this method cannot determine the uniqueness of the node timer, and cannot determine whether there are malicious users pretending to be multiple nodes in order to improve the probability of selection.
7. Proof of Authority (PoA) [63]: PoA is similar to Pos, but the difference is that Pos judges by currency and PoA by reputation. This method is more suitable for private

chain due to its rapidity and scalability. However, this mechanism has too few verifiers, which will make it easier for malicious node to implement freezing and other attacks.

8. Directed Acyclic Graph (DAG) [64]: DAG is a data structure. Blocks are connected to many previous blocks, and users need to verify the two previous transactions. Although DAG can reduce delay and transaction costs, it cannot be expanded and is easy to be attacked.

2.2.3. Cryptography

In the blockchain system, the most important thing is encryption to ensure the security, privacy and anonymity of the system [65]. Hash function is a very common method in cryptography. It can quickly convert a value of any length to a hash value of a fixed length, and the process is irreversible. It is difficult to reverse the source plaintext from the hash value, and changing any number of the source input value will change the result, so it is almost impossible to have the same hash finally calculated from two pieces of content with different plaintext. These features realize the tamper proof function of the blockchain, provide security for the blockchain, and also provide a basis for other encryption methods. The types of Hash currently include: (1) MD family: MD4, MD5. (2) SHA family: SHA1, SH2 (SHA-224, SHA-225, etc.), SH3, etc. In Bitcoin, SHA256 is used to construct the blockchain, and RIPEMD160 is used to generate Bitcoin addresses.

The core of cryptography is encryption algorithm. The process of encryption is to encrypt the key through the algorithm, and then encrypt the plaintext to get the ciphertext. The process of decryption is to decrypt keys through the decryption algorithm, and then decrypt the ciphertext to get the plaintext. Encryption algorithms are mainly divided into symmetric encryption and asymmetric encryption. The way to judge whether the encryption method is symmetric is to see whether the keys used in the encryption and decryption process are consistent. If consistent, it is symmetric encryption, otherwise it is asymmetric encryption. In some cases, the two encryption methods can be combined to obtain a hybrid encryption algorithm.

The current security technologies are divided into the following categories:

1. Hash-based Message Authentication Code and Digital Signature [66]: This method solves the tamper proof and authentication problems by encrypting the message digest. The message verification code is based on symmetric encryption to ensure the integrity of the message. The digital signature uses asymmetric encryption, which can not only ensure the integrity of the content, but also trace back to the source, that is, Non Representation.
2. Digital Certificate [67]: Public key distribution is an important part of asymmetric encryption and digital signature. Because the publicity of public key, there are problems such as forgery and tampering. Digital certificates can solve these problems well. Encryption certificates can prevent information disclosure. The signing certificate can protect the public key. The certification authority (CA) is responsible for the issuance and endorsement of certificates. The authoritative CAs mainly include DigiCert, GlobalSign, VeriSign, etc. Users can also create their own local CAs for private networks.
3. Public Key Infrastructure (PKI) [68]: PKI is the security guarantee of the CA. PKI mainly solves the authentication and management of certificate life cycle, including CA, Registration Authority (RA) and integer database. PKI first requires users to provide identity and other information, and apply for certificates through RA. Then the RA will be sent to CA after passing the review. Finally, after CA audit, the certificate is manufactured and sent to the user. To revoke a certificate require the permissions from CA.
4. Merkle Tree [69]: Merkle Tree is a binary tree structure, also called hash tree. Merkle Tree calculates the n-1 layer hash value from the bottom layer data in pairs. Then hash the n-1 layer hash value in pairs to get the n-2 layer hash value, and so on, until

the top unique root node is obtained. Any change of underlying data will change the value of the root node, so Merkle Tree can well protect data from tampering.

5. Bloom Filter [70]: The bloom filter is based on hash, which can quickly find whether an element is in the set. Suppose the set has N elements and the number of hash functions is N . BF first initializes the dimension array, and each bit is 0. For N elements in the set, N hash values are obtained by mapping N hash functions, and each value corresponds to a bit of the dimensional array, which is marked as 1. In the query process, use the above N hash functions to calculate the hash value of the number X , and map it to the digit group, respectively. If N bits are all 1, the number X exists in the set. If one or more bits are not 1, X does not exist in the set. BF is suitable for fast lookup based on hash. However, when the mapping is too large, a hash conflict may occur, and there is a certain error rate. Figure 5 shows the working principle of Bloom Filter.
6. Homomorphic Encryption [71]: Homomorphic encryption allows processing of encrypted data without exposing the original data. Furthermore, after the processed data are decrypted, the processed results can be processed. Homomorphic encryption can enable other users to operate on the source data without exposing the source data.

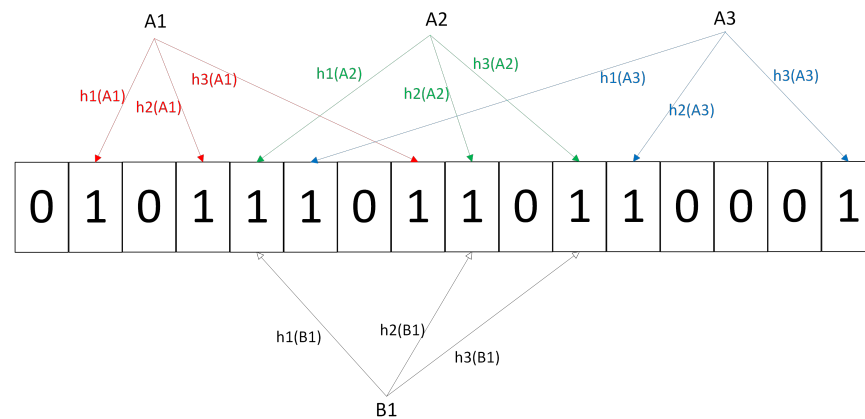


Figure 5. Bloom Filter.

2.2.4. Smart Contract

In 1994, Smart Contract was proposed [72]. At that time, the concept of smart contract was to combine user interface and protocol to ensure network specification and security. Smart contracts are used in contract and protocol related fields, such as credit, payment and copyright management. With the development of blockchain, blockchain 2.0 supports programmable contracts. So smart contracts are applied. Smart contract refers to a deterministic computer program. When certain conditions are met, the code will be triggered to complete the specified task. Smart contracts have the characteristics of openness and transparency. The openness, transparency and tamper proof of blockchain depend on the implementation of smart contracts.

The combination of smart contract and blockchain 2.0 can improve the scalability and convenience of blockchain. Smart contracts can be distributed among all nodes of the blockchain. This decentralized distributed structure can reduce central dependency and avoid single points of failure. Since smart contracts are deterministic codes, no matter which node runs the contract, the results will be consistent, so they can be used to verify and prevent malicious attacks. In addition, the reason why the contract is called “smart” is that smart contracts can be executed independently. When the specified conditions are not met, the contract will enter the “sleep state”. Once the conditions are met, it will be executed immediately without manual intervention. Smart contracts are rules designed in advance and written manually, which increases the flexibility of smart contracts. At the same time, once the contract is deployed, it cannot be changed, which can prevent malicious nodes from tampering with the code. The tamper proof feature of blockchain

also relies on smart contracts. Transparency and without relying on trust in the blockchain originate from smart contracts. Smart contracts are openly and transparently deployed in the public blockchain, and can be seen by all nodes. At the same time, since smart contracts cannot be changed, node can still interact through smart contracts when they do not trust each other and do not rely on a third party.

However, smart contracts are manually written, which will inevitably lead to defects and loopholes. At present, there have been two major security incidents for smart contracts. On 18 June 2016, according to the major loophole in the DAO contract, the hacker recursively flushed in the transfer function, and could withdraw the ether without reducing its own balance, which caused a loss of at least 50 million dollars. On 23 April 2018, hackers attacked BEC tokens. The contract loophole was used to transfer a large number of contract tokens to external accounts in a short time, resulting in a rapid decline in the price of the token or even close to zero.

At present, smart contracts have four major risks: (1) contract failure: there may be some unreasonable failure handling mechanisms for manually written code, which will lead to exceptions; (2) Privacy disclosure: the smart contract is open and transparent, which means that all users can see it, which will increase the risk of privacy disclosure; (3) Transaction spillover and anomaly: the smart contract itself has constraints such as transaction order dependency and conditional competition, which increases the risk of spillover and anomaly; (4) Denial of service: Attacks such as external operations or circular arrays will cause the smart contract to fail to be used normally by users for a period of time, which will result in the loss of the address of the contract owner's account.

2.2.5. Peer-to-Peer Networking (P2P)

Different from the traditional client/server (C/S) structure, P2P means that every entity can share resources in the network. Resources provide services in the network, and other peer node can access each other without intermediate entities. Participating node can not only share resources, but also obtain resources [73]. Bitcoin is built on P2P networks. The decentralized feature of blockchain relies on P2P networks. Each node on the network shares data records to keep the account ledgers consistent, so as to establish a distributed ledger.

P2P network has four development stages:

1. Centralized: The index server saves the index information (IP address, port, etc.) of all nodes, and other node index to the index node to find the information of other node. The centralized structure is simple, easy to implement, and suitable for network structures with fewer nodes. However, with the increase of node, the efficiency of centralized mode will be greatly reduced, and the probability of single point failure will be greatly increased.
2. Pure distribution: pure distribution removes the central node and establishes random connections in P2P node. New node randomly select any node in the network to connect. The node sends messages to its neighbor node, and the neighbor node sends messages to the neighbor node to complete the whole network broadcast. This method is called flooding mechanism. Pure distribution eliminates the central node, so there will be no single point of performance and single point of failure, and it has good scalability. However, pure distribution has the problem of flooding cycle and responding to message storm.
3. Hybrid: Hybrid combines centralized and purely distributed structures. Some node in the network are super node. Each super node has multiple ordinary node under it to form a local network, and super node form a distributed network. When an ordinary node joins, first select a super node to join the local network. Then the super node pushes the information of other super node to the node, and the node finally determines the super node through judgment. This form of network is highly flexible and easy to implement.

4. Structured P2P network: Different from random pure distributed network, structured P2P network is orderly organized according to a certain structure (ring, tree, etc.). In structured P2P networks, node space stores all nodes, and resource space stores the resource collection saved by all nodes. Resources and nodes will be numbered and mapped so that they can be located accurately. However, in practical applications, it is difficult for the node ID to correspond to the resource ID.

3. Motivations of This Survey

In this section, we highlight the current challenges of IoV, including: performance, trust and security, and privacy protection. On this basis, according to the characteristics of the blockchain, we propose the motivation to combine the blockchain with IoV to show how the blockchain can deal with the above challenges.

3.1. The Challenges in IoV

With the maturity of communication technology and transmission protocol, ITS is developing rapidly. ITS will bring unprecedented changes to our lives. As an important application of ITS, IoV will also face greater challenges. Unlike traditional vehicles, IoV is a special IoT. IoV also faces challenges such as security, privacy and trust. However, due to its special application scenarios, IoV may bring more challenges if only Internet technology is applied in the IoV field. With the increase of vehicles, IoV ecology becomes more and more huge. The demand for safe, scalable, stable and seamless information exchange between vehicles, users and roadside infrastructure is difficult to meet. For example, when a traffic accident occurs, accident related data is an important factor in judging the responsibility of the accident. How to store these data safely, reliably and efficiently is a challenge in IoV. In addition, real-time dynamic route planning by collecting the surrounding road traffic environment can bring convenience to vehicles, but it will also increase the risk of information leakage.

3.1.1. Performance

A. Data-based performance

In terms of IoV performance, there will be a lot of data when the vehicle is driving. How to effectively store data and ensure that data is not tampered with and embezzled is a challenge in IoV. In addition, the interconnection between vehicles needs to share or trade data. If all data are uploaded to the network, they will cause network congestion, increase delay, and reduce the efficiency of network information processing. Therefore, how to determine whether the data are useful and how to select useful data to share with specific node or the entire network is a major challenge for IoV.

B. Resource = based performance

The system resources are difficult to deal with massive amounts of data. In the case of limited resources such as vehicle computing, network communication and node storage, how to allocate resources correctly and reasonably and increase system throughput is also one of the problems. This problem can be solved by resource sharing between vehicles, but how to develop a sharing scheme is a difficult problem. In addition, with the proposal of the concept of green travel, more and more EVs have joined the IoV network. The problem faced by EVs is the transaction of power resources. For example, how to ensure that resource demanders and resource providers provide corresponding remuneration and services to each other as agreed during the charging process of EV. Furthermore, how can we effectively use the resources of stationary vehicles?

In addition, if the intelligent vehicle chooses not to connect to the network, it will form a data island, which will lead to incomplete traffic network. In the future, intelligent vehicles will gradually increase and IoV network will become larger and larger. If the vehicle is forced to access the network, it is likely that the vehicle is unwilling to share

resources with other vehicles. Therefore, how to create an incentive mechanism to stimulate more vehicles to join the network is also a problem.

3.1.2. Trust and Security

A. Trust

IoV not only connects vehicles, but also V2N, V2I and V2P. When vehicles communicate with each other, how to make both parties trust each other is a problem that needs to be considered in IoV. In addition, when the vehicle is connected to other entities except the vehicle, there may be a greater trust crisis between heterogeneous devices. How to determine the legitimacy of each other's identity between different devices, and how to quickly establish trust, choose whether to share information and establish a trusted connection is one of the current challenges of IoV. Even if vehicles fully trust each other's identity, there are also problems such as outdated information transmitted by vehicles with legal identity due to location, time and other factors, which will result in information failure. Some malicious node will also attack honest node, and use honest node to publish error information to destroy the network. Therefore, while ensuring identity trust, it is also necessary to confirm the trust of messages sent by nodes.

B. Security

The foundation of trust between vehicles is network security, and the foundation of identity trust is identity authentication. Identifying malicious nodes by establishing an authentication mechanism will improve the security of data. The foundation of information trust is the security of vehicle communication. When the vehicle transmits data in the network channel, it may be monitored, stolen or even tampered by malicious node, which will cause great losses. For example, if the map information uploaded by the user is tampered with, it may lead to the misjudgment of other vehicles, thus causing traffic accidents. One of the data security considerations is to ensure that the information received by other vehicles is complete and reliable. In addition, since IoV network is open, it is more vulnerable to attacks. How to resist attacks and ensure the security of the whole system is also an important issue.

3.1.3. Privacy Protection

In the era of the Internet of Everything, all the information of users is exposed in the network. When the intelligent vehicle is connected to the network, the information of the vehicle and the driver will be exposed in the network, and there is a risk of disclosure at any time, which seriously affects the security of IoV and increases the possibility of malicious attacks. Attackers can infer users' personal privacy by listening to broadcast, vehicle tracking, trajectory prediction and other ways to attack vehicles. In addition, when user privacy cannot be effectively guaranteed, users will no longer actively participate in the network, which will reduce user participation. Therefore, privacy protection is becoming more and more important.

In order to protect vehicle privacy, traditional methods use cryptography, certificateless signature, group signature, identity-based signature, public key or private key methods. These methods all need to set the trust value in advance in the central phase, which belongs to the centralized deployment structure. However, IoV is a high-speed mobile network. When the vehicle drives out of the original area, the set trust value will not be recognized, and the trust value needs to be rejudged. Therefore, the centralized deployment structure will greatly increase the communication delay but cannot prevent attacks such as Dos and DDos.

3.2. Motivation for Using Blockchain in IoV Scenarios

As a decentralized DLT, blockchain can bring novel solutions to IoV scenarios. In the IoV scenario, vehicles will generate and exchange massive data. In addition, traditional methods may not be applicable to IoV due to the heterogeneity of IoV network equipment

and the openness of VANET. How to efficiently establish network connection and securely share data in IoV is a challenge. Blockchain is a distributed ledger, which has the characteristics of immutability, tamper resistance and data security. Therefore, the application of blockchain to the IoT not only improves the performance of IoV, but also ensures the security of the system, and automatically establishes mutual trust between systems on the premise of ensuring the privacy of node.

First, in terms of data storage, blockchain is a decentralized distributed ledger structure. The blockchain can establish a network without intermediate node and connect node through P2P, which can reduce the delay in IoV. Distributed network architecture can support high-speed moving vehicles and frequently changed network topology. The node in the network can manage and operate independently, and can choose whether to share information with other node or whether to accept the information sent by other node, so as to avoid wasting resources by receiving uninterested information. This process does not need to apply to the central node, which reduces the network delay. With the addition of the blockchain, IoV will eventually form a secure autonomous network of vehicles.

Second, the most typical applications of blockchain are digital currencies such as Bitcoin and Ethereum. Therefore, in the resource transaction, the use of blockchain's outstanding achievements in digital currency can make the IoV resource transaction process more secure, without causing payment repudiation, currency dual payment and other problems. In addition, the blockchain supports rewarding vehicles in the form of currency, which can stimulate more vehicles sharing resource.

Third, blockchain is a P2P direct connection that supports heterogeneous node to establish connections. Node do not need to be of uniform type, and node can independently master their own operations. The blockchain allows the establishment of a trusted connection between untrusted node according to consensus algorithms and smart contracts, and the transaction can be completed without the vehicle verifying the credibility of node, which can reduce the verification time. In addition, based on the consensus algorithm, the entire transaction can be passed and uploaded to the chain only after being checked by other node in the network, which ensures the accuracy of information. Moreover, once the information is linked, it cannot be changed, so the credibility and security of the information are guaranteed, and the audit and traceability of the information are also increased.

Fourth, for IoV network security issues, digital signatures, certificates and other methods can be used to authenticate the identity, ensuring the integrity of node, which is the basis for heterogeneous untrusted node to establish trusted connections. Smart contract can also ensure the invariance of the protocol, and the cryptographic principles can also ensure the security of data. In addition, once fraud is found, the data and node will be recorded in the ledger. The ledger is not allowed to be modified, which ensures the security of the system. In terms of attack resistance, blockchain can effectively avoid single point, interruption and other attacks because all nodes synchronously maintain a ledger and save the same ledger copy locally.

Finally, the blockchain has increased the protection of vehicle privacy with the support of modern cryptography. Hash function is a good irreversible encryption method, which can encrypt the identity. The identity information encrypted by hash function has good invisibility. Even if the attacker obtains the identity information, the real identity of the vehicle cannot be inferred. In addition, blockchain also has a good performance in digital signatures and digital certificates. Using blockchain signatures and issuing certificates can ensure the integrity of identity content, and signatures can be cracked only when the corresponding private key is obtained. The private key can be saved locally to protect the privacy of users.

4. Application of Blockchain in IoV

After reading and summarizing articles on blockchain technology, IoV technology and blockchain's application on IoV, this paper divides blockchain's application on IoV

into five aspects: data management, resource management, privacy management, trust management and security management. Next, the five aspects are described, respectively.

4.1. Data Management

In traditional IoV, with the increase of vehicles and RSUs, nodes generate more and more data. A large amount of data brings data management pressure to IoV network. Although the emergence of edge computing alleviates the storage pressure of IoV, because the edge node is open, it is more vulnerable to attacks by malicious nodes. In addition, different edge nodes have different service operators, which makes the trust mode between nodes different, so it is difficult to share data.

In order to solve the above problems, it would be a good choice to introduce blockchain into IoV to manage data. Since blockchain is a decentralized distributed ledger structure, this structure stores data in each node in a distributed manner, effectively avoiding single point attacks and other problems. In addition, the tamper resistance of the blockchain can effectively protect data from being changed by malicious nodes. Consensus protocols and cryptography are used to ensure the correctness and privacy of data in the process of blockchain data trading and sharing. It is worth mentioning that the data on the blockchain are traceable. Therefore, if there are malicious nodes, the blockchain can immediately query them and give corresponding penalties, which reduces the suspicion of vehicles on other nodes. Even if both parties do not trust, the blockchain can establish a trusted connection between untrusted nodes, which greatly improves the enthusiasm of vehicles for data transactions.

This section will describe the blockchain-based IoV data management in two aspects: data storage and protection, and data sharing and trading.

4.1.1. Data Storage and Protection

In IoV, massive data generated by vehicles needs the storage platform to store data in the highest utilization rate. In addition, for some special cases, such as attacks by malicious nodes, single point failures, privacy leaks, etc., how to ensure data security is also a point to consider.

The storage pressure of traditional IoV vehicles is high. Introducing edge computing into the IoV network will reduce the amount of information stored in vehicles. However, high-quality connections need to be guaranteed between moving vehicles and edge servers, and large amounts of data stored on edge servers or vehicles are vulnerable to attacks. Storing data in the cloud will increase communication delay. Blockchain is used to enable data storage in IoV to solve above problems, and this can ensure data security [74]. The proposal deploys the blockchain in the edge server, which can avoid the problem of unstable communication caused by the dynamic change of network topology during the movement of vehicles. The vehicle transmits the data to the edge server and the edge server acts as a miner node to compete for permission to write blocks, which can well ensure the credibility of the data. Simultaneously, to ensure the miners' communication time, the scheme uses a random method to design the deployment of miners' nodes. The experimental results show that the addition of blockchain can make IoV system store data more safely and quickly.

However, although data storage on the blockchain can improve security, too much data will cause great pressure on the storage of the blockchain. The work [75,76] considered the storage capacity of blockchain, and proposed to use lightweight blockchain to store data.

In IoV based on edge computing, MEC usually needs to do a lot of work [75]. Especially after joining the blockchain, MEC's storage capacity has faced a huge challenge. In order to balance the work of MEC, it is a good choice to reduce the storage capacity of blockchain. This paper is dedicated to building a lightweight blockchain to reduce the storage pressure of MEC. In the proposed scheme, vehicle calculation, unloading and caching are regarded as Markov decision-making processes (MDP), and asynchronous advantage actor-critic (A3C) algorithm is used to optimize decision-making. At the same time, the purpose of maximizing blockchain throughput is achieved by reducing the number of miners, block

interval time and block storage. Finally, the author simulated the situation of 30 vehicles and 6 BS with 3–4 RSUs around. The experimental results show that with the increase of vehicles, the performance of this scheme in terms of total consumption will be more superior. Figure 6 shows the system model.

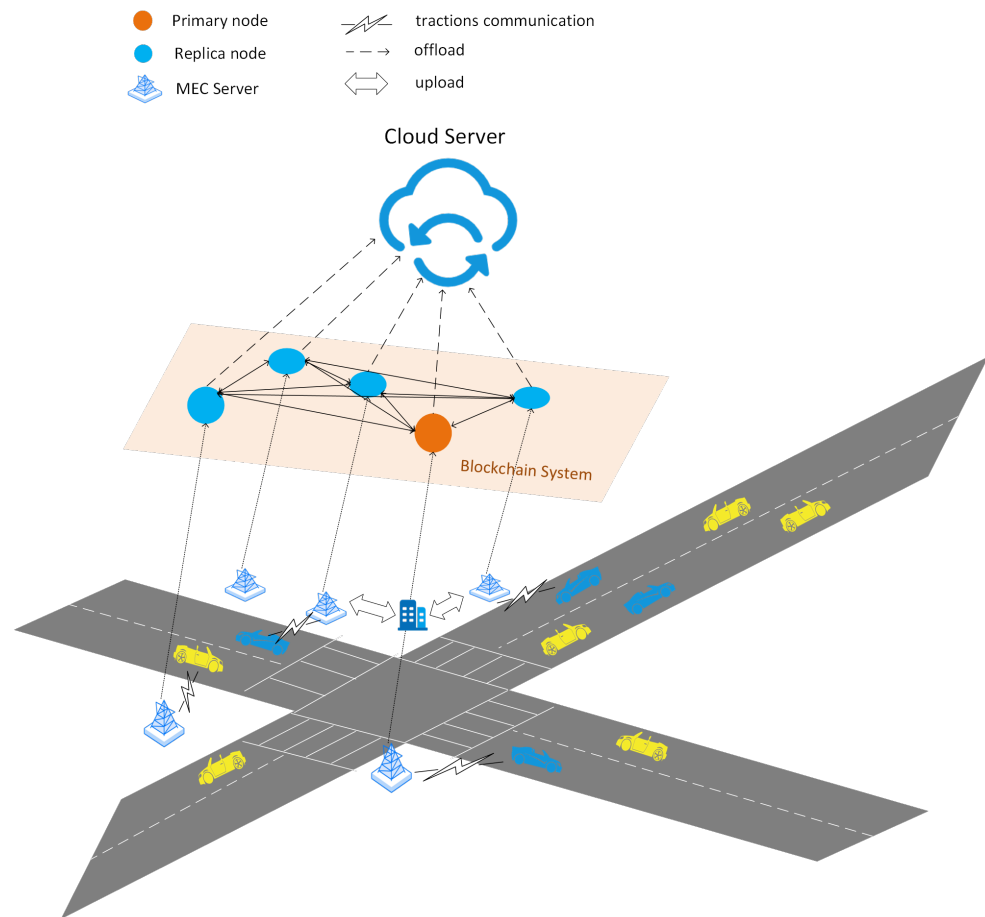


Figure 6. MEC and Blockchain-Enabled Energy Efficient Internet of Vehicles Based on A3C Approach structure in [75].

In paper [76], author believes that it is a safer choice to introduce blockchain into IoV for data storage. However, a large amount of data puts storage pressure on the blockchain and increases the delay. To solve the deflection of low data storage utilization and long block response time in IoV, the author proposes a lightweight blockchain storage structure. Different from [75], this structure uses collaborative caching when RSU builds the blockchain, enabling RSU to search and store blocks cooperatively. When the RSU receives a request, it first searches the local storage. When the situation is not found, a request will be made to the neighbor RSU. The neighbor RSU calls its own local cache to respond. This data storage method effectively reduces the response delay of the block chain in IoV. At the same time, according to the different requirements of different vehicles for service data, the block filtering algorithm is used to develop customized blocks according to the needs, which reduces the data storage pressure of the blocks and improves the storage space utilization of the blockchain.

Except above problems, how to ensure the safe storage of data is also a significant part in the event of an accident. Considering that traffic accidents often require the video in the Video Event Data Recorder (VEDR) to divide the responsibility for accidents. However, with the increase of node, the large video files will grow exponentially.

To reduce the pressure on the storage data of traditional blockchain increases with the increase of node, the author of Ref. [77] proposes a data management scheme based on blockchain and IPFS. This scheme uses blockchain to ensure the correctness of data, and uses IPFS to reduce the storage capacity of video data generated by node. At the same time, KPI encryption algorithm is used to issue public and private keys to node to ensure that only upload node can access data and ensure data security. First, the leader node PL is randomly selected in the blockchain network, and the common node PN uploads data to IPFS. IPFS returns a hashIPFS. PN sends the encrypted hashIPFS to PL as a transaction, and PL creates blocks. Then, all nodes use the private key to decrypt hashIPFS in order to verify whether their transactions are correct. If it is correct, it will be sent to the next node. After all nodes pass the verification, the last node will send the block to PL for confirmation. After the PL is confirmed, the block will be released. Once the block is published, it cannot be changed, and only the user who uploads the video can decrypt the video using the private key. The author has carried out upload and download experiments. The upload delay of 20.4 MB video is between 143 and 272 ms, and the download delay is between 49 and 138 ms. The results show that the time of the data management scheme proposed in this paper increases linearly with data growth. Compared with exponential growth, the storage performance of blockchain and IPFS is significantly higher.

In addition, in the event of a traffic accident, in some cases, vehicles collide with vehicles or vehicles collide with people, while in other cases, vehicles may collide with roadside public facilities. In the second case and the first case, there is no witness when death occurs or vehicles hit and run. Therefore, digitizing the accident evidence and ensuring the correctness of the evidence are important factors for the division of accident responsibility. The author of Ref. [78] designs an IoV vehicle accident data protection platform based on blockchain. First, when any element in the IoV (including people, vehicles, signal lights, etc.) detects a traffic accident, it will immediately report to the RSU and upload relevant data. After receiving the alarm, the RSU requests more accident related data from node near the accident and summarizes them. In order to free more data storage space to store more data, the author uses the Interplanetary File System (IPFS) storage mode. Storing the data on the RSU in the IPFS can reduce the data storage capacity of the RSU. The RSU only needs to store the hash value in the IPFS. After completing the above steps, RSU generates the accident ID and vehicle ID and maps them, and then calls the smart contract to write the evidence into the blockchain. Once the evidence is linked, it cannot be changed, which ensures the authenticity of the evidence. At the same time, stakeholders of the accident can apply to RSU for data access through smart contracts. Investigators finally upload the result generation report to the blockchain for settlement through verification of evidence.

Furthermore, for data protection, the author of Ref. [79] proposes a data protection scheme. The scheme transmits data to the cloud in a collusion resistant manner to ensure the correctness of data, and uses distributed blockchain to avoid single point attacks. This scheme transmits data to the cloud through the IoV node, and each transmission will be stored as a transaction in the blockchain, and the transaction data will also be stored in the blockchain in a decentralized manner. In addition, to ensure the legitimacy of the data source, the system adds a certificate/key revocation mechanism to ensure that the communication node is not a malicious node or an honest node injured by a malicious node. The author analyzes the security of this proposal when it is attacked by Forgery, Replay and Modification. In addition, the author also analyzes the security of data timeliness, public key security, block necessity and access control. The analysis results prove that the proposal can make the data in IoV more secure.

In addition, federated learning has also achieved good results in IoV data protection by uploading local training models. However, the difference of upload models of different nodes leads to the risk of data leakage when FL is used only. The author of Ref. [80] Join the blockchain on the basis of FL, and protect system data by autonomous authorization. The author believes that there are two types of data protection risks in FL based IoV, one

is local data and model leakage, the other is malicious node deliberately upload wrong models to damage the system. Based on the above two problems, the author uses the blockchain to endorse node, and automatically selects node participating in training to ensure transparent profit distribution and illegal tracking. Simultaneously, to prevent inference attacks, differential privacy (DP) is introduced to ensure the security of local models and data. Furthermore, to ensure the honesty of node, the malicious update removal algorithm of the reliability filter is added to reduce impacts of malicious node uploading wrong data on the system. Finally, the author designed an IoV system containing 50 devices, 5 MECs and a cloud to conduct simulation experiments. The experimental results show that the system can still maintain a low attack success rate of 9.54% in the case of 50 consecutive attacks and increasing attackers.

4.1.2. Data Sharing and Trading

There is massive data exchange in IoV, including sharing and trading. To make up the defect of the traditional data exchange system cannot transmit information safely and efficiently, it is a good choice to introduce a secure and transparent blockchain into the data sharing system. The authors of Refs. [81,82] work on the security problems that are easy to occur in the process of data transaction. The author of Ref. [81] proposes a federal learning knowledge trading platform in blockchain-assisted IoV. This platform is utilized to solve the security problems of the centralized trading market, such as single point failures and untrusted central node. The vehicle learns through data transactions with other vehicles, and this process will send a large number of broadcast requests to the RSU. However, too many requests will cause network congestion and waste of resources, affecting network efficiency. To solve this problem, the author uses smart contract automation to disperse vehicle requests to coordinate transactions. After the transaction, the blockchain is responsible for keeping the transaction data and results to prevent historical data from being tampered with. The author analyzes the security, profitability and efficiency of the system. The platform has been proved to be able to efficiently and safely meet the data transactions in IoV.

In paper [82], the author proposes to introduce federated blockchain into IoV data transactions to ensure the security and authenticity of transactions. The alliance blockchain's tamper resistance can audit and verify transaction records. On this basis, the blockchain-assisted IoV transaction framework was designed. The blockchain includes three core components: transaction data, blockchain architecture and consensus. In addition, the author also designed an iterative double auction mechanism to maximize social welfare so that the transaction price can satisfy both parties. The transaction process hides the identity information to avoid the disclosure of privacy.

In traditional IoV, vehicles share data through RSU. However, RSUs are semi trusted node. The data stored in the RSU may be wrong, and the RSU cannot ensure the correctness of the shared data. In addition, after the data is tampered, the RSU cannot track the tampered node. Based on the above problems, the author of Ref. [83] similar to [82], proposes to use the alliance blockchain to store data instead of RSU. The alliance blockchain can ensure that data will not be tampered by malicious node, and can track malicious node when attacked. In addition, malicious node may also gain illegitimate benefits by stealing other people's data for sharing or sharing data in a dual payment attack similar to the blockchain. To solve this problem, the author not only creates conditional privacy protection through enhanced DPoS consensus, but also designs a trust scoring mechanism to ensure that the data signature has been used only once. Besides, the author also uses smart contracts for automated credit rating verification. Finally, the author evaluates the block generation speed, throughput and transmission performance of the blockchain by simulating 400 vehicles and 21 miners' nodes. Experimental results show that the block generation speed of this scheme is 1.5 s, 10 times that of Ethereum and 400 times that of Bitcoin. The maximum throughput can reach 4000 Transaction Per Second (TPS), while the

throughput of Ethereum is only 25 TPS. The block confirmation time is 12 s and Bitcoin 3600 s. The above data shows that the scheme has a good effect in IoV data sharing.

The author of Ref. [84] also uses the alliance blockchain and proposes a vehicle data sharing system based on the alliance blockchain. The alliance blockchain can trust the sharing right to node and let node choose whether to participate in the sharing process. Simultaneously, to ensure data security sharing, the author designed a smart contract: ISSC for vehicle information sharing on the blockchain by taking advantage of the feature that smart contracts cannot be tampered with once deployed. First, the vehicle (VI) requesting data downloads the latest block from the DAG and queries the desired data. They will find the VI that uploaded the data and send them a sharing request. Then VI verifies the VM identity and sets access permissions, and send data private key, VM public key and other information to nearby DAG1, and triggers ISSC. The ISSC judges the legitimacy of their identities and data. Once it passes the judgment, the ISSC sends data related information to the VM. If the VM is not within the DAG1 communication range, it will be sent to the DAG2 near the VM, and the DAG2 will communicate with the VM. This process can ensure that the data will not be tampered during transmission, and the sharing process will be triggered through smart contract automation. In addition, the smart contract also restricts access, and unauthorized users cannot participate in the sharing process.

The author of Ref. [85] uses Federal Learning (FL) for IoV to achieve efficient traffic management. FL requires massive data sharing between nodes. Ensure data security and privacy protection during sharing has become a research hotspot. To solve this problem, the author applies blockchain to FL-based IoV, uses blockchain network to protect FL data sharing process, and provides a safe and reliable data sharing platform for the network. The author believes that RSUs participating in IoV have different resources, so they are divided into three roles: light node, full node and miner. In addition, the trusted institutions responsible for registering and issuing certificates in the cloud and blockchain are also set as miners. Miners need to sort out all the data they receive, compete for block writing rights, and finally create a block to store model data. Besides, to improve utilization rate of storage resources, the blockchain does not need to save all training parameters, but can delete non key historical data locally, just save the bills with transactions.

The above works only consider the security of data, not the privacy. The author of Ref. [86] proposes a blockchain-enabled adaptive neuro-fuzzy payment system to solve the problem that the privacy of vehicles in IoV is violated in the process of data sharing and the resulting low sharing participation. First, in the initialization process, the system uses a pseudonym exchange mechanism and smart contracts to ensure the privacy and security of users. Each vehicle has its own block to store the information of identity exchange, and the block update is completed by the smart contract, which improves the credibility of the identity. Secondly, the author proposes to combine blockchain and adaptive neuro-fuzzy to evaluate the quality of data shared by vehicles, so as to give corresponding rewards to vehicles through different data quality. The quality of data is comprehensively evaluated by vehicle location, time and other factors, which fully guarantees the fairness of evaluation. Finally, in order to avoid the honest node being attacked maliciously illegally transferring data in the network, the scheme cancels the vehicle's pseudonym according to the vehicle's pseudonym exchange history table so that it cannot share data in the network. However, this scheme does not punish the malicious node.

The author of Ref. [87] proposes a smart contract to punish malicious node. To ensure data security, this paper proposes a dual blockchain IoV data sharing scheme. The scheme includes two parallel blockchain running simultaneously. The blockchain to be uploaded is used to save vehicle information and store the user's request. The scheme mainly provides four smart contracts to automate the information sharing process. (1) Registration contract: the data provider registers data through consensus, and then the miners generate blocks. (2) Automatic contract execution: when the demander applies for data from the blockchain, the encrypted data will be automatically transferred to the demander. Once the data are decrypted, it will prove that the data meet the requirements, and the smart contract will

automatically execute the transaction. (3) Grievance contract: both the supplier and the demander can appeal when there is an exception in the sharing process. (4) Penalty contract: automatically executed when the complaint takes effect. These four smart contracts ensure the security and legitimacy of data sharing.

Table 1 summarizes the research directions and applications of papers related to data management.

Table 1. Data Management Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[74] [75] [76] [77]	Reduce storage pressure on vehicles, RSUs and blockchain.	<ol style="list-style-type: none"> 1. Data are stored on the blockchain, and then the blockchain is deployed on the edge server instead of the cloud to reduce latency. 2. Reduce the size of the blockchain by reducing the number of miners, block intervals, etc. 3. Reduce RSU storage by collaborative caching. 4. Using IPFS to store data, the blockchain only needs to store hash values. 	Storing data in the blockchain can reduce the storage pressure on vehicles.
[78] [79] [80]	Data correctness protection.	<ol style="list-style-type: none"> 1. Design the data protection platform and write the evidence in the blockchain. 2. Add a certificate/key revocation mechanism on the basis of the blockchain to ensure the legality of the data source. 3. Secure the federated learning process through the blockchain. 	<ol style="list-style-type: none"> 1. Utilizing the non-tamperable modification of the blockchain, storing the evidence in the blockchain can ensure the accuracy of the evidence. 2. Use the distributed storage structure of the blockchain to prevent single-point attacks. 3. Use the blockchain as an endorsement for uploading local models, and use the transparency of the blockchain to ensure that the data is legal.
[81] [82] [83] [84] [85]	How to ensure the safety of transactions.	<ol style="list-style-type: none"> 1. All transaction processes are audited and recorded by the Consortium blockchain to ensure transaction security. 2. Entrust the sharing right to the node, so that the node can independently choose whether to participate in the transaction. 	<ol style="list-style-type: none"> 1. The transaction process is independently determined by using the alliance blockchain, the security of the data is not leaked. 2. Automatically complete the transaction process by using consensus and smart contracts to make the transaction undeniable.
[86] [87]	Protect the privacy of data.	Creating a Reputation Evaluation Mechanism with Blockchain.	The integrity of nodes is determined through the blockchain, and dishonest nodes are punished.

4.2. Resource Management

Although many data management schemes have been introduced in the previous section, data management needs a lot of resources, such as computing resources and storage resources. How to use resources safely and efficiently to achieve better data management is a problem that needs to be discussed.

4.2.1. Resource Scheduling

The author of Ref. [88] believes that applying blockchain to IoV can solve the single point of failure problem of IoV and increase the scalability of IoV. However, channel

resources are limited. If all vehicles are in the same channel at the same time, congestion will occur. It will also cause too many transactions in the blockchain, leading to response congestion. How to maximize the channel utilization in the limited channel resources is a challenge. The author proposes a blockchain multi-channel scheme based on vehicle density, which allows vehicles to select different channels according to their service requirements (low throughput or low latency) to maximize resource utilization. At the initial stage of blockchain construction, nodes choose to install blockchain programs according to their roles. At this time, the vehicle does not participate in the consensus. The infrastructure, as an endorsement node, joins multiple channels to provide flexible services. Then the vehicles need to register its own identity information in the CA to ensure that it can legally join the blockchain network, and the vehicles registered successfully can participate in the transaction. The RSU monitors the density of vehicles in the channel at all times, and selects an appropriate channel for vehicles according to the density of vehicles in the next transaction. Authors use Hyperledger Fabric to conduct simulation experiments, assuming that there are 1000–2000 vehicles in the fixed area, and vehicles send information every 10 s, and 100 transactions every time. Based on this condition, the best communication channel with different service requirements under different vehicle densities is selected. If the number of vehicles is greater than 2000, the throughput sensitive vehicles select channel 4, and the delay sensitive vehicles select channel 1. The experimental results show that selecting a reasonable channel for vehicles with different service requirements under different densities will improve the channel utilization and improve the efficiency of transaction processing. Although this method makes full use of channel resources, it does not consider that the length of the blockchain will increase with the increase of vehicles.

To make up the defect of resource tension caused by too large blockchain in blockchain-based IoV system, the author of Ref. [89] proposes a network architecture of sub chains in different regions. Specifically, the architecture divides the blockchain into main chain and sub chain. Vehicles within a certain area form a sub chain, and all sub chains form a main chain. The system consists of a sub chain with fewer node and relatively idle resources, which helps the main chain to undertake some computing and storage work, so it can reduce the resource burden of the main chain. In the sub chain, RSU, as a consensus node, participates in the whole process of blockchain construction and maintenance. Therefore, vehicle joining or exiting the region will not affect sub chains. The construction of the main chain is the responsibility of the service agency as the whole node. The vehicle only needs to communicate with the sub chain. The consensus node in the sub chain communicates with the consensus node in the main chain, which reduces the communication cost of the vehicle.

Different from the above work, Refs. [90–93] consider the computing resources in the network. The author of Ref. [90] proposes a blockchain-based hierarchical resource scheduling model for IoV with limited computing resources. This model solves the problem of computing resource shortage in IoV by efficiently allocating computing resources, and effectively improves the behavior of IoV. In this scheme, the priority order of resource scheduling is blockchain service layer, infrastructure layer and network layer. This scheme decouples the three layers resources and realizes flexible resource scheduling. In other words, when the current indicators of the system are lower than expected, the resources of service layer should be dispatched first. If the resources of the service layer are insufficient, the resources of the infrastructure layer will be retrieved. If the resources of the first two layers are insufficient, the network layer resources will be called finally. This hierarchical resource scheduling method effectively solves the problem of resource shortage, and also avoids resource waste. In addition, the author designed a resource monitoring system to monitor the utilization of resources in the system in a continuous and real-time manner and analyze the current running status of the system. With the help of this system, the resource layering system can understand the real-time resource surplus and demand more quickly and allocate the limited resources better.

Similar to the idea of hierarchical scheduling in [90], there are [91]. However, unlike [90], the author of Ref. [91] prefers to create blockchain of different sizes according to the different capabilities of node to achieve the effect of flexible resource utilization and make resource utilization more efficient. Aiming at the problem of low resource utilization in the existing blockchain-assisted IoV system, the author proposes a blockchain IoV network structure based on RSU classification. The author combines three factors: distance within clusters, distance between clusters, and network coverage of clusters. The scheme first clusters the RSUs and clusters the RSUs that are close to each other. Then, cluster heads are selected to build a blockchain network based on the resource and performance differences of heterogeneous RSUs. The resource rich RSU is responsible for handling more complex tasks. This method can control the size of the blockchain network according to the ability of the RSU to make the construction of the blockchain more flexible. In addition, other RSUs with limited resources do not perform calculation. It can use resources for storage and transmission, which improves the throughput of the cluster while ensuring the utilization of network resources. This resource management scheme improves the resource utilization of node in the network, thus improving the performance of the blockchain. Besides, to save the storage resources of the blocks, the data will not be completely uploaded to the blockchain, but will be selectively stored locally in the cluster, which reduces the storage capacity of the blockchain and saves the storage resources of the blockchain. Figure 7 is the system structure diagram.

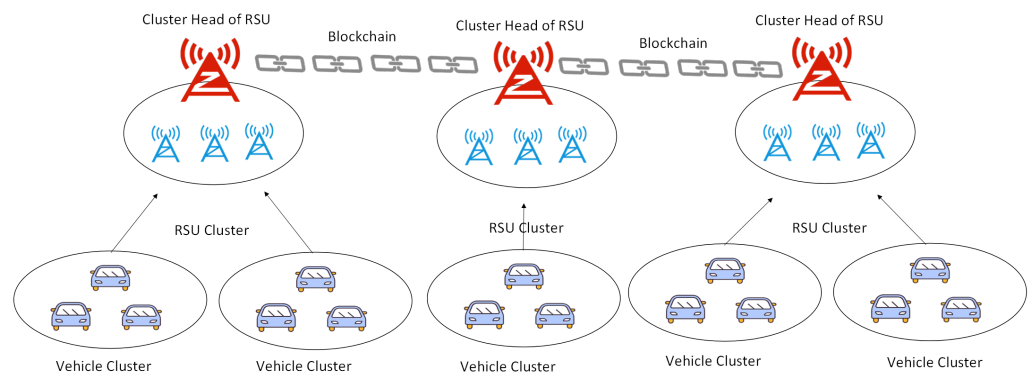


Figure 7. Heterogeneous resource scheduling scheme based on blockchain proposed in [90].

Compared with the resource allocation method mentioned above, the author of Ref. [92] considers the dynamic topology change caused by vehicle movement. The author believes that the centralized data acquisition of traditional IoV has problems such as low efficiency and high consumption of computing resources, so it is a trend to choose distributed machine learning (DML) in IoV. However, for IoV environment, high-speed mobile and heterogeneous vehicles seriously affect the learning efficiency. Based on the above problems, the author proposes a learning framework based on the combination of blockchain and deep compression method: CLDC. This method aims to build a distributed network architecture in the IoV environment through the blockchain, so as to efficient utilization of computing resources and communication resources. First, the CLDC algorithm is used to improve the local training efficiency of node. Then, the blockchain's tamper resistance is used to ensure the accuracy of node 'shared results. The redundant Byzantine fault-tolerant consensus method based on learning is used in blockchain network to ensure the quality of node 'training results. Experiments show that this method can achieve good results in computing and communication resource allocation.

Moreover, with the maturity of UAV technology, UAV is applied in IoV. The intelligent transportation IoV mode of sky assisted ground has become a new paradigm. At present, the centralized UAV assisted vehicle communication needs to consume a lot of resources (computing resources, network resources, etc.), which brings a lot of trouble to calculation and task unloading. The author of Ref. [93] introduces blockchain to assist UAVs and vehicles to build a distributed communication system, making the whole communication life cycle transparent and safe. Based on the V2X infrastructure, the author proposes the “B-UV2X” architecture based on the alliance blockchain and designs four smart contracts, which are, respectively, used for registration, transaction addition, update of the blockchain and monitoring resource management and customization. The architecture also ensures the security of blocks through two-way verification and the consensus mechanism in the hyperledger fabric. In addition, NuCypher threshold proxy re encryption mechanism is used for encryption to ensure the security of the system. The simulation results show that the system consumes 12.17% less network resources than the traditional centralized network structure. In terms of computing resources, the computing load is reduced by 7.93% compared with traditional methods, and the security is improved by 9.76%.

However, these methods need a lot of resources in the construction of blockchain. For the problem of resources storage, the author of Ref. [94] proposes a lightweight blockchain-assisted IoV security framework. The traditional blockchain-based IoV framework needs to deploy the blockchain on physical devices, but this will increase the pressure on devices. On the basis of the traditional blockchain, the author defines a branch blockchain to reduce resource consumption while ensuring system security. The scheme is divided into two layers. The centralized layer is used to provide vehicle registration services, authorize and verify the identity of vehicles. The branch layer is used to provide communication for vehicles registered successfully. The network settings of the blockchain are vehicles (automatic cars, taxis and buses), smart contracts, RSUs, miners’ node, control node (providing corresponding services when the miners’ node cannot process transactions, such as no response or no memory) and distributed servers (different interaction servers between blockchain, providing communication between blockchain). This scheme achieves the effect of reasonable resource allocation by introducing lightweight branch blockchain.

The above methods all consider a single vehicle resource. If the vehicle and RSU resources can be combined, the resource utilization rate of IoV will be improved. The author of Ref. [95] proposes a blockchain-based resource management scheme in IoV. The scheme takes RSU as a miner and allows them to hire nearby vehicles to provide computing resources for them. First, RSU predicts the vehicles within the range of verification in the next block based on the historical data and vehicle speed of other RSUs. Then the transaction is packaged into blocks and uploaded to RSU for verification. After the signature of the block is verified, the RSU delivers the legal block to the vehicle predicted in the first step for verification. After vehicle verification, the results will be returned to RSU. Next, after RSU collects the verification results of all vehicles, it will be handed over to other RSUs for mutual verification, and RSU will save the final verification results. Finally, after more than two-thirds of the verification results in the system pass, RSU will send the result confirmation report to the block claiming this, and it will be added to the blockchain. This method saves RSU resources and enables RSU to devote itself to more complex work by fully invoking the computing resources of vehicles and giving simple computing programs to vehicle computing. The author compares the traditional calculation method using only RSU. The system has achieved good results in terms of maximum block verification delay, blockchain throughput and system security. The results show that the scheme can balance system throughput and security in terms of resource utilization.

Table 2 summarizes the research directions and applications of papers related to resource scheduling.

Table 2. Resource Scheduling Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[88] [89]	How to Utilize Communication Resources Effectively.	<ol style="list-style-type: none"> 1. Multi-channel resource management of blockchain based on vehicle density. 2. Build a blockchain network architecture with sub-regional sub-chains and main chains. 	<ol style="list-style-type: none"> 1. According to the vehicle density, provide the optimal communication channel selection scheme for vehicles according to the vehicle blockchain service requirements. 2. Sub-chains are formed in a small area, and all sub-chains form the main chain. The sub-chains only need to communicate with the consensus nodes of the main chain, reducing communication resources.
[90] [91] [92] [93]	How to Utilize computing resources efficiently.	<ol style="list-style-type: none"> 1. Hierarchical scheduling of computing resources based on blockchain. 2. Create different blockchains according to different capabilities of nodes. 3. Combining blockchain with CLDC approach. 4. Blockchain-assisted UAVs and vehicles build a resource management platform. 	<ol style="list-style-type: none"> 1. The system prioritizes scheduling blockchain resources to alleviate the problem of computing resource shortage. 2. Use clustering to divide vehicles by region, and select communication nodes according to their capabilities to build blockchains of different sizes to alleviate the shortage of computing resources for other vehicles. 3. The blockchain builds a distributed architecture in the network to reduce the impact of dynamic topology on the computing process. 4. Create a distributed blockchain computing and offloading solution for UAVs and vehicles.
[94] [95]	How to Utilize storage resources efficiently.	<ol style="list-style-type: none"> 1. The resources of single-vehicle are stored in the lightweight blockchain. 2. Vehicles and RSUs combine to build a storage pool. 	<ol style="list-style-type: none"> 1. Divide the blockchain into two layers, and decouple registration and communication to achieve the purpose of effective utilization of storage resources. 2. The vehicle and RSU jointly build resource storage through the blockchain to improve the utilization of storage resources.

4.2.2. Resource Sharing and Trading

The author of Ref. [95] proposed the method of integrating other vehicle resources by employment, which provides a new direction for resource management in IoV. Common vehicles share computing, storage and other resources with each other, which will greatly improve the performance of IoV network.

For vehicle resource sharing, the author of Ref. [96] fully considers the vehicle location and resource availability, introduces the alliance blockchain into IoV resource sharing, and designs a lightweight resource sharing scheme based on the alliance blockchain. The interaction process is packaged as a transaction and uploaded to RSU, which is responsible for the establishment and maintenance of the entire blockchain ledger. Different from the public blockchain, the alliance blockchain allows node not to participate in all transaction processes, but only to participate in transactions of interest, which reduces the communication cost in the resource sharing process, and also ensures that the shared data is not obtained by other vehicles. In terms of resource matching and pricing, the author combines deep reinforcement learning (DRL) and smart contracts to dynamically match resources

according to vehicle locations. Compared with the traditional unified pricing method, the performance of this resource matching method is improved by 30%. In addition, on the consensus mechanism, the author proposes a reputation proof scheme (PoR) to compensate for the computational power waste of the traditional consensus mechanism. This scheme calculates the reputation value according to the performance of the vehicle transaction process, and updates it in real time. The consensus mechanism determines the record node through the reputation value.

The author in [96] only considers the resource transaction and sharing of moving vehicles but ignores stationary vehicles. In real life, the resources of stationary vehicles are more abundant than those of mobile vehicles. Ignoring stationary vehicle resources greatly wastes the available resources in IoV. Parking vehicles (PV) have very rich idle resources due to their non moving, non computing and other characteristics. In addition, compared with mobile vehicles, the stationary vehicle network topology changes little, so the vehicle network is easier to build. How to efficiently use the idle resources of stationary vehicles and add them to IoV to maximize resource utilization is very challenging. The author of Ref. [97] considers the stationary vehicles. In vehicle edge computing (VEC), ParkingChain network is built for IoV resource sharing, which makes the sharing process more secure and efficient. First, PV registers the account, and the credit institution is responsible for verification and account distribution. Then the source requester (SR) issues the request, including service time, task size, resource reward, etc. Then the resource provider PV selects the request by accessing the smart contract. After PV determines the request, both sides will sign the contract through the smart contract. At the same time, PV needs to pay a deposit to the smart contract to ensure the QoS, and then send the task to SR. PV starts to execute after receiving the task, and the execution result is uploaded to the smart contract for judgment. If the service terminates abnormally (such as the PV becomes running) or the PV calculation result does not meet the requirements, the deposit will be sent directly to the SR. Finally, if the service provided by PV passes the verification, it means that the service is completed, and SR needs to pay the promised reward to PV, and the deposit is also returned to PV. For resource security sharing and efficient service, a multi weight subjective logic delegated byzantine fault tolerance (DBFT) consensus mechanism is designed. The mechanism selects PV with high reputation value as the consensus node to audit transaction records and store them in ParkingChain

The author of Ref. [98] also believes that PV resources are important resources in IoV. However, due to the participation of trusted institutions, the resource sharing scheme in [97] faces problems such as centralization, insecurity and poor scalability. For these problems, the author proposes a blockchain-based IoV real-time payment system. Vehicle to vehicle, vehicle to infrastructure can be paid safely and timely in resource exchange. This scheme uses blockchain to connect different participants in IoV, and uses Ethereum to build a parking payment system. The system is divided into three layers. The first layer is the perception layer. The perception layer is the IoT application for car renters and parking providers. Its main function is to communicate with vehicles, find parking spaces and manage transactions. Next is the network layer, which is responsible for the communication between the device and the cloud. Finally, the application layer is responsible for building a blockchain system to build a distributed secure payment management, eliminate central management, and avoid single points of failure. In this scheme, blockchain is responsible for managing all payment operations. Every parking and payment of the vehicle is saved to the blockchain as a transaction to prevent the transaction from repudiation and protect the interests of both sides. Finally, the author demonstrates the effectiveness of the proposed scheme from eight aspects: security, cost, execution and processing time, memory and consumption, integrity, consistency, confidentiality, and immunity.

How to motivate vehicles to participate more actively in the network is a problem except security in the direction of resource sharing. To solve this problem, the author of Ref. [99] proposes a reputation based incentive mechanism to stimulate vehicles to participate more actively in resource sharing to improve the quality of sharing. The

mechanism first initializes the reputation value of the node and stores this value and the identity information of the node in the CA. Then two thresholds of honesty and malice are designed. When the honest value of a node is greater than the malicious value, the system considers that the node is honest, whereas the node is malicious and needs to revoke its identity certificate. After initializing the reputation value, the node can independently choose to service the requester according to the service requirements and rewards published by the service requester on the network. After the task is completed, the requester evaluates the service effect and sends corresponding reputation rewards according to the evaluation results. The better the service effect, the higher the reward of honesty and credibility. When the node has malicious behavior, the system will increase the malicious reputation value of the node according to the evaluation of the requester. If the malicious reputation value of a node is greater than the honest reputation value, it will be defined as a malicious node, and the system will revoke its certificate. This reputation value incentive method can make more nodes willing to participate in the learning process to obtain higher benefits.

However, the reputation value of the vehicle cannot directly bring immediate benefits to the vehicle. In terms of immediate benefits, the author of Ref. [100] uses resource coins as a reward mechanism, and uses contract theory based methods to distribute them to vehicles. The higher the quality of computing resources provided by the vehicles, the more resource coins will be obtained. In addition, in the process of resource transaction, this work proposes a blockchain-enabled vehicle computing resource transaction scheme based on edge computing, which is used to improve the legitimacy of the transaction. In the construction of the blockchain, the author uses RSU as the miner's node to participate in the creation and maintenance of the blockchain, where the consensus uses the PoW consensus algorithm. In addition, to prevent resource waste caused by the use of some resources to calculate income in the process of block creation, gradient descent algorithm is used to optimize the income calculation function to find the optimal resource management scheme. The simulation experiment constructs a network of 10 vehicles, and analyzes the relationship between rewards and resources, which proves the effectiveness of this method.

Compared with the reward problem considered in [99,100], the vehicle may prefer its privacy not to be disclosed. Privacy disclosure will lead to many vehicles unwilling to join the network, and ultimately lead to low participation of intelligent vehicles in resource sharing, which will reduce the source of IoV resource acquisition and lead to incomplete network coverage. Therefore, how to improve the participation of intelligent vehicles needs to be discussed. The author of Ref. [101] adds blockchain to privacy protection to ensure that location privacy is not disclosed. At the same time, the work designed an incentive scheme to encourage more vehicles to participate in the network through credibility and virtual currency. The higher the credibility, the higher the priority will be in the spectrum allocation process. This mechanism uses integrity as an incentive for users to design a reward and punishment mechanism, and updates users' integrity according to user behavior and evaluation algorithm. In addition, the scheme also designs rewards and punishments for income and deposits. Users who participate in the construction of anonymous zones will be rewarded with revenue, which is determined by user operation and legitimacy. In the margin reward and punishment strategy, the higher the credibility, the less the user's margin. Once the user violates the rules, the deposit will be released to the victim's account as compensation. The author combines three incentive mechanisms to effectively stimulate the participation of vehicles. In the experiment, users who actively share idle spectrum, occasionally share spectrum and never analyze spectrum are initialized to 20%, 60% and 20% respectively. Then it compares the user participation with and without incentive mechanism. The results show that after the use of incentive mechanism, user participation has increased from 0.3 to 0.5 to 0.7–0.9, increasing by 0.4.

However, in the era of advocating the concept of green travel, more and more EVs are replacing traditional cars. How to allocate electric power resources of EVs and how to safely buy and sell electric power have become a challenge. On the one hand, resource payers may refuse to trade and refuse to pay rewards. In addition, resource collection may

be dishonest in the transaction process, and resources may not be provided as promised. The industry has carried out the following work in the direction of EV resource trading:

The author of Ref. [102] designs a PoW consensus mechanism for EV energy trading based on Practical Byzantine fault Tolerance (PBFT), and used the stackelberg game model to stimulate honest node. This method first clusters cars, and cluster heads collect buyer information and broadcast it to the blockchain. Then the consensus mechanism based on Pow is available for the verifier to choose. Finally, in the transaction phase, the seller first publishes the price as the leader, and then the final price is determined by the stackelberg game model.

The author of Ref. [103] introduces an EV energy trading model based on p2p. This model uses Hyperledger fabric to build a blockchain network and complete the entire transaction process through smart contracts. The model will collect quotations every hour and generate a weighted bipartite graph according to user roles and needs. Then the improved Kuhn Munkres algorithm is used for matching and verification. Finally, the price is determined by game theory to maximize the interests of both parties.

However, there are not only EVs that need to be charged, but also EVs with surplus power resources in the trading market. To solve the problem of how to efficiently use all resources in the trading market, the author of Ref. [104] proposes a P2P power resource trading and payment system based on blockchain, which aims to prevent EV power waste in trading market. This scheme allows users with excess power resources to sell resources to charging stations, which provide resources for vehicles to be charged. Each node makes payment through electronic wallet. This process is automatically carried out by the smart contract, and the credibility of the entire transaction process is guaranteed by the blockchain. The system divides node into three categories: EVs, charging stations and prosumer. Node functions are shown in Figure 8. EVs equipped with renewable energy systems can serve as resource producers to provide power resources for charging stations. All nodes have their own electronic wallet accounts on the blockchain. After the resources are provided or the charging is completed, the vehicle will use the electronic wallet to pay automatically through the smart contract. All consumption records are uploaded to the blockchain for retention. The transparent blockchain ledger allows anyone to query records, which has a good defensive effect on dual payment and denial.

Nevertheless, everyone's query of the blockchain may cause problems such as privacy disclosure. Based on this question, the author of Ref. [105] fully considers user privacy and designs a charging platform EVChain. The platform introduces blockchain to share charging points, and use local blocks to manage sharing activities. The local block contains the main title and credit title. The credit title contains device management parameter, security parameter, charge management field parameter, charging trigger function parameter and threshold parameter. The specific functions are shown in the table. EVChain defines two types of transactions as peer to server and peer to peer separately. The user's client ID is used as a public key to protect customer privacy. At the same time, sub blockchain networks are used to create information sharing pools so that members can share ledgers.

Table 3 summarizes the research directions and applications of papers related to resource sharing.

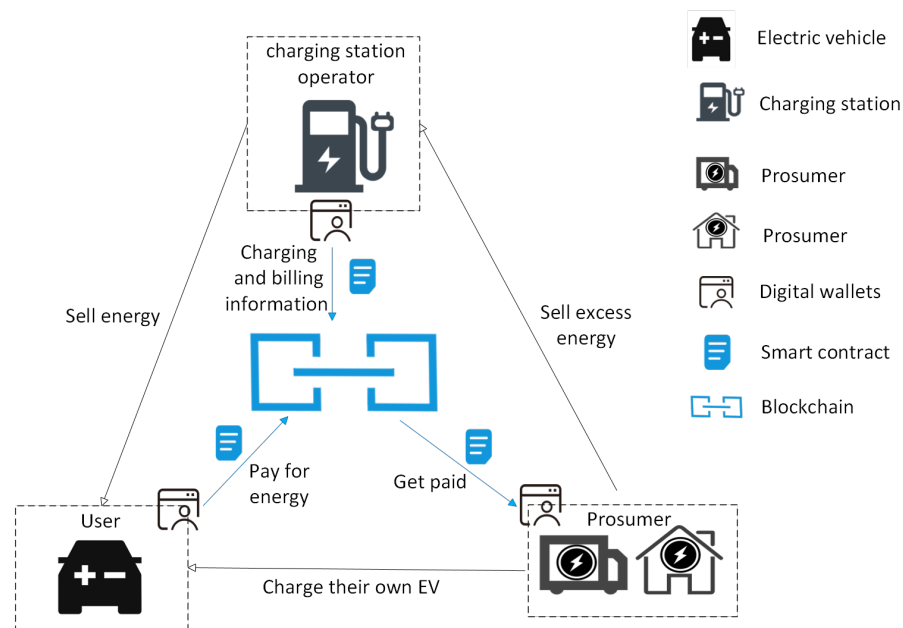


Figure 8. The working procedures of the blockchain-based p2p energy trading and charging payment system proposed in [104].

Table 3. Resource Sharing Related Papers.

Papers	Focused Challenges	Short Descriptions	How Blockchain Brings Opportunities
[95] [96] [97]	The problem of resource sharing.	<ol style="list-style-type: none"> 1. Build a consortium blockchain based on vehicle location and resource availability. 2. Effective use of stationary vehicles to share additional resources for the system. 	<ol style="list-style-type: none"> 1. The consortium blockchain can provide non-tamperable and verifiable services, and vehicles can share redundant resources through the consortium blockchain. 2. Link stationary vehicles with the system through the blockchain, so that a large number of resources of stationary vehicles can participate in the system to achieve the purpose of resource sharing.
[98] [99] [100]	How to incentivize vehicles to participate in sharing.	Vehicles are incentivized by rewards so they can participate more in sharing. In addition, the protection of vehicle privacy enables vehicles to be shared with confidence.	Blockchain is used to build digital currency to reward vehicles, and to protect vehicle privacy according to integrity.
[101] [102] [103] [104]	EV's Power Resource Trading.	An electric vehicle power resource trading system is constructed, using blockchain to build a vehicle electronic wallet, and using smart contracts to automate the power resource transaction process.	The non-repudiation and attack traceability of the blockchain help the construction of the trading platform to ensure the security of the transaction process.

4.3. Trust Management

In the process of data management and resource management, vehicle and vehicle, vehicle and RSU and other entities do not trust each other. How to make the entities that do not trust each other jointly build a network and carry out work related to interests on the network is another aspect that IoV needs to consider.

Trust management needs to decide whether to interact with an entity based on its credibility. The method of evaluating the entity's credibility is called trust management. In the IoV environment, when the vehicle receives information from other entities, it needs

to verify the credibility of the entire information, including entity trust and content trust. Trust management plays a key role in defending against network attacks. For example, the emergency control system needs to quickly decide whether to brake when a traffic accident occurs nearby. When the system receives the emergency information transmitted by other vehicles, it needs to use trust management to evaluate the credibility of the sending node and the credibility of the content sent by the node, and judge the correctness of the information and whether it comes from a malicious node. In this delay sensitive situation, the trust management system needs to immediately evaluate the trust of the source and message. Once the system is evaluated as a credible message, the emergency control system needs to immediately take corresponding measures such as emergency braking. If the send node is judged by the trust evaluation system to be a malicious node or a false message sent by a node, the message will be ignored and the trust value of the node will be reduced.

At present, many researches have considered trust management methods. However, the high-speed mobility of IoV node will lead to frequent changes in network topology, which requires that the trust management system has the ability to quickly evaluate the trust value of new node. Traditional methods can only establish trust and update trust values when the network node remain unchanged, but they cannot quickly establish different trust networks. At the same time, the vehicle will encounter a large number of other vehicles that have never met. The trust management system needs to immediately evaluate the trust of this node when meeting for the first time. Therefore, it is necessary for a trust management network to manage the global trust value.

Trust management is very important for IoV. Blockchain can effectively solve problems in trust management system. The decentralized feature of the blockchain can ensure that all nodes participate in the calculation and recording of global trust, which eliminates the dependence of the central trusted authority (TA), and ensures that when one or more node fail, other node can work normally without being affected. At the same time, the blockchain's tamper resistance can ensure that the stored trust data will not be changed by malicious node, which can ensure the credibility of the trust values stored on the blockchain. Finally, the transparency of the blockchain enables node to quickly obtain the trust records of other node when needed.

Trust management is mainly divided into the trust of entity and the trust of content.

4.3.1. The Trust of Entity

Entity trust refers to that the vehicle needs to check whether the identity information of the sender is legal, whether the sender can trust other node, and whether node and node disagree with each other's identities, which is also called node trust. In IoV, data is transmitted between vehicles on a large scale, and both the sender and receiver need to confirm whether the data source is reliable and should be trusted.

The author of Ref. [106] introduces blockchain into IoV for entity trust management. They uses the CA to register or revoke the vehicle certification, which can establish a trust link and transfer data between entities that do not trust each other. They has designed the DrivMan scheme to establish a credible data source without disclosing vehicle privacy in VANET. First, vehicles submit a registration application, and DrivMan checks its legitimacy, and uses the PKI to generate a unique encrypted fingerprint for legitimate users. The encrypted fingerprint is sent to the vehicle through the CA, and the trusted data source database will be established. The data submitted by vehicles in the blockchain cannot be changed at will. Once a malicious vehicle attacks the network, CA can immediately track the vehicle fingerprint to identify and log off the vehicle. The vehicle can then transmit data in the network. During transmission, DrivMan determines whether the user is legal by checking whether the certificate is in the trusted database. The DrivMan solution does not require the data upload and download parties to mutually confirm their identities. Even if both parties do not trust each other, they can still establish a trusted connection and share

data, and protect the privacy of both parties by not directly authenticating. However, this method requires the participation of a third-party certificate authority.

In order to eliminate the possible single point attacks and other problems of third-party organizations, the author of Ref. [107] proposes a scheme based on reputation. To avoid the distrust between entity node, the scheme uses blockchain to establish trusted connections between untrusted node. In this scheme, the blockchain is responsible for building trust between node and node, and between node and the cloud. After the local model is updated, it communicates with the cloud to update the global model. This process is completed by the blockchain, which not only ensures the credibility of data, but also establishes a trusted connection between untrusted clouds and node. On this basis, the author also uses reputation rewards to ensure the honesty of node and make node more credible. The honesty of node will also be recorded in the blockchain to ensure that dishonest node cannot change their reputation values.

On the basis of [107], the author of Ref. [108] considers that it is difficult to quickly establish trust with other vehicles due to the high speed of vehicle movement, fast state change and difficulty in tracking. In addition, when the vehicle is connected to the RSU, the vehicle does not fully trust the RSU, so the RSU is semi trusted. Therefore, based on the problem that trust data is not synchronized in time, the author proposes a trust management system based on blockchain to synchronize trust data while ensuring data authenticity. The scheme is shown in Figure 9. The author deployed blockchain on RSU. RSU is responsible for calculating the reputation of the vehicle and writing the vehicle information and its reputation value into the blockchain. This process cannot be tampered with, so the vehicle reputation value is permanently trusted, which solves the problem of trust between vehicles. Furthermore, to solve the semi trusted problem of RSU, the system also uses joint PoW and PBFT in the consensus mechanism to improve the credibility of RSU. The author resists four kinds of security (authenticity, integrity, anonymity, and non connectivity) and five kinds of attacks (Resistance of Replay Attack, Resistance of Man in Middle Attack, Prevention of Message Spoofing Attack, Defense of Bad Mouthing and Ballot Stuffing Attack, Resiliency Agency Compelled RSU) to prove the effectiveness of the proposed scheme. Experiments show that when other node oppose a node at 30%, 50% and 80% respectively, node reputation will increase, remain unchanged and decline. The reputation value of dishonest node will decrease over time. Therefore, the proposed scheme is effective. Finally, this paper also conducts relevant research on the trust of EVs.

The author of Ref. [109] proposes a trust mechanism for EV charging piles based on double-layer blockchain. This mechanism combines the subjective evaluation of users with the objective evaluation of charging piles, and finally calculates the reputation of EV. Simultaneously, to improve the consensus efficiency of the blockchain, this paper introduces the reputation mechanism into the consensus, and proposes a method combining route and consensus to determine the bookkeeping right. This method consists of multiple charging station (CS). CS is divided into server and client. The CS local server stores the user's evaluation of CS. The blockchain is divided into lower chain and upper chain. Lower chain is divided by region, and all CS servers in the region constitute lower chain. Lower chain is responsible for storing the hash value of evaluation content. All the lower chains of all regions form the upper chain. The block identification, CS information and identity information of the lower chain are stored in the uplink. The transaction process is as follows: (1) The BTS integrates all information and transmits the information to the lower chain. (2) Lower chains calculate score data. (3) The scoring data is broadcast to the lower level node for verification, and if it passes the verification, it will be uploaded to the lower chain. (4) The upper chain consensus node extracts data and calculates credibility. (5) The calculation results are broadcast to the upper chain for verification. If verified, the system updates the blockchain. By combining subjective and objective evaluations, the scheme finally forms EV reputation value, which improves consensus efficiency and increases the trust between node.

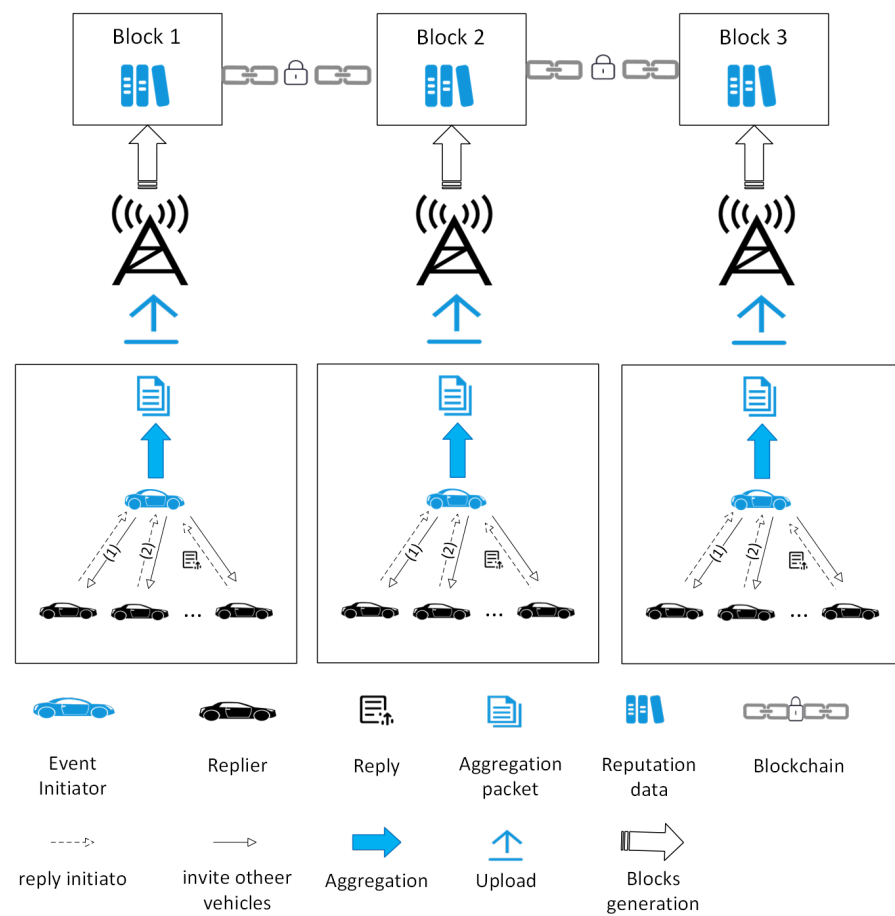


Figure 9. Structure of Privacy-Preserving Announcement Protocol With Blockchain-Based Trust Management proposed in [108].

4.3.2. The Trust of Content

After the entity credibility is confirmed, the credibility of the content sent by the entity also needs to be evaluated. Even if the vehicle confirms that the identity of other entities is trusted, the information sent by the trusted node may still be biased due to time, location and other factors. In addition, if a trusted node is attacked by a malicious node, it will also send bad information for the network when its identity is trusted.

In a large-scale IoV network, achieving mutual trust among all nodes require large communication and computing overhead, so it is impossible to achieve full trust in the network. For how to make vehicles fully trust the data transferred from untrusted vehicles, the author of Ref. [110] proposes a data reputation management scheme based on blockchain. This scheme calculates the accuracy of the uploaded information by combining the basic information of vehicles, reliability scores, vehicle traffic data and other information in the blockchain. If the vehicle uploads an error message, the reliability score of the vehicle will be reduced. If the reliability score is low, the system revokes the vehicle's authentication certificate, and the vehicle will not be allowed to exist in the network. In the process of consensus, the author improved the PBFT protocol and jointly decided the right to create blocks in combination with Proof of Trust (PoT). The author simulates 50,000 data generated by 2000 vehicles. The data allocated for training, verification and testing are 35,000, 7500 and 7500, respectively. The model converges when the training sample is 4000, and the accuracy rate of the model rises from 51.61% to 70% when the sample rises from 100 to 4000. In this proposal, if there is a dispute, it needs to be reviewed manually. At present, the system cannot be fully automated.

The author of Ref. [111] designs an automated trust mechanism, which is committed to solving the trust problem of message transmission between untrusted vehicles in IoV. The

author proposes a message trust evaluation mechanism based on the alliance blockchain. The vehicle judges the credibility of messages sent by other nodes through reputation rating. Credit rating is completed on the blockchain. The message provider will send messages periodically, and the message evaluator will rate the messages through the threshold. For example, the author believes that in traffic accidents, the messages sent by the nodes in the accident center are the most reliable. The closer the other node are to the accident center, the more reliable the messages they send. On this basis, smart contracts are used to automate the entire process. Smart contracts can automatically reward vehicles through vehicle contributions, which effectively encourages the participation of vehicles. The system eliminates the dependence of the centralized system on the central node and the third-party node. It provides a distributed message trust management mode for the IoV network, and the blockchain can ensure that the credibility has not been changed.

Inspired by the traffic accident examples mentioned in [111], the author of Ref. [112] focuses on how to efficiently store accident evidence in traffic accidents. To solve the problem of how IoV with edge server can efficiently transmit data between node, the author combines blockchain with the IoV edge service architecture based on machine learning (ML). This scheme uses decentralized trust algorithm to ensure that nodes fully trust the message content transmitted in the network, and reduces network delay and resource waste by reducing node verification time. This proposal designs a trust algorithm to confirm the necessity of data transferred between edge servers. If the result of algorithm verification is necessary, the transaction will be written into the blockchain. In addition, the consensus mechanism uses a consensus algorithm and PBFT to ensure the accuracy of the block writing process. The experiment compares the transaction approval delay of traditional algorithms. The traditional method has a maximum delay of 88.6786 s and a minimum delay of 2.8758 s, while the system delay proposed by the author is only 0.7184 s. However, this scheme only considers the necessity of data transmission, and does not verify the accuracy of data.

To verify the accuracy of data, authors of Ref. [113] introduce a trusted verification scheme based on blockchain. This scheme uses the characteristics of the blockchain, such as tamper proof, decentralization and traceability, and uses the blockchain as an intermediate verification platform for intelligent connected vehicle and edge node to ensure the correctness of the delivered content. The system designs a method to store interactive evidence. After receiving the message, the device will apply to the blockchain for verification services, mainly to verify the legitimacy and security of the message. Since the blockchain is tamper proof, the verified data has not been replaced or illegally tampered with, so the transmitted content can be fully trusted. On this basis, the message is encrypted by using off chain integrity and on chain hash, and authenticated by the digital certificate of the blockchain, which fully guarantees the security of the message. In addition, in terms of user privacy, the system also uses blind signature technology. Users request services anonymously to ensure the hiding of users' real information.

The above methods consider how to confirm the message content. In contrast, the author of Ref. [89] focuses on the information transmission process. If the delivery platform is trusted, the information is trusted. Aiming at the trust problem of data transferred in vehicles in IoV, the author proposes an on chain and off chain solution to split smart contract computing work. In short, it is to put the work with high trust requirements under the trusted chain to complete the calculation to ensure the credibility of the data. The system consists of a trusted platform and a blockchain platform. The public data is calculated by the blockchain, and the credibility of the data is guaranteed by the miners through the consensus mechanism. In addition, the computing work requiring higher trust is calculated by the trusted platform off the chain. The trusted platform ensures the security of the computing process and the accuracy of the data through the trusted execution environment, thus improving the credibility of the information.

Table 4 summarizes the research directions and applications of papers related to trust management.

Table 4. Trust Management Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[106] [107] [108] [109]	How to trust each other between nodes.	Use CAs to connect untrusted entities. Node credibility is determined by reputation value or evaluation.	The blockchain is used for registration, and the reputation of nodes is stored in the blockchain, so that untrusted entities can build trusted connections through the reputation on the blockchain.
[110] [111] [112] [113] [89]	How to determine whether the content transmitted between nodes is credible.	<ol style="list-style-type: none"> 1. Evaluate the credibility of the content transferred between nodes to determine the credibility of the content. 2. Protect the channel for nodes to transmit information. If the channel is credible, the content is credible. 	<ol style="list-style-type: none"> 1. Build a reputation evaluation mechanism by the blockchain. Since the blockchain cannot be changed, the reputation of the content will not be changed, thus ensuring that the content is credible. 2. Blockchain is used to build an information delivery platform to ensure the credibility of the delivery.

4.4. Security Management

Although many works focus on trust management, ensuring the security of each node is the basis of trust management. Aiming at the IoV network security issues, this article introduces the following aspects.

4.4.1. Identity Authentication

Some researchers authenticate entities based on trusted institutions. Since IoV is that most networks are vehicle ad hoc networks, which are self-organizing and open networks, they are more vulnerable to malicious attacks. The attacker's favorite is to steal vehicle privacy. In order to prevent malicious attacks in IoV, it is necessary to authenticate nodes. Identity authentication is an effective means of preventing attacks. The blockchain is introduced into identity authentication, and the traceability and non-tamperability of the blockchain can be used for effective identity authentication.

The author of Ref. [114] proposes a blockchain-assisted vehicle identity authentication scheme. The scheme mainly consists of trust agencies, RSUs, trusted nodes and vehicles. Trust agencies are responsible for storing vehicle privacy and issuing identity certificates, and tracking malicious nodes when needed. RSU is responsible for mobile phone traffic information (identity, location, etc.). Trusted nodes have the right to write to the blockchain and to record transactions in the network. Vehicles cannot join the network until their identities are registered with a TA. In registration, the author uses a hybrid identity code verification method to hide the real identity of the vehicle to achieve anonymous vehicle authentication. This scheme verifies the identity of the vehicle through RSU and broadcasts it, and the trusted node writes the identity verification result into the blockchain to achieve the purpose of identification. Simultaneously, aim to reduce the authentication delay, the author proposes a time-windowed task processing algorithm to improve the utilization of idle resources.

The author of Ref. [115] provides a blockchain-based scheme for vehicle identity authentication in IoV, which aims to use blockchain to manage and store identity authentication information to ensure vehicle security and privacy. The scheme is improved on the basis of Ethereum, and digital signatures are used to ensure the privacy and data accuracy of vehicles. When a node wishes to join the network, it needs to register identity information with a trusted organization for subsequent identity authentication before transactions. The blockchain encrypts node identities based on digital signatures and stores node registration information in a distributed manner. When a node receives data transmitted by other nodes, it needs to request identity verification from the blockchain to ensure the

legitimacy of the data source. In addition, in order to make better use of communication resources, the author divides the transmitted data into emergency data and non-emergency data, and divides the IoV network into emergency network and non-emergency network. The emergency network is used to transmit emergency data without being affected by other non-emergency data. The system processes emergency data first and uses the remaining resources to process non-emergency data. This method of prioritizing data can improve resource utilization.

However, the identity authentication of vehicles in the above two papers relies on trusted institutions. Once the trusted institution is attacked, the authentication mechanism will no longer be available. For this problem,

The author of Ref. [116] proposes to use edge computing to eliminate the centralization of trusted institutions. To prevent the information leakage and tampering caused by wireless communication of each node (vehicle, RSU, edge server) in IoV, the author proposes a blockchain-assisted vehicle network edge server registration and authentication platform. The platform ensures the authenticity of the vehicle identity by registering the vehicle and RSU with the edge server. The authors divide edge servers into primary and secondary servers, and the platform determines authentication venues through different levels of trust. For vehicles with successful identity verification, the edge server must follow the same consensus to write the vehicle into the blockchain, where PBFT is used to provide consensus for the network. The author's experiments on the Raspberry Pi prove that the authentication delay of the platform is 66%, and the communication overhead is 49%, which is better than the traditional method. However, this method does not consider the problem of malicious node attacks.

The author of Ref. [117] in order to solve the problem that malicious nodes may forge and steal identities in edge IoV entity authentication, the author focuses on developing a blockchain-based IoV entity identity authentication scheme. Here, the blockchain is selected as the consortium blockchain. In the beginning, the author transfers the entity's authentication data from the cloud to the blockchain according to the immutability of the blockchain. Edge nodes do not need to access the cloud during authentication, but only need to make a request to the blockchain, which can reduce access paths and communicate quickly. Next, the author adopts the method of key agreement to enable independent sessions between entities to protect vehicle privacy and sensitive data. Finally, the author simulates the proposed system experimentally. In 50 identity authentication tests, the system has achieved good results in terms of delay and communication overhead. The above two schemes only describe the mutual authentication between vehicles, ignoring the overall inefficiency that may be brought about by complex consensus algorithms, and the existing schemes cannot balance the security and efficiency.

The author of Ref. [118] fully considers the problem of authentication efficiency in the authentication system, and for the authentication problem in IoV, proposed a high security IoV authentication strategy using blockchain, which uses blockchain to authenticate members in the network. The distributed structure based on blockchain can prevent the problem of single point of failure and relieve the resource tension of the central server. The process is divided into three stages: initialization, registration and authentication. The blockchain is constructed and maintained by RSU. RSU is responsible for verifying the information of the vehicle during the registration phase. After the verification is passed, the vehicle is written into the blockchain using consensus. On consensus, the authors improved PBFT. Traditional PBFT works better in static networks because it takes up too many communication resources. However, in IoV, moving vehicles form a dynamic network, so the author designed the SG-PBF algorithm to improve the consensus efficiency in the dynamic network. Experiments show that when the number of nodes reaches 1000, the delay of the consensus algorithm is 27% of the traditional method, and the algorithm overhead is reduced by 60% at most.

However, the above-mentioned blockchain vehicle identity authentication methods all require the verifier to perform identity authentication through a smart contract. Identity

authentication will generate a large number of certificates, and the process of generating certificates is computationally expensive. In addition, the storage and management of certificates also consume many resources, which increases the processing time. Once the identity of the node is leaked, the authentication security will also be reduced. The author of Ref. [119,120] propose certificateless identity authentication schemes, respectively. In paper [119], author proposes a blockchain-based cross-domain certificateless anonymous authentication scheme. To prevent repeated verification caused by frequent replacement of RSUs by mobile vehicles, this scheme hands over the verification of the vehicle to the first RSU that the vehicle passes through, and uploads it to the blockchain after the verification is passed. The blockchain guarantees the uniqueness and invariance of the certification. Therefore, when the vehicle passes by other RSUs, it only needs to query the corresponding evidence in the blockchain without re-verification, which reduces communication and saves network costs. In authentication, the private key of the vehicle is formed by combining a pseudonym issued by a trusted institution and a part of the private key generated by the Key Generation Center (KGC). Since the process does not generate certificates, it saves certificate storage and management overhead.

The author of Ref. [120] proposes an authentication protocol-PBAG that does not need to query the certificate in the blockchain. The framework uses global commitments for identity authentication through bilinear pairing, and is divided into three layers. The bottom layer is composed of vehicles and RSUs, which are responsible for communication. The middle layer is jointly created and maintained by Trust Registration Authority (TRA) and RA for the purpose of validating vehicles and RSUs. The top layer is responsible for the registration of vehicles. The keys owned by the RA are offline, so there is no fear of key loss. Vehicles achieve high-speed security authentication through different authentication methods for trusted/semi-trusted entities and untrusted entities. In addition, the article utilizes smart contracts in key update and revocation, which reduces the delay. The system updates the key if it still wants to maintain the network connection after the vehicle key expires. When the vehicle wants to leave the network or the key is lost or the certificate expires, the system will revoke the vehicle key. Experiments prove that the average verification time of this authentication method is 0.36 ms, the authentication delay is reduced by 33.8%, and the loss rate is less than 9.6%.

In [114–120], the identity verification method is that RSU communicates with the vehicle as a reputation authority. However, due to the fast moving speed and heavy traffic volume of vehicles, the RSU may have no time to authenticate during the verification process, or too many authentication messages may cause network congestion. The author of Ref. [121] in order to solve the above problems of IoV centralized authentication, blockchain is introduced into IoV, and game theory is added for authentication to ensure the security of IoV. As shown in Figure 10, the author proposes a three-tier IoV identity authentication structure based on blockchain and game theory, which uses two blockchain networks. The first is the infrastructure layer. This layer is composed of intelligent devices and vehicles. These nodes communicate with the RSUs of the second layer. All RSUs form the first blockchain Network—local blockchain, which is a local private blockchain. Finally, the RSU transmits the data to the third layer—the cloud. The cloud here is not a centralized single point cloud, but a second Global blockchain network composed of multiple independent clouds. Such a distributed design is decentralized, which can effectively avoid the problems caused by the centralized structure.

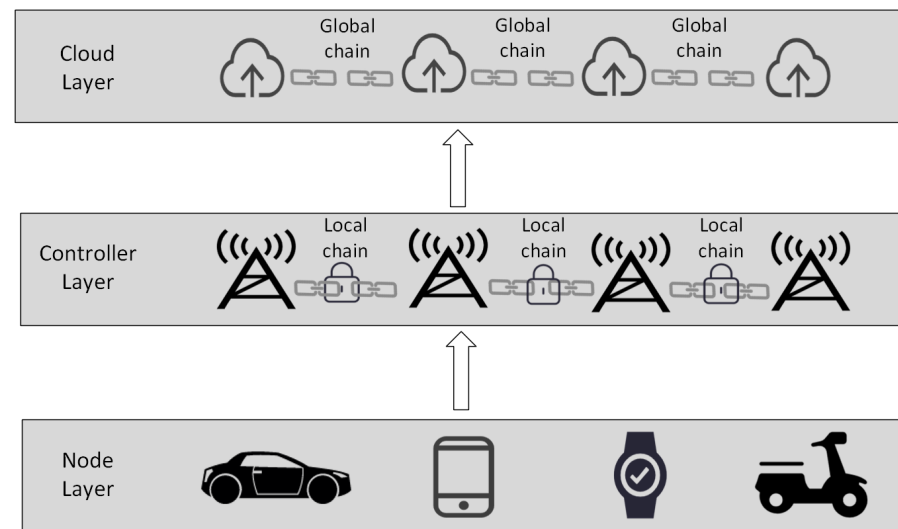


Figure 10. 3-layer structure of Game Theory-Based Authentication Framework to Secure Internet of Vehicles with Blockchain in [121].

It also uses a double-layer blockchain to build an identity authentication system, and author of Ref. [122] pays more attention to the reputation of vehicles. The authors introduce blockchain into a cloud-based IoV system. Blockchain is used to manage vehicle reputation. The smart contract is deployed on the blockchain to automatically calculate the reputation value and encrypt it. Finally, the blockchain performs identity authentication and allocation according to the vehicle reputation value. The scheme designs two private blockchains (authorization chain and identity chain) and divides the IoV system into three layers. Among them, the vehicle, RSU and watchdog (trusted entity) belong to the vehicle network layer. The fog layer is deployed on those nodes in the area that are assigned authorized authority, and these nodes maintain the blockchain and smart contracts. Finally, there is the cloud layer. The cloud platform is built by nodes with RA identities in each region. The cloud platform has functions such as registration, identity verification and reputation update, and the identity information is stored in the identity information blockchain. Simulation experiments show that the scheme uses blockchain for data transmission and storage to make the system more secure. In addition, the system intelligently analyzes the reputation value in an encrypted manner while ensuring that the privacy of the vehicle is not leaked, and assigns identities with different permissions to nodes according to the reputation value.

In paper [123], IoV network is not only the connection between vehicle and pedestrian and RSU. With the development of UAV technology, some researchers have started to design ground-to-air network in recent years. As a new type of transportation, UAV play a new role in IoV and bring new opportunities for IoV. In order to solve the problem of communication security and identity verification between IoT devices and UAV, the author proposes a consensus mechanism for identity verification based on blockchain. The mechanism is divided into two stages: user registration and authentication. The first is user registration. At this stage, the UAV acts as an intermediate node to connect the user to the nearest MEC server. The UAV receives the identity sent by the user. Then user collects environmental data and sends it to UAV. The UAV decrypts the data with Bloom filter. By the way, the validity needs to be verified by UAV, and the UAV forwards it to the MEC server. After the MEC server receives the user identity, it checks the validity. After the user is proved to be valid, MEC calculates the user's aid through the user's information. Next is authentication. MEC verifies whether the user's uid is legal. If the identity is invalid, the data will be discarded. If the user with this id continues to send data, the data will be blocked by the UAV. If the identity is valid, the aid will be sent to users through UAV,

and the users will communicate with each other using aid. After all users have obtained their aid, UAV creates a blockchain and adds all legitimate users to the chain. When MEC receives the information, it can check the legitimacy of the user through the blockchain. If the user is legal, the information sent by the user will be broadcast to the blockchain.

Table 5 summarizes the research directions and applications of papers related to identity management.

Table 5. Identity Management Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[114] [115]	How to authenticate.	A third-party trusted organization authenticates the identity of the vehicle and RSU.	The blockchain manages and stores the vehicle's identity information.
[116] [117] [118]	How to eliminate dependence on Third-Party CA.	Vehicles are certified by smart contracts instead of third-party CA.	Smart contracts in the blockchain are used to automate authentication, and the blockchain is also used to store vehicle identity.
[119] [120]	How to reduce certificate generation and ensure authentication efficiency.	A certificateless management scheme is proposed, which uses keys to manage node identities.	RSU is responsible for identity verification, issuing a key for vehicle registration, and the key confirms the identity of the vehicle.
[121] [122] [123]	How to reduce the dependence on RSU in the authentication process in dynamic IOV.	An identity verification platform is built using a double-layer blockchain approach.	By building a two-layer blockchain network, storing identity information in the cloud, or decoupling registration and authorization, the system's dependence on RSU authentication can be reduced.

4.4.2. Communication Security

Communication security is the basis for ensuring the correct delivery of information. After ensuring the identity information of the vehicle, the communication security between vehicles also needs to be considered.

The author of Ref. [124] aims to solve security issues such as the openness of the IoV network and its vulnerability to attacks, a blockchain-based certificateless key agreement protocol; therefore, Block CLAP is proposed. This protocol is mainly used to enable the nodes of each layer in the vehicle network to build a secure network communication. The protocol establishes verified key management in the three communication networks of vehicle cluster head and RSU, adjacent vehicle cluster, and RSU and cloud. The vehicle transmits the collected data to the RSU, and the RSU transmits it to the cloud. Cloud server will create block and construct transactions. At the same time, the leader selects the consensus node by executing the formula algorithm based on voting, and the consensus node writes the block into the blockchain. Specifically, there is no unique trusted RA in the system, and there is a trusted RA in each vehicle ad hoc network. The scheme analyzes the security of the protocol through the Real-Or-Random (ROR) model. At the same time, it also conducts an attack test on the system. In seven kinds of attacks (Replay Attack, Man-in-The-Middle Attack, Impersonation Attack, Privileged-Insider Attack, Denial-of-Service (DoS) Attack, Physical Vehicle Capture Attack and Ephemeral Secret Leakage (ESL) Attack) tests, the system showed good performance. However, this system increases resource overhead.

In order to reduce system overhead, the author of Ref. [125] chooses a lightweight method to ensure communication security. The article discusses the security limitations of current centralized IoV networks. In most cases, the centralized network cannot handle single point of failure, and the traditional IoV network cannot guarantee the security of

communication and the security of privacy in the high autonomy vehicle environment. In addition, the limited computing and storage resources also challenge the traditional network. To solve the above problems, the author proposes a lightweight blockchain security protocol based on secure communication. The author chooses the blockchain with the required permissions and the improved PBFT to build a blockchain-based IoV network, and ensures the security of communication by ensuring that the data has not been tampered with and the attack is traceable through the permissioned blockchain. At the same time, the scheme combines two cryptographic functions of Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA256) to ensure the safe transmission of messages. By calculating the communication cost, energy consumption, calculation cost and storage cost, the protocol reduces by 85%, 55%, 55% and 90%, respectively. In addition, the author also made six tests for the proposal, including identification of Identification Theft, Message Integrity, Sybil Attack, Message Replay Attack, Botnet Attack, Man-in-The-Middle Attack, which proved the security of the protocol. The communication channel in this scheme lacks security.

In paper [126], the communication environment of traditional IoV is open, and the communication of this open network is vulnerable to attack. To ensure the security of communication, the author proposes an vehicle anonymous key exchange mechanism based on blockchain. First, send the message to the cluster head. Then a private session channel is established for parties who need to communicate, and a key is set. The key is sent to the vehicles. The vehicle carries the key and sends the request to the cloud through the RSU. Cloud organizes the messages from the RSU and stores them in the blockchain as transactions, and the process of adding blocks is determined by a voting-based formula method. Note that the identity of the algorithm is irrevocable, even for malicious nodes. The scheme proposed in [127] cancels the identity of malicious nodes.

The purpose of [127] is also to establish a secure communication channel in IoV to ensure safe communication between vehicles. Secure communication is realized by identity authentication. During construction, the most important thing is how to ensure efficient authentication while preventing vehicle privacy from being violated. Based on this problem, the author proposes a blockchain-based IoV communication protocol. The protocol uses certificateless signcryption for key management. This signature method overcomes a series of problems caused by key escrow, and at the same time reduces certificate management consumption, saves resources, and finally efficiently authenticates identity. The structure of the blockchain is P2P, which uses node-to-node transmission to reduce network delay and realize real-time data auditing. In addition, smart contracts can automate the system, and transactions are undeniable, then malicious nodes will be discovered by the system and prevented from delivering malicious messages. To save computing resources between vehicles, scheme adopts online/offline signcryption method on the basis of blockchain. Compared with the existing scheme, the calculation cost of this scheme is reduced by 67.9–84.2%, and the total consumption is reduced by 62.3–75.4%.

The author of Ref. [128] builds IoV network by integrating digital twin technology on the basis of big data. In addition, for the problem of how to ensure the safe of communication in IoV, a blockchain-based IoV communication framework is designed, and the block chain can not be tampered with and traceable to realize the safe communication between vehicles. With the assistance of the blockchain, the vehicle's public key, historical communication and other data are stored in the blockchain and cannot be revoked. In addition, all nodes of the blockchain jointly maintain the network formed by vehicles to ensure communication security. In the blockchain of the proposed scheme, vehicles only store block headers to build a lightweight blockchain. In addition, a consensus is reached on the access results through a consensus mechanism and uploaded to the blockchain. However, this method does not fully consider privacy issues.

A scheme to protect individual privacy is proposed in [129]. The author believes that although Iov with MEC can increase computing power of mobile vehicles and reduce delays, how to ensure data security and individual privacy during data transmission

from vehicles to edge nodes is a problem. To solve this problem, the author integrates blockchain into IoV to ensure data security and privacy. The role of blockchain is to ensure the authenticity of billing, and to find a suitable MEC server for the consensus nodes to handle computing tasks. Among them, the consensus algorithm is PBFT. In addition, both blockchain and MEC are decentralized distributed system structures, and MEC can calculate tasks generated in the blockchain, so the two can be better integrated. The network structure of this article is mainly divided into three parts: 1. Equipment layer: It consists of various vehicles and is covered by RSU. In addition, the RSU is responsible for forwarding those tasks of vehicle unloading to the BS, and there are multiple RSUs within the range of one BS. 2. Edge layer: The edge layer is composed of BS, which is responsible for configuring the MEC server and computing tasks offloaded from the vehicle. At the same time, a blockchain is built at this layer, and BS also acts as a blockchain node to verify and account transaction. 3. cloud layer: it is mainly responsible for providing resources for building blockchain, including data such as consensus and records. The throughput test experiments of different block sizes and different transaction sizes show that the network construction using blockchain can obviously handle more transactions when the block size increases.

The author of Ref. [130] on the basis of [129], considering that vehicles move at high speed in the IoV environment, it is a challenging problem how to safely build the communication between vehicles in the case of rapid changes in network topology. Based on this problem, the author proposes to apply blockchain to IoV, and use smart contract and consensus mechanism to ensure the communication security of the network. Blockchain and smart contract provide communication protection and privacy protection for the communication channel of the system. In terms of consensus, the author chooses PoA, which is faster than PoW, to select write nodes for the system. In addition, how vehicles efficiently utilize resources on the communication network in IoV is also one of the problems. The problem of task allocation can be well solved by integrating fog calculation into IoV. Fog computing also uses a distributed architecture, so it can better integrate with blockchain to jointly provide safe and efficient communication for vehicles. In addition, software-defined networking (SDN) is also used in the blockchain to separate the flat layer and the data layer to better manage the IoV network. The system divides the network structure into perception layer (vehicles, RSUs and other devices in the network), blockchain layer (providing secure communication between perception layer devices and fog layer), fog layer (calculating the data of perception layer in real time) and cloud layer (providing storage resources for big data and decision-making services for the system).

Moreover, to ensure the security of transmitted messages, Refs. [131,132] work as follows. For the transmission security of IoV, the author of Ref. [131] proposes a blockchain-based transmission framework—sIoVChain. The purpose of the framework is to securely share information between vehicles timely and store it in the blockchain. The main processes are registration, communication and ordering node selection. During registration, the vehicle and RSU establish a trust link, and only the nodes that have completed the registration can communicate. After the registration is completed is the communication phase. In the communication phase, it is necessary to establish a secure communication channel in the insecure public channel. First, the communication channel is established by devices and nodes, and the node uses the transaction verification algorithm to ensure the legitimacy before the transaction. Finally, there is the ordering node selection stage. In this stage, the ordering node is responsible for endorsing the transaction, and creating a block and uploading it to the blockchain. Ordering nodes are jointly determined based on throughput, response time and trust value. Experiments on the raspberry PI 4 platform show that sIoVchain is less than 50% of the verification delay, 50% of the encryption delay and 49% of the communication overhead of the traditional scheme. However, this method registers the device into only one node. First, the device cannot determine whether the registered node is trusted, which reduces the participation interest of the node. Secondly, once the node is malicious, it will cause losses to the system.

Consider the problem of single registered node in [131]. The author of Ref. [132] considered message security in large-scale IoV networks, especially the security of emergency messages, a double blockchain communication protocol is proposed. One chain is responsible for storing the identity information of vehicles. All vehicles need to be registered before joining the network. The registration process is completed by this chain. Another chain is responsible for storing emergency messages, analyzing the location of emergency messages, and publishing the location and messages to the IoV network. Especially to reduce the waste of blockchain storage resources, the author does not put the vehicle location information in the blockchain, but in the location database. The blockchain will not provide information unless there is an urgent message to find the location. This solution decouples identity information and traffic information, builds a lightweight blockchain, and achieves the purpose of secure message transmission.

Ground-to-air is also the development trend of IoV in recent years. The author of Ref. [133] proposes a blockchain-based distributed autonomous flight plan management system—UTM. The blockchain is introduced into the UAV system to ensure the security of network communication. The process is as follows: 1. The user sends a route reservation request to the UTM system. 2. UAVs communicate through the blockchain and establish a consensus on requests. 3. If the request is passed, it will be stored in the blockchain. If the request is rejected, the UAV will generate a new route through the existing information and confirm to the user whether the route is feasible.

Table 6 summarizes the research directions and applications of papers related to communication Security.

Table 6. communication Security Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[124] [125] [126] [127] [128] [129] [130]	Security Issues of Communication Channels in IOV.	Build a secure communication channel by blockchain and use anonymity to ensure network security.	The decentralized and distributed structure of the blockchain can ensure that the communication process is not affected by a single point of failure. In addition, immutability and transparency can ensure that the communication process is safe and reliable.
[131] [132] [133]	How to ensure the security of transmitted messages in IOV.	1. Ensure the accuracy of sources by registering. 2. Confirm the legitimacy of the request through consensus.	The registration and communication process is completed by the blockchain to ensure that the entire process is legal.

4.4.3. The Protection of Attack

The openness of the IoV network makes the communication between vehicles very fragile, which reduces the security and increases the probability of being attacked. How to avoid attacks has become the focus of discussion in the industry.

It can be found in identity authentication that most identity authentication systems tend to use trusted institutions as identity registration agencies. However, in the traditional vehicle authentication method based on a single TA, the authentication is performed on one TA. Once the TA is attacked, the system will crash. Therefore, in order to prevent damage to the system caused by single-point attacks, the author of Ref. [134] uses blockchain to build a TA platform. The blockchain stores the trust value of vehicles as the basis for secure and transparent exchange of messages between vehicles. The system consists of RSU, vehicles, messages and blockchain network. The blockchain is a public blockchain. The consensus algorithm adopts the PoW method. RSU needs to regularly upload the real-time trusted value of the vehicle to the blockchain to prevent the initially honest vehicle from becoming a malicious node as time goes by. Blockchain-based distributed storage of vehicle

reputation values can well prevent single-point attacks. However, this method is based on the reputation value. If the attack vehicle only executes one attack and does not care about its own reputation value, this method cannot prevent the attack very well.

Different from this method, to solve the problem of single credit institution and vulnerability to single point attack in the traditional blockchain-based IoV network, the author of [135] proposes a blockchain key management scheme based on multi credit institutions. As the only management organization for vehicle registration and key distribution, once the trusted organization is attacked, the whole system will collapse. The traditional IoV network based on blockchain usually has only one credit institution, which leads to the centralization of key management. This increases the computational and storage overhead. The most dangerous thing is that it is vulnerable to attack by malicious nodes, thus losing all information. To solve this problem, the author proposes to deploy multiple credit institutions in the IoV system, and all credit institutions are connected in the form of consortium blockchain. The vehicle registration information is stored in the blockchain, which reduces the storage pressure of credit institutions and ensures the normal operation of the network when a credit institution is attacked. At the same time, the blockchain ensures that the registration information of the vehicle will not be modified after a credit institution is attacked, so that the attack fails. When there is no gain from the attack, malicious nodes will give up the attack, thus protecting the system security.

Different from the previous two methods, the author of Ref. [136] for the Packet-Dropping Attack, Decryption Failure Attack and Man-in-the-Middle (MITM) Attack methods that exist in vehicle data transmission in IoV, the author proposes a traceability and authentication key exchange protocol. This solution introduces blockchain on Packet-Dropping Attack. Transparency allows vehicles on both sides of the transaction to observe the content of the negotiation, ensuring data exchange based on the success of the negotiation. This makes up for the problem that the traditional key exchange scheme cannot confirm whether the negotiation between the two parties of the data exchange is successful. Secondly, the protocol stipulates that only the sending vehicle and the receiving vehicle can verify the key, which solves the problem of decryption failure caused by the receiving vehicle receiving the wrong decryption key, and prevents the decryption failure attack. Finally, in order to prevent MITM Attack, the author proposes the identity verification mechanism (signature) in the blockchain to enable the vehicles of both parties to verify the identity of the other vehicle before transacting, and the third party cannot carry out MITM Attack because it cannot obtain the correct signature.

Compared with [136], which achieves the purpose of protection by tracking the attack, the author of Ref. [137] prefers to prevent attack before it occurs. Therefore, they propose a network security system based on Blockchain Governance Game (BGG). BGG is a stochastic games model, which is superior in preventing and finding network attacks. The author introduces BGG into IoV to prevent malicious nodes from attacking vehicles. The blockchain network of the model is composed of internal components of the vehicle, service center and headquarters database. In BGG, two players play a confrontation game. The goal of capturing attack behavior in advance is achieved by simulating attackers and blockers. This method reduces the probability of the system being attacked and successfully prevents the attacker from attacking the system.

The above schemes are aimed at the protection of external attacks, without considering the security of internal data. The author of Ref. [138] proposes a blockchain-based anti-attack security scheme. In this scheme, lattice cryptography is used to prevent quantum attacks and data forgery attacks. The public information of the vehicle is stored on the blockchain to protect the system and prevent the system from malicious nodes. There are five entities in this system: 1. Vehicles: collect and transmit data in real time. 2. RA: As a semi-trusted third-party node for vehicle registration. 3. System administrator: The system administrator manages the trust value of entities in the entire system. 4. Edge device: accept the message transmitted by the vehicle, and deliver the message to the traffic control system for processing. 5. Traffic control system: Analyze the data obtained from the

edge nodes, and make decisions for vehicle based on the data analysis results. The system analyzes the attacks on the inside of data by malicious nodes with data access rights and the attacks of external attackers whose target is not data. Five kinds of attack behaviors are analyzed, including modification attack, man in the middle attack, impersonation attack, stolen verifier table attack and replay attack. The results show that the system has better attack resistance. In addition, this scheme improves the performance by 43% and reduces the storage by 25% compared with the traditional scheme.

In addition, there are usually attacks on payments during resource transactions. In the process of EV energy trading, malicious EVs often attack CS by submitting orders multiple times. Aiming at such malicious attacks, in paper [139], author proposes an anonymous authentication method based on consortium blockchain. In the initialization phase of this method, the public key certificate is first issued to the charging station, EV and financial institution, and the key pair is generated by the Key Distribution Center (KDC) for digital signature. Then the KDC generates a unique key pair for the EV, and the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) algorithm is used to generate parameters and bind certificates. Finally, the parameters are exposed to the system for prefix linkable anonymous authentication. In the process of purchasing currency, EV purchases signed currency from Financial Institution (FI). Since FI only saves the instantaneous value of currency, EV cannot be identified by currency. During the transaction, the system first makes the CS broadcast the bidding message and upload it to the blockchain according to the information such as time and place. EV gives the price by querying the bidding scheme in the blockchain, uploads the reservation information to the blockchain, and is verified by the blockchain. Then there is the charging stage, EV verifies the reservation information, once the verification is passed, it can charge and pay digital currency in the blockchain. Finally, the digital currency is deposited into FI, and after FI verifies, CS can exchange it into real currency.

With the development of machine learning, the method of combining federated learning and IoV has been applied by more and more researchers. The author of Ref. [140] aiming at the problem that federated learning in IoV is vulnerable to attack, a blockchain-based secure FL scheme is proposed for IoV. In the scheme, blockchain is used as a security guarantee to ensure that the training model is not tampered with by malicious nodes by using smart contracts, so as to ensure the security of data. In addition, blockchain eliminates the dependence of the system on the central node, and this distributed structure well prevents the single point attack problem. This scheme allows the vehicle to train the model locally using private data. To avoid the damage of malicious nodes to local model parameters or data, the author uses consensus algorithm and smart contract to verify the accuracy of the model. If abnormal behavior is found, the system allows trusted nodes to verify the abnormal data through their own private data. Blockchain is built and maintained by all authorized nodes. The first authorized node that receives the local model uploaded by the vehicle aggregates all models, forms the final training result, and writes the resulting block into the blockchain. Compared with other FL schemes in IoV, the failure rate of this scheme is reduced by 5% when the proportion of malicious nodes is high. However, in this scheme, the selection of write nodes is not a consensus method, but the node which is first received data, which cannot guarantee that there are enough resources to aggregate all models.

Autonomous driving is the ultimate goal of Intelligent Connected Vehicle. However, there are many problems to be solved in the process of the transformation from intelligent connected vehicles to automatic driving. Network attack is one of the representative challenges. Attackers can intercept the information sent by vehicles in the network and discard or replace it with false information. In order to solve network attacks, the author of Ref. [141] proposes a method based on blockchain and hybrid cryptosystem by taking advantage of the good security of blockchain. The proposal process is shown in Figure 11. First, vehicles transmit route information to the control center (CC). CC verifies and encrypts the data, then generates a key pair and sends it to vehicles. Simultaneously, all RSUs in the vehicle path build blocks through the verification request sent by CC, and then send the

blocks to CC for verification. After the block is verified by CC, CC transmits the vehicle session key to RSU. When the vehicle passes the RSU, it is decrypted through the session key. At the same time, CC builds a private blockchain using the blocks sent by RSU. Finally, vehicles send requests to RSUs, and RSUs send a message after authenticating it. The vehicle decrypts messages and repeats above steps. The author simulated the packet loss rate and accident rate of two self driving vehicles when they were attacked on the road. The results show that the proposal reduces the packet loss rate of about 3% and the accident rate of about 80% compared with the existing proposal, which is a great improvement for automatic driving. Therefore, it can be proved that network attacks can be avoided through this pre-authentication method.

Table 7 summarizes the research directions and applications of papers related to the protection of attack management.

Table 7. protection of attack Management Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[134] [135]	The third-party organizations are vulnerable.	Build a third-party platform with blockchain.	The distributed structure of the blockchain is used to ensure that third-parties are not harmed by single-point attacks.
[136] [137]	The problem of external attacks on the network by malicious nodes.	<ol style="list-style-type: none"> 1. Track the attack of malicious nodes and record the identity of the attacking node to avoid secondary attacks. 2. Simulate the attack behavior before the attack to achieve the purpose of pre-judgment. 	Since the blockchain is attack-traceable, after a malicious node attacks, the node can be tracked and identified. In addition, the blockchain can be used to record simulated attack behaviors. Once a real attack occurs, it can be discovered and prevented immediately.
[138] [139] [140] [141]	Internal data attack-transaction process attack.	<ol style="list-style-type: none"> 1. Blockchain can prevent attacks on internal data such as data forgery and information discarding. 2. The method of anonymous verification prevents multiple order submission attacks. 	The consensus in the blockchain can determine the correctness of the information, and it can also confirm whether the node has made multiple payments.

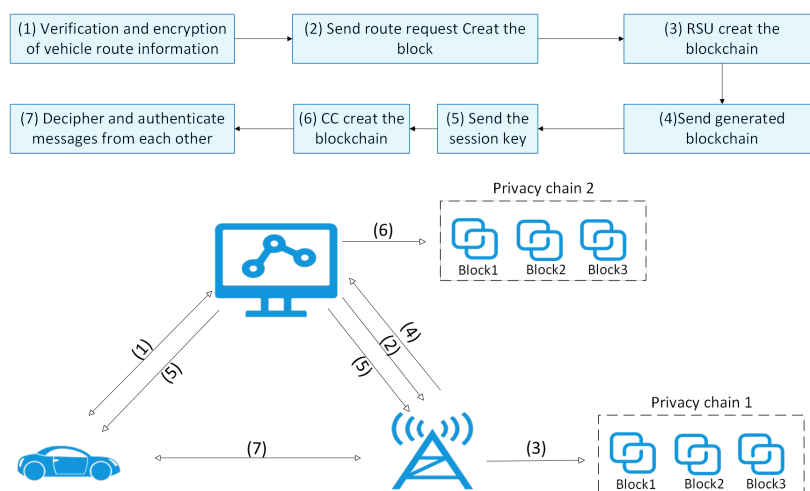


Figure 11. A security scheme based on blockchain and hybrid cryptosystem proposed in [141].

4.5. Privacy Management

While ensuring the security of the IoV network, the privacy of the vehicle is also an issue that needs to be considered. In the era of the Internet of Everything, all user information is exposed on the Internet. In IoV, the information of vehicles and drivers is also exposed on the network, and there is a risk of being leaked at any time, which seriously affects the security of IoV and increases the possibility of malicious attacks. If privacy is not well protected, it is likely to lead to problems such as vehicle identity theft, which will put the aforementioned trust and security mechanisms in vain. Not only identity privacy, but also vehicle location privacy should not be leaked. In the IoV environment, there are mainly two types of privacy protection. 1. Identity privacy: The identity privacy method is used to prevent unauthorized entities from knowing the identity of the vehicle or driver, so as to protect privacy from being leaked. 2. Location privacy: Unauthorized entities should not see the vehicle's location information. At the same time, authorized entities should not obtain the vehicle's real-time location information at unnecessary time (such as after the transaction ends). The location information includes driving path and positioning coordinates, etc.

The following summarizes the work carried out by scholars on identity and location privacy.

4.5.1. The Privacy of Identify

Identity authentication is widely used in IoV as the basis for ensuring security, but the existing centralized identity authentication schemes have the problem of privacy leakage.

In paper [142], the author proposes a blockchain-based privacy protection scheme for vehicles in IoV. The scheme uses cryptographic primitives to hide the identities of vehicles, RSUs and users to privacy protection. The system divides roles in IoV into five types, namely: TA is responsible for registering identities for other roles and tracking malicious data senders during the initialization phase. The EV is the data sender and receiver. User is the driver and passengers in vehicles. The RSU is a communication relay node between EVs and is responsible for storing blockchain ledger data. The blockchain is built on RSU as a safe and reliable information platform. First of all, users, vehicles and RSUs need to register their identities with TA, and TA issues a unique identification code. Then the data sender sends data to RSU, and RSU publishes the verified signature and data to the blockchain to ensure that the data is not tampered with. Finally, the receiver gets the data from the RSU. The method can improve the efficiency of data sharing through the P2P connection mode. The method of using RSU as an intermediate node can effectively avoid the leakage of identity information caused by the connection between the sender and the receiver, and also avoid the privacy attack of malicious nodes on other nodes.

With the increasing number of vehicles in IoV, the burden of computing and storage increases. People in the industry often use edge computing to offload computing tasks to edge servers. However, this method increases the communication cost, and also puts forward higher requirements for communication security. Different from the cryptographic identity hiding in [142], the author of Ref. [143] proposes to replace the real identity with a pseudonym. The author aims at how to ensure that the privacy of the vehicle is not leaked during the communication process. The author proposes a method that combines blockchain with edge computing, adopts pseudonym and identity signature mechanism, and provides a conditional identity privacy protection while ensuring the authenticity of data. The blockchain here adopts the consortium chain. In this system, the network in IoV is divided into 4 entities 1. TRA: TRA is considered to be completely credible, and is mainly responsible for vehicle registration and pseudonym assignment. 2. RSU: RSU is an intermediate node that communicates with TRA and vehicles at the same time. At the same time, some RSUs are also responsible for the construction and maintenance of the alliance blockchain network as edge server clusters (ESC). All RSUs jointly carry out the consensus process, and each RSU is a node in the consortium chain and stores the ledger. 3. Vehicle: The vehicle is equipped with multiple on board units (OBU), which provide data

and computing power for the vehicle. The vehicle transmits the data into the RSU. 4. Cloud: After receiving the data uploaded by RSU, the cloud analyzes and processes the data and then saves it permanently. On this basis, to ensure that the privacy of the vehicle is not leaked, a one-time pseudonym is used. During the registration phase, TRA registers offline and records the Vehicle Lone Number (VIN) at the local service area. Then, TRA calculates a one-time pseudonym and key for each vehicle through a set of random numbers, and sends it to the vehicle. When the vehicle leaves or joins the consortium, it needs to re-register. Through the security evaluation of the system on anonymity, security, and unlinkability, it is proved that the system can effectively prevent privacy attacks by malicious nodes through data mining, and effectively protect the privacy of vehicles. However, in this scheme, the selection of the vehicle leader is as follows: when there is only one vehicle in the cluster, this vehicle is the leader, and when there are more vehicles, the leader is selected according to the average speed. This leader selection scheme cannot prevent malicious nodes from participating in the leader election. Once a malicious node is elected as the leader, it will endanger the security of the entire cluster. If a consensus mechanism can be added to the scheme, security will be improved.

The author of Ref. [144] consensus mechanism was taken into consideration when designing the system. As shown in Figure 12, the authors propose a blockchain-based authentication framework to protect the privacy of vehicles, which is authorized through CyberTwin (CT) and reduces storage and communication costs, called CyberChain. In the traditional authentication framework that builds the blockchain on physical entities (vehicles or RSUs), the operation of the blockchain depends on the performance of physical nodes, and the consensus mechanism also requires communication between nodes. Different from the traditional scheme, this scheme transmits the physical vehicle situation to the cyberspace through the RSU, and builds a blockchain in the CT. The consensus process will no longer be carried out in physical nodes. The purpose of this is to protect the privacy and security of vehicles while building a lightweight blockchain and reduce the cost of blockchain creation and maintenance. In addition, the diffusion practical byzantine fault tolerance (DPBFT) consensus mechanism is used to reach a consensus in a small area before conducting a comprehensive consensus. This method can effectively reduce delays. On this basis, to protect the privacy of vehicle identity, the system also combines zero-knowledge proof and Pedersen commitment (P4C). The author proves that the proposed framework has lower communication overhead through the analysis of DPBFT, single point of failure, and P4C algorithm. Simultaneously, the author simulated Conspiracy Attack, Man-in-The-Middle Attack and Replay Attack, and the system showed good privacy protection and security in the three attacks.

On the basis of privacy protection, the author of Ref. [145] adds preventive measures—identity attack detection. This scheme prevents privacy disclosure and attack caused by the use of open network when transmitting data between entities in IoV. To prevent entity identity from being stolen, the author introduces blockchain into IoV network and proposes a blockchain-based IoV entity identity security framework (P2SF-IoV). Since the blockchain is immutability, transparency, and attack traceability, the combination of the blockchain and the entity data transfer process in IoV can well protect the security of vehicle identity. P2SF-IoV is divided into initialization, registration, authentication, block creation and update phases. The author details the verification process of different identities at various stages and the establishment of the blockchain network. In addition, based on this protocol, in order to prevent network attacks, the author also added a deep learning module to use the data stored in the blockchain to detect attacks and intrusions. By comparing the existing non-blockchain security protocols, it is concluded that the use of blockchain can ensure network privacy. At the same time, the use of hash chain increases the cost of malicious modification, reduces the possibility of network attack and intrusion, and achieves the effect of privacy protection and attack resistance.

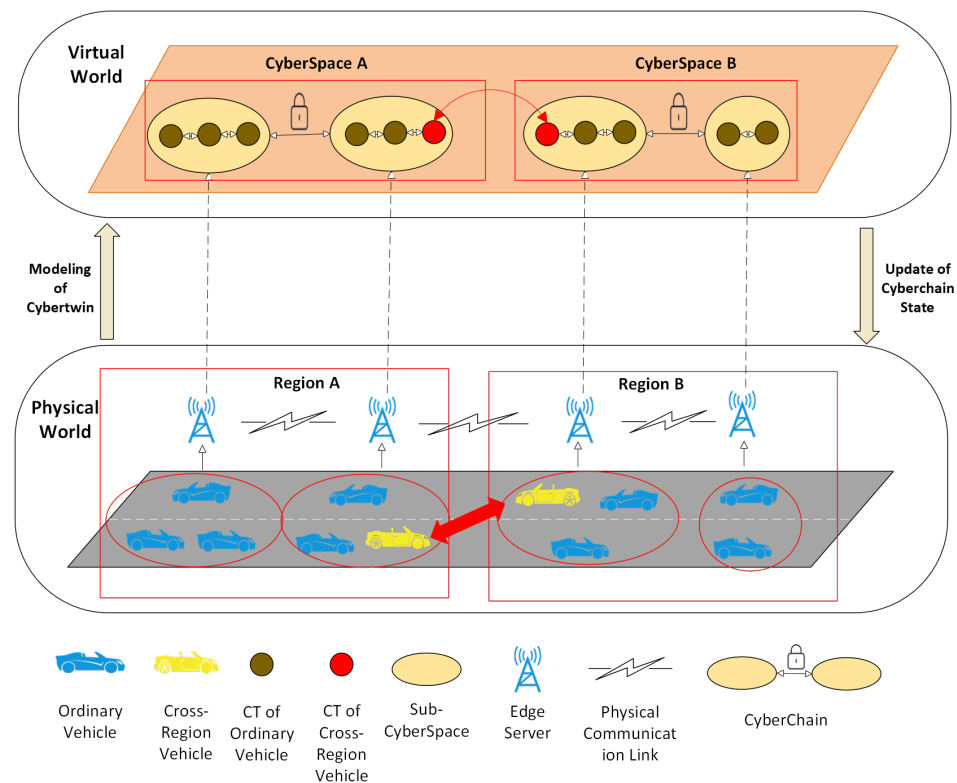


Figure 12. CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-Preserving Authentication proposed in [144].

In paper [99], the author adopts the blockchain to build a privacy protection platform for IoV based on FL, and uses the distributed blockchain as the FL network framework. It aims to prevent malicious nodes stealing user privacy or attacking the system by uploading incorrect data in traditional FL-based IoV. In terms of blockchain selection, the author chooses the consortium blockchain, which uses channel and smart contract technology to better protect the privacy of users. All learning processes are transactions in the consortium blockchain. During the combination of blockchain and FL, homomorphic encryption technology is used to further encrypt the data to prevent malicious nodes from uploading wrong data. In addition, the author also uses the method of distributed verification to improve the efficiency. Different from the previous method, Refs. [146,147] uses anonymous voting to protect the vehicle identity information.

The author of Ref. [146] aiming at the privacy disclosure and malicious attacks of intelligent vehicles in IoV, an anonymous privacy protection method based on consortium blockchain is proposed. This method provides conditional privacy for vehicles, which aims to protect the identity information of the vehicle and trace the attack at the same time. The vehicle nodes are anonymous during the data transmission and voting process, which fully guarantees that the identity information of the vehicle will not be leaked. Simultaneously, to improve the reliability of consensus nodes in the process of consensus, a voting scheme is proposed to evaluate the reputation of consensus nodes. Experiments show that the system can control the reputation of malicious nodes, and the detection rate is much higher than the traditional scheme.

On the basis of [146], the author of Ref. [147] considers the unstable connection of vehicle network. In order to protect vehicle privacy, an anonymous voting scheme is constructed by using attribute based encryption in the process of vehicle participation in decision-making. In this scheme, only vehicles with decision attributes and RSUs are allowed to vote anonymously, and other vehicles are not allowed to vote. Instead of the traditional way of voting by identity, this scheme can effectively protect the privacy of vehicle identity by classifying nodes according to their attributes. In addition, if some

vehicles need to participate in decision-making, but at this time they are disconnected from the system due to problems such as network instability. This scheme proposes a proxy voting method. This scheme allows vehicles to delegate voting rights to surrounding trusted nodes before disconnection. The trusted node can vote instead of the original vehicle. After the connection of the vehicle is restored, the trusted node returns the voting right. This process only exchanges voting attributes and does not involve vehicle identity information, so there is no risk of vehicle identity information leakage. After all nodes vote, the blockchain will record the voting results. The immutability of the blockchain ensures the credibility of the voting history. In addition, the reward and punishment smart contracts related to the voting results are designed, so that the system can automatically motivate the vehicle decision-making and ensure the honesty of the nodes.

At the same time, EVs are more vulnerable to privacy leakage during charging. Anonymous scheme also has great application in privacy protection of EVs. To eliminate influences of the third party in the charging system, the author of Ref. [148] proposes an anonymous blockchain charging system. Firstly, three key pairs are introduced: 1. PKU, SKU: provided by distributed PKI systems. 2. PKC, SKC: used to generate zero knowledge proof ZKP. 3. PKR, SKR: key pair used to represent user signature. The system is divided into three stages. The first is the registration phase. At this stage, the user's certificate is obtained by applying to the PKI through the hash value of the real identity. After receiving the user's hash value, the KPI uses registration blockchain (RBC) and certificate blockchain (CBC) vote consensus to issue certificates. The second is the charging scheduling stage. The user puts forward the demand, EV-charging Service Providers (EVSPs) issue PKC and SKC to the user, and the user provides SKC and time stamp to generate zero-knowledge proof ZKP. At this time, among the three smart contracts in the CBC, the "verification" contract embedded in the PKC performs the verification process. After verification, the system will assign a token to the user as a passport. Then, EVSP uses the "scheduling" contract to give the user tokenT. The user uses tokenT to prove their identity to the charging station, RBC verifies the local information, and starts charging after the verification is passed. Finally, in the payment phase, the charging station provides the user with the bill, the user confirms the payment and signs, and finally the charging station sends the signature to CBC.

In paper [149], for the privacy problem of EVs, the distributed system of Ethereum blockchain and smart contract is used to deal with the privacy protection problem. To ensure the privacy of users, the author uses zero knowledge proof to allow the receiver to verify the sender's information without exposing the contents of the proof. After EV passes the smart contract, it will receive the token issued by Ethereum. The token uses random addresses to decouple the verification and charging process to protect privacy such as EV location information from being obtained by charging station. On the other hand, to reduce the overhead of blockchain, Pederson Commitment is used. This method can hide the submitter information without a token, so that everyone except the submitter can not know who is the submitter.

4.5.2. The Privacy of Location

IoV provides a wealth of services for vehicles, such as parking, charging, highway tolls, etc. However, these services require the location of vehicles, but the leakage of these location information will lead to the vehicle being tracked. In addition, some operators may use the vehicle's location to send targeted advertisements that the vehicle does not want to receive. How to protect the location privacy of vehicles has become a hot topic. Different research objects have different research angles, such as considering location privacy in vehicle data sharing.

The author of Ref. [129] proposes a vehicle location privacy protection mechanism based on private blockchain—IMLP. In the process of vehicle spectrum data sharing, blockchain is used to protect the location information of vehicles. At the same time, the distributed K-anonymity algorithm is combined with the blockchain to ensure that malicious nodes cannot analyze the real location of the vehicle even if they obtain spectrum

allocation information. The system is composed of fusion center and vehicle. The fusion center is responsible for calculating the spectrum data, allocating the idle spectrum to the VN of vehicles in need, and the VN requests position protection from other vehicles in the network. They work together to build anonymous areas and share spectrum without disclosing location. The scheme designs credibility mechanism, anonymous area creation mechanism, reporting and adjudication mechanism and incentive mechanism. The credibility mechanism is mainly responsible for measuring the credibility of users. The system tends to use vehicles with higher credibility to establish anonymous areas. Anonymous zones mainly use k-anonymity scheme to protect location privacy, and the construction of anonymous zones is regarded as transactions in the blockchain. The information (the ID of the requesting user and the cooperative user, and the location of the cooperative user) of user is encrypted and stored in the blockchain as the transaction ledger. For violations, the system uses reporting and ruling mechanisms to punish malicious nodes. Finally, the incentive mechanism is used to stimulate more vehicles to participate in the position protection. At the same time, the system also considers the problem of location leakage in the process of receiving service and paying after service.

A vehicle location privacy protection scheme based on blockchain was proposed by [150]. The author uses blockchain as a payment method to eliminate the dependence of central bank in traditional payment methods. The author proposes a new algorithm: zk-sigproof, which uses blockchain to complete the correct payment process while ensuring the privacy of vehicle location. The payment process is automatically completed by the smart contract. The system is set as follows: the vehicle interacts with other entities through a pseudonym account and uploads public information to the blockchain. Some stations are responsible for generating signatures for the vehicles passing by them. Therefore, when the vehicle completes the transaction, the exit will sign, and the vehicle will upload the exit signature to the blockchain to ensure the hiding of location information. The toll gate is a fund management account in the blockchain. It is worth noting that the account does not verify the payment amount, but only saves funds and ledgers. The verification process is completed by the miner node through the consensus algorithm. Miners verify the bills through smart contracts, and then compete for the right to write in the blockchain to obtain corresponding benefits. The author tested 4000 transactions and proved the effectiveness of the system by testing the transaction delay and system performance.

In addition, the charging process of EVs is more prone to location leakage. The author of Ref. [151] aiming at the problems of charging stations stealing vehicle location privacy, detecting vehicle locations and tracking and sending advertisements, this article proposes a blockchain-based charging station selection protocol based on pricing and distance of EVs. the protocol is divided into four stages: (1) Exploration stage. The EV sends a request to the blockchain within a certain time and space. The request only contains the ID of the EV and does not contain location information, so the EV cannot be located according to the existing information. At this point, the request will be displayed to everyone on the blockchain. (2) in the bidding stage, the charging station queries all requests from the blockchain and determines whether to participate in the bidding according to its own location. Participants give quotations and upload them to the blockchain. and by taking advantage of the transparency and immutability of the blockchain, charging stations are stimulated to participate in more bids. This process is repeated until the EV accepts a certain offer. EVs can also accept only the first round of bids, which will incentivize charging stations to make lower bids and reduce blockchain storage space to complete the bidding process faster. (3) in the evaluation stage, EV and customers comprehensively evaluate the price and distance outside the blockchain, and finally decide to select a charging station for charging. The system stores the ID of the EV and the hash value of the charging station in the blockchain. (4) During the charging phase, the EV finds the charging station for charging.

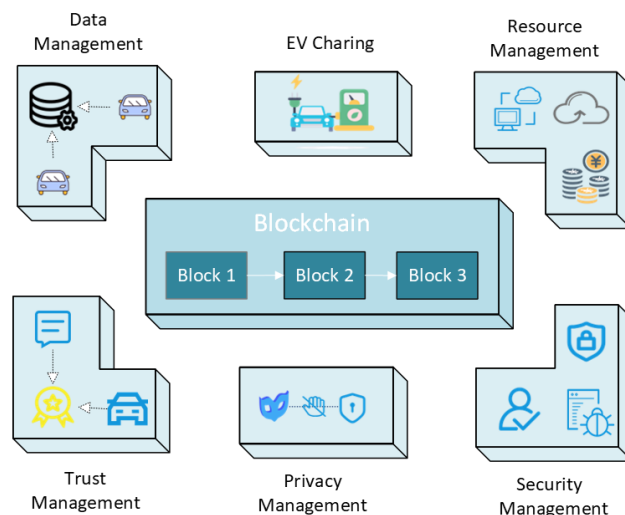
Table 8 summarizes the research directions and applications of papers related to privacy management.

Table 8. Privacy Management Related Papers.

Papers	Focused Challenges	Short Descriptions	How BlockChain Brings Opportunities
[142] [143] [144] [145] [99]	Protect vehicle identity privacy from being leaked, and prevent identity theft.	<ol style="list-style-type: none"> 1. The vehicle identity is effectively encapsulated through blockchain cryptography and pseudonyms to protect vehicle identity information from being leaked. 2. Attack detection prevents vehicle identity information from being stolen. 	Cryptography in the blockchain can hide the true identity of the vehicle, in addition to the use of hash values to ensure that the vehicle identity has not been tampered with, thus protecting identity privacy.
[146] [147]	Protect vehicle identity information during communication.	During the voting process, anonymous voting is used to ensure that identity is not leaked.	The conditional privacy of the vehicle is provided by the blockchain, and the traceability of the attack protects the vehicle from being attacked by malicious nodes during the voting process.
[148] [149]	Identity Privacy Issues During EV Charging.	<ol style="list-style-type: none"> 1. The anonymous charging scheme protects privacy. 2. Guaranteed privacy with Ethereum and smart contracts. 	Anonymous or zero-knowledge proofs are integrated with the blockchain to ensure that vehicle privacy is not obtained by other malicious nodes.
[129] [150] [151]	How to ensure the privacy of vehicle location is not leaked.	<ol style="list-style-type: none"> 1. The combination of anonymity algorithm and blockchain ensures that even malicious nodes cannot analyze the real location even if they know the information. 2. The payment process is completed with the blockchain, and the vehicle location is protected through pseudonyms and concealment methods. 	<ol style="list-style-type: none"> 1. Build an anonymous integrity mechanism and use the blockchain to create a shared spectrum that does not reveal the location. 2. The blockchain is used as the payment method, and the payment process is completed by a pseudonym or ID. This process does not contain location information, so as to ensure that the location is not leaked.

4.6. Remarks

In the above research, we analyzed some blockchain applications on IoV. We elaborated from data management, resource management, trust management, security management, and privacy management. The widespread application of blockchain in IoV is shown in Figure 13.

**Figure 13.** Applications of blockchain in IoV.

5. Future Research Opportunities

In addition to the directions discussed in Section 4, there are some open challenges that need to be discussed. In this section, we will describe these challenges in detail, and based on these challenges, we propose future research directions and explain how to use blockchain in conjunction with other advanced technologies to increase the performance of IoV systems in all aspects.

5.1. The Limitations of Using Blockchain In IoV

While the blockchain brings many benefits to IoV, it also has some limitations, such as the privacy issues of the blockchain and the storage issues brought about by the blockchain. We discussed some of the limitations of introducing blockchain into IoV.

5.1.1. Privacy Protection of Blockchain

Although the use of blockchain can effectively protect the privacy of vehicles in IoV through third parties and cheating resistance, the privacy of blockchain also needs to be guaranteed.

First of all, blockchain was first used in digital currency to protect the privacy of transactions by using cryptography principles. However, for blockchains without currency transactions, such as some Consortium blockchains, it is also necessary to protect their privacy. As blockchain is a public ledger, any node can join the blockchain at any time for public chain and Consortium blockchain. As a network member, this node can see and copy all transaction ledger data of other nodes. Once a malicious node breaks through the identity limit to join the network, it will cause the data leakage of the system. At present, the Consortium blockchain adopts the method of dividing “domain” and “namespace” for this kind of privacy protection, sharing data with the “domain”, and other nodes are not allowed to access the data in the “domain”.

However, this method also has great shortcomings. First, although the node cannot access this part of data in the blockchain, it is still possible to access this part of data in the network layer. (such as ordering service in fabric). Secondly, privacy is divided by “domains”. A large number of “domains” need to be built to ensure privacy in all Consortium blockchains. The construction and maintenance of such a large number of “domains” require a lot of resources. In addition, nodes in the same “domain” can still access all data, and the granularity of privacy protection is not detailed enough. Finally, the construction of a “domain” depends on the assumption that all nodes in the “domain” are honest nodes and will not maliciously disclose privacy. However, this assumption reduces the credibility of blockchain. When there are enough nodes, the system cannot guarantee that these nodes do not contain dishonest nodes.

To solve the above problems, there are also some researches on the methods of Federated learning [80,81]. In these cases, the node first trains the model locally, and then uploads the analyzed data and model parameters. This method can make the data available, but can not see the original data. The privacy issue of the blockchain can be used as a research direction.

5.1.2. Blockchain Storage Redundancy

Since the blockchain requires all nodes to save all ledger information, some nodes store ledgers that they are not interested in, resulting in storage redundancy and increasing the storage pressure on nodes. In response to this problem, some scholars use the consortium blockchain [117,135,139]. The consortium blockchain allows nodes to choose to join interested organizations and only store the organization’s ledger. The consortium chain can reduce the storage pressure of nodes and improve storage efficiency. In addition, some scholars use the method of digital twins to solve this problem [144]. The digital twin is to synchronize the physical world to the twin world in real time to realize the synchronization of the two worlds. The ledger transactions in the physical world are implemented and stored in twins. Since twins are generally built in servers such as the cloud, the storage

capacity of physical nodes can be reduced. The above two methods can well reduce the storage capacity of the vehicle, so as to achieve the purpose of efficient utilization of storage resources. A more in-depth discussion on this issue can be conducted in the future.

5.2. Special Challenges in IoV Scenarios

5.2.1. High Mobility

Different from the IoT scenario, IoV is a network composed of high-speed mobile vehicles. The node position in the network changes frequently, and the nodes will constantly exit and join the new network. The network topology changes all the time, which makes the network construction more difficult. Moreover, the vehicle running speed is different. When the vehicle is running in a sparse BS or passing through a tunnel, the vehicle's ability to accept signals is weak, which also brings challenges to the stability of the network. In addition, the different communication modes of different vehicles make it impossible to build the network quickly, which is the challenge brought to IoV by the rapid movement of vehicles. The distributed structure of blockchain can bring new changes to the high mobility IoV environment. By joining the blockchain network, the vehicle can no longer rely on the stable communication brought by the static topology, but can trade with different nodes, which greatly reduces the impact of the rapidly changing topology. At present, there are not many researches on high-mobility blockchains, and this aspect can be used as a future research direction.

5.2.2. Delay Sensitive

There are requirements for delay. For example, in an emergency, the vehicle needs to respond quickly to avoid more serious injuries. Moreover, road planning also requires real-time dynamic path planning. Once the delay increases, the planned path is likely to no longer be applicable to the current traffic situation, which will cause a waste of computing resources. More importantly, in the process of uploading the cloud server in the traditional method, the network delay will increase because the vehicle is far away from the cloud. Moreover, in the case of large traffic flow, the network will be congested, and the delay will also be caused by the untimely processing of information on the cloud. Therefore, a fast and efficient transmission protocol is needed to connect the vehicle with the surrounding nodes and transmit information to reduce the delay. At present, the construction of IoV network has caused some delay, and after the blockchain is added to IoV, the construction and maintenance of blockchain will also increase the system delay. Therefore, there should be more research in the direction of reducing delay.

5.3. Reliance on Third Parties

Through the analysis of the IoV network construction method combined with blockchain in Section 4, we found that most methods require the vehicle to register before joining the network. However, the current PKI-based methods all require a centralized certification verification authority. The identity registration of vehicles basically depends on Ca and TA. CA is the certification authority of the vehicle, and TA is the trusted authority in the network. The above two kinds of institutions are called third-party certification institutions. The first step for each vehicle to join the network is to submit a registration application to a third-party CA. This authentication mechanism leads to the centralization of identity authentication, which is out of the original intention of using blockchain distributed ledger structure. Moreover, whether the third-party organization is absolutely credible, how to ensure the absolute trust of the third-party organization, and how to make the vehicle believe that the third-party organization is credible are very important issues. In addition, even if the third-party organization is absolutely credible, there are certain risks in this centralized authentication method. The centralized network structure is more vulnerable to single point attack. Once the third-party authentication authority is destroyed, the whole trusted mechanism will collapse. In addition, the ID based authentication mechanism also needs a key generation server, which is prone to key escrow problems.

Another problem is that trusted institutions need to establish a large number of certificates or identity matches, which will consume many resources. simultaneously, the way that the vehicle verifies with the third party increases the communication overhead and communication delay. In the environment of high-speed mobile vehicle network, delay will lead to information obsolescence, so reducing the delay is very important. At present, there are not many methods to consider the serious dependence of blockchain-based IoV network on third-party trusted institutions [98,124,134,140]. Therefore, we believe that this issue is the direction of future research.

5.4. Incentive Mechanism

If the vehicle is not willing to join the IoV network, the vehicle data will become a data island. How to fully motivate EVs and make more EVs participate in the network construction is a difficult problem. Blockchain was first proposed to serve the digital currency. The immediate (economic) benefits that can be seen in the digital currency. If blockchain is introduced into the incentive mechanism, the enthusiasm of vehicles' participation will be increased by driving vehicles through interests. Refs. [100,101] and other schemes proposed to take advantage of the good performance of blockchain in digital currency, introduce blockchain into the incentive mechanism, and use economic incentives to increase the participation of vehicles. However, the current research takes motivation as an additional research, and there is little special consideration on motivation, so this direction is also more challenging.

5.5. Other Directions in ITS

5.5.1. The transaction of Vehicle

In recent years, with the development of network technology, more and more young people tend to trade vehicles online. On the one hand, neither the seller nor the buyer is willing to give up their own interests in the online transaction. The seller considers whether he will not be able to receive the transaction payment from the buyer if the goods are shipped first. What the buyer is worried about is whether the seller will not deliver the goods if he pays first. On the other hand, whether the information of second-hand vehicles is all open, transparent and true is also an issue that needs to be considered in transactions. In response to these two problems, the introduction of the blockchain into the vehicle transaction scene not only ensures that the interests of both parties are not damaged, but also ensures that the vehicle information is completely credible. This is another research direction of the combination of blockchain and IoV.

5.5.2. Traffic problems

A. Traffic Accident

With more and more vehicles, it is inevitable that there will be traffic accidents during driving. The data in the accident is an important standard for the determination of responsibility. The preservation of evidence should not only ensure the privacy of vehicle data, but also ensure that the data is not tampered with during the review process. In addition, it also needs to be open and transparent after the formation of the evidence chain. Refs. [77,78,111] considered traffic accidents and proposed IoV model based on blockchain. Therefore, we believe that using blockchain to ensure the preservation of evidence chain in traffic accidents will achieve good results.

B. Path planning and dynamic navigation

Whether it is assisted driving or intelligent driving, it is necessary for the vehicle to have a reasonable planning for the path and dynamically navigate for the driver according to the planning. There are many factors to be considered in path planning, such as whether the current time is the peak period, the density of vehicles on a certain road section, whether there is traffic congestion, and the switching time of signal lights in different road sections.

Path planning needs to comprehensively consider these factors. How to quickly and safely obtain these real-time data is a direction that needs to be discussed in the future.

Another problem is dynamic navigation. When the route planning is successful, due to some emergencies, such as traffic accidents in the vehicle ahead or the road section in the route, how can the vehicle quickly obtain the real-time information of the accident, and make the minimum change on the basis of the original planning according to the degree of the accident, the road section and other information. For example: the overall driving direction is not changed, only the lane is changed. This is a problem that needs to be considered in dynamic navigation.

Both of the above problems require high storage and computing resources, and the requirement of real-time also brings challenges to IoV. At present, there are few researches on path planning and dynamic navigation direction [152]. The application of blockchain in these two fields can make the vehicle driving process safer.

C. The Service of Entertainment

The development of intelligent vehicle systems has promoted the development of vehicle entertainment services. These include advertising, radio broadcasting, and online shopping. The more entertainment in the vehicle, the lighter and happier the driver and passengers will be while in the vehicle. However, it is more difficult to provide entertainment services for users personalized according to their interests while ensuring that their privacy is not illegally used. Therefore, the good performance of the blockchain in privacy protection has brought great opportunities for intelligent entertainment services. However, there are not many studies on entertainment services at present [153].

5.5.3. Electric Vehicle

With the proposal of the concept of green traffic, EVs will be the main force of the future transportation system. However, EVs consume fast power and need frequent charging. How to quickly find a charging station for EVs without disclosing the privacy of the vehicle is a challenging task. At present, some scholars have been committed to applying blockchain to the EV energy trading market [102–105]. We believe that using blockchain to power the future EV will be a very good solution.

5.5.4. Ground-to-Air Communication

In addition to vehicle to vehicle communication, UAV has a wide field of vision in the air and can provide a wider range of traffic information for vehicles. Therefore, IoV can also combine UAV with vehicles to form a new type of ground to air cooperation mode. However, vehicles and UAVs are absolutely heterogeneous. Although some researchers have been committed to introducing blockchain into unmanned research [93,123], the current research on UAVs is mostly about how to apply blockchain between UAVs, and the joint trust between ground and air has not been well solved. In addition, UAVs are involved in the air field. Due to some civil aviation and military factors, UAVs cannot ensure full coverage in the air. How to make up for this defect is a problem to be considered in the future.

6. Conclusions

In this paper, a survey on blockchain-enabled telematics applications is presented. As the basis of ITS, IoV has become a research hotspot. How to build an IoV network safely and quickly is one of the problems that need to be solved at present. Introducing blockchain into IoV can better realize V2X by utilizing the characteristics of blockchain such as de-centralization, distribution and non-tampering. Our article first introduces some basic background of IoV, and also discusses the technology of blockchain. In addition, this paper also discussed the current challenges of IoV and the research motivation of this paper. The survey listed the benefits of integrating blockchain into IoV. Then, we systematically and comprehensively investigated the recent research on blockchain enabling IoV in the industry, explained the work of each research and how to add blockchain to IoV, and

summarized them. According to different purposes, these studies were divided into data management, resource management, trust management, safety management and privacy management. Finally, existing challenges as well as future research directions and opportunities are enumerated. To sum up, it is hoped that the blockchain-enabled Internet of Vehicles will bring a new direction of development. We hope this paper can provide research basis for other researchers.

Author Contributions: Conceptualization, J.G. and C.W.; methodology, S.G.; formal analysis, C.P. and C.W.; investigation, J.G. and G.H.; writing, original draft preparation, J.G.; writing, review and editing, C.W. and G.H.; supervision, T.Y. and C.W.; project administration, S.G. and C.W.; funding acquisition, G.H. and S.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the National Natural Science Foundation of China under Grant No. 62062031, in part by ROIS NII Open Collaborative Research 22S0601, and in part by JSPS KAKENHI grant numbers 20H00592 and 21H03424.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author, [Celimuge Wu], upon reasonable request.

Conflicts of Interest: No potential conflict of interest was reported by the authors.

Abbreviations

The following abbreviations are used in this manuscript:

5th Generation Mobile Networks	5G
6th Generation Mobile Networks	6G
Artificial Intelligence	AI
Certification Authority	CA
Charging Station	CS
Delegated Byzantine Fault Tolerance	DBFT
Delegated Proof of Stack	DPoS
Directed Acyclic Graph	DAG
Distributed Ledger Technology	DLT
Electric Vehicle	EV
Intelligent Transport System	ITS
Internet of Things	IoT
Internet of Vehicles	IoV
Mobile Edge Computing	MEC
Peer to Peer	P2P
Practical Byzantine Fault Tolerance	PBFT
Proof of Authority	PoA
Proof of Stake	PoS
Proof of Work	PoW
Public Key Infrastructure	KPI
Quality of Service	QoS
Radio Frequency IDentificatio	RFID
Registration Authority	RA
Road Side Unit	RSU
Trusted Authority	TA
Trust Registration Authority	TRA
Unmanned Aerial Vehicle	UAV
Vehicle to Cloud	V2C
Vehicle to Infrastructure	V2I
Vehicle to Network	V2N
Vehicle to Pedestrian	V2P
Vehicle to Road	V2R
Vehicle to Vehicle	V2V
Wireless-Fidelity	WI-FI

References

1. Gulati, K.; Boddu, R.S.K.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in Internet of Things (IoT). *Mater. Today Proc.* **2022**, *51*, 161–165. [\[CrossRef\]](#)
2. Das, S.; Acharjee, P.; Bhattacharya, A. Charging scheduling of electric vehicle incorporating grid-to-vehicle (G2V) and vehicle-to-grid (V2G) technology in smart-grid. In Proceedings of the 2020 IEEE International Conference on Power Electronics, Smart Grid and Renewable Energy (PESGRE2020), Cochin, India, 2–4 January 2020; pp. 1–6.
3. Barron, L. The Road to a Smarter Future: The Smart City, Connected Cars and Autonomous Mobility. In Proceedings of the 26th International Conference on Automation and Computing (ICAC), Portsmouth, UK, 2–4 September 2021; pp. 1–6.
4. Rajasekhar, K.; Kumar, R.; Kiran, M.; Rammohana Reddy, G. Next-Generation Technologies Empowered Future IoV. In Proceedings of the 7th IEEE International conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2022; pp. 1–5.
5. Alladi, T.; Kohli, V.; Chamola, V.; Yu, F.R.; Guizani, M. Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles. *IEEE Wirel. Commun.* **2021**, *28*, 144–149. [\[CrossRef\]](#)
6. Jiang, X.; Yu, F.R.; Song, T.; Leung, V.C. Edge Intelligence for Object Detection in Blockchain-Based Internet of Vehicles: Convergence of Symbolic and Connectionist AI. *IEEE Wirel. Commun.* **2021**, *28*, 49–55. [\[CrossRef\]](#)
7. Li, W.; Xia, C.; Wang, C.; Wang, T. Secure and Temporary Access Delegation With Equality Test for Cloud-Assisted IoV. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 20187–20201. [\[CrossRef\]](#)
8. Saleem, M.A.; Mahmood, K.; Kumari, S. Comments on “AKM-IoV: Authenticated key management protocol in fog computing-based internet of vehicles deployment”. *IEEE Internet Things J.* **2020**, *7*, 4671–4675. [\[CrossRef\]](#)
9. Nekovee, M. Transformation from 5G for Verticals Towards a 6G-enabled Internet of Verticals. In Proceedings of the 14th International Conference on Communication Systems & NETWORKS (COMSNETS), Bangalore, India, 4–8 January 2022; pp. 1–6.
10. Garcia, M.H.C.; Molina-Galan, A.; Boban, M.; Gozalvez, J.; Coll-Perales, B.; Şahin, T.; Kousaridas, A. A tutorial on 5G NR V2X communications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1972–2026. [\[CrossRef\]](#)
11. Cugurullo, F.; Acheampong, R.A.; Gueriau, M.; Dusparic, I. The transition to autonomous cars, the redesign of cities and the future of urban sustainability. *Urban Geogr.* **2021**, *42*, 833–859. [\[CrossRef\]](#)
12. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1160–1192. [\[CrossRef\]](#)
13. Hammoud, A.; Sami, H.; Mourad, A.; Otrouk, 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. [\[CrossRef\]](#)
14. 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.* **2020**, *8*, 4157–4185. [\[CrossRef\]](#)
15. Shah, K.; Chadotra, S.; Tanwar, S.; Gupta, R.; Kumar, N. Blockchain for IoV in 6G environment: Review solutions and challenges. *Clust. Comput.* **2022**, *25*, 1927–1955. [\[CrossRef\]](#)
16. Kapassa, E.; Themistocleous, M. Blockchain Technology Applied in IoV Demand Response Management: A Systematic Literature Review. *Future Internet* **2022**, *14*, 136. [\[CrossRef\]](#)
17. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [\[CrossRef\]](#)
18. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [\[CrossRef\]](#)
19. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [\[CrossRef\]](#)
20. Bernabe, J.B.; Canovas, J.L.; Hernandez-Ramos, J.L.; Moreno, R.T.; Skarmeta, A. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* **2019**, *7*, 164908–164940. [\[CrossRef\]](#)
21. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 5 February 2023)
22. Chohan, U.W. The Double Spending Problem and Cryptocurrencies. 2021. Available online: <https://ssrn.com/abstract=3090174> (accessed on 5 February 2023).
23. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [\[CrossRef\]](#)
24. Chen, H.; Pendleton, M.; Njilla, L.; Xu, S. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–43. [\[CrossRef\]](#)
25. Wang, Z.; Jin, H.; Dai, W.; Choo, K.K.R.; Zou, D. Ethereum smart contract security research: Survey and future research opportunities. *Front. Comput. Sci.* **2021**, *15*, 1–18. [\[CrossRef\]](#)
26. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart contract development: Challenges and opportunities. *IEEE Trans. Softw. Eng.* **2019**, *47*, 2084–2106. [\[CrossRef\]](#)
27. Balcerzak, A.P.; Nica, E.; Rogalska, E.; Poliak, M.; Klieštík, T.; Sabie, O.M. Blockchain technology and smart contracts in decentralized governance systems. *Adm. Sci.* **2022**, *12*, 96. [\[CrossRef\]](#)
28. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [\[CrossRef\]](#)

29. Sayeed, S.; Marco-Gisbert, H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl. Sci.* **2019**, *9*, 1788. [\[CrossRef\]](#)
30. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [\[CrossRef\]](#)
31. Arena, F.; Pau, G.; Severino, A. A review on IEEE 802.11 p for intelligent transportation systems. *J. Sens. Actuator Netw.* **2020**, *9*, 22. [\[CrossRef\]](#)
32. Jabbar, R.; Dhib, E.; Ben Said, A.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 20995–21031. [\[CrossRef\]](#)
33. Zhou, H.; Xu, W.; Chen, J.; Wang, W. Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities. *Proc. IEEE* **2020**, *108*, 308–323. [\[CrossRef\]](#)
34. Goel, A.; Paredes, J.A.; Dadhaniya, H.; Islam, S.A.U.; Salim, A.M.; Ravela, S.; Bernstein, D. Experimental implementation of an adaptive digital autopilot. In Proceedings of the 2021 American Control Conference (ACC), New Orleans, LA, USA, 25–28 May 2021; pp. 3737–3742.
35. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the internet of vehicles: Network architectures and applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [\[CrossRef\]](#)
36. Elsagheer Mohamed, S.A.; AlShalfan, K.A. Intelligent traffic management system based on the internet of vehicles (IoV). *J. Adv. Transp.* **2021**, *2021*, 4037533. [\[CrossRef\]](#)
37. Hou, X.; Ren, Z.; Wang, J.; Cheng, W.; Ren, Y.; Chen, K.C.; Zhang, H. Reliable computation offloading for edge-computing-enabled software-defined IoV. *IEEE Internet Things J.* **2020**, *7*, 7097–7111. [\[CrossRef\]](#)
38. Yang, Y.; Mao, Y.; Sun, B. Basic performance and future developments of BeiDou global navigation satellite system. *Satell. Navig.* **2020**, *1*, 1–8. [\[CrossRef\]](#)
39. Zhang, Z.; Zhao, J.; Huang, C.; Li, L. Learning Visual Semantic Map-Matching for Loosely Multi-sensor Fusion Localization of Autonomous Vehicles. *IEEE Trans. Intell. Veh.* **2022**, *8*, 358–367. [\[CrossRef\]](#)
40. Li, Y.; Ibanez-Guzman, J. Lidar for autonomous driving: The principles, challenges, and trends for automotive lidar and perception systems. *IEEE Signal Process. Mag.* **2020**, *37*, 50–61. [\[CrossRef\]](#)
41. Kramer, A.; Harlow, K.; Williams, C.; Heckman, C. ColoRadar: The direct 3D millimeter wave radar dataset. *Int. J. Robot. Res.* **2021**, *41*, 351–360. [\[CrossRef\]](#)
42. Yao, H.; Chen, C.; Liu, S.; Li, K.; Ji, Y.; Huang, G.; Wang, R. Lane marking detection algorithm based on high-precision map and multisensor fusion. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e5797. [\[CrossRef\]](#)
43. Kanhere, O.; Rappaport, T.S. Position location for futuristic cellular communications: 5G and beyond. *IEEE Commun. Mag.* **2021**, *59*, 70–75. [\[CrossRef\]](#)
44. Motroni, A.; Buffi, A.; Nepa, P. A survey on indoor vehicle localization through RFID technology. *IEEE Access* **2021**, *9*, 17921–17942. [\[CrossRef\]](#)
45. Adi, P.D.P.; Sihombing, V.; Siregar, V.M.M.; Yanris, G.J.; Sianturi, F.A.; Purba, W.; Tamba, S.P.; Simatupang, J.; Arifuddin, R.; Prasetya, D.A.; et al. A performance evaluation of ZigBee mesh communication on the Internet of Things (IoT). In Proceedings of the 3rd IEEE East Indonesia Conference on Computer and Information Technology (EICoCIT), Surabaya, Indonesia, 9–11 April 2021; pp. 7–13.
46. Khan, A.R.; Jamlos, M.F.; Osman, N.; Ishak, M.I.; Dzaharudin, F.; Yeow, Y.K.; Khairi, K.A. DSRC technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT system for Intelligent Transportation System (ITS): A review. In *Recent Trends in Mechatronics Towards Industry 4.0*; Springer: Singapore, 2022; pp. 97–106.
47. Oughton, E.J.; Lehr, W.; Katsaros, K.; Selinis, I.; Buble, D.; Kusuma, J. Revisiting wireless internet connectivity: 5G vs. Wi-Fi 6. *Telecommun. Policy* **2021**, *45*, 102127. [\[CrossRef\]](#)
48. Bazzi, A.; Berthet, A.O.; Campolo, C.; Masini, B.M.; Molinaro, A.; Zanella, A. On the design of sidelink for cellular V2X: A literature review and outlook for future. *IEEE Access* **2021**, *9*, 97953–97980. [\[CrossRef\]](#)
49. Kumar, O.P.; Kumar, P.; Ali, T.; Kumar, P.; Vincent, S. Ultrawideband antennas: Growth and evolution. *Micromachines* **2021**, *13*, 60. [\[CrossRef\]](#)
50. Spandonidis, C.; Giannopoulos, F.; Sedikos, E.; Reppas, D.; Theodoropoulos, P. Development of a MEMS-based IoV system for augmenting road traffic survey. *IEEE Trans. Instrum. Meas.* **2022**, *71*, 1–8. [\[CrossRef\]](#)
51. Dewangan, D.K.; Sahu, S.P. RCNet: Road classification convolutional neural networks for intelligent vehicle system. *Intell. Serv. Robot.* **2021**, *14*, 199–214. [\[CrossRef\]](#)
52. Li, L.; Lin, Y.; Du, B.; Yang, F.; Ran, B. Real-time traffic incident detection based on a hybrid deep learning model. *Transp. A Transp. Sci.* **2022**, *18*, 78–98. [\[CrossRef\]](#)
53. Irresberger, F.; John, K.; Mueller, P.; Saleh, F. *The Public Blockchain Ecosystem: An Empirical Analysis*; NYU Stern School of Business: New York, NY, USA, 2021.
54. Chen, X.; Nguyen, K.; Sekiya, H. An experimental study on performance of private blockchain in IoT applications. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3075–3091. [\[CrossRef\]](#)
55. Alkhateeb, A.; Catal, C.; Kar, G.; Mishra, A. Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors* **2022**, *22*, 1304. [\[CrossRef\]](#) [\[PubMed\]](#)
56. Fu, X.; Wang, H.; Shi, P. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Sci. China Inf. Sci.* **2021**, *64*, 1–15. [\[CrossRef\]](#)

57. Schinckus, C. Proof-of-work based blockchain technology and Anthropocene: An undermined situation? *Renew. Sustain. Energy Rev.* **2021**, *152*, 111682. [\[CrossRef\]](#)
58. Saleh, F. Blockchain without waste: Proof-of-stake. *Rev. Financ. Stud.* **2021**, *34*, 1156–1190. [\[CrossRef\]](#)
59. Chen, S.; Xie, M.; Liu, J.; Zhang, Y. Improvement of the DPoS Consensus Mechanism in Blockchain Based on PLTS. In Proceedings of the 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl. Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl. Conference on Intelligent Data and Security (IDS), New York, NY, USA, 15–17 May 2021; pp. 32–37.
60. Bou Abdo, J.; El Sibai, R.; Demerjian, J. Permissionless proof-of-reputation-X: A hybrid reputation-based consensus algorithm for permissionless blockchains. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4148. [\[CrossRef\]](#)
61. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain consensus: An overview of alternative protocols. *Symmetry* **2021**, *13*, 1363. [\[CrossRef\]](#)
62. Aggarwal, S.; Kumar, N. Cryptographic consensus mechanisms. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 211–226.
63. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A research survey on applications of consensus protocols in blockchain. *Secur. Commun. Netw.* **2021**, *2021*, 6693731. [\[CrossRef\]](#)
64. Yang, W.; Dai, X.; Xiao, J.; Jin, H. LDV: A lightweight DAG-based blockchain for vehicular social networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5749–5759. [\[CrossRef\]](#)
65. CHEN, L.; XIANG, F.; SUN, Z.x. A survey of blockchain security technologies based on attribute-based cryptography. *Acta Electron. Sin.* **2021**, *49*, 192.
66. Dalimunthe, S.; Reza, J.; Marzuki, A. The Model for Storing Tokens in Local Storage (Cookies) Using JSON Web Token (JWT) with HMAC (Hash-based Message Authentication Code) in E-Learning Systems. *J. Appl. Eng. Technol. Sci. (JAETS)* **2022**, *3*, 149–155. [\[CrossRef\]](#)
67. Maulani, G.; Gunawan, G.; Leli, L.; Nabila, E.A.; Sari, W.Y. Digital Certificate Authority with Blockchain Cybersecurity in Education. *Int. J. Cyber IT Serv. Manag* **2021**, *1*, 136–150. [\[CrossRef\]](#)
68. Pal, O.; Alam, B.; Thakur, V.; Singh, S. Key management for blockchain technology. *ICT Express* **2021**, *7*, 76–80. [\[CrossRef\]](#)
69. Castellon, C.; Roy, S.; Kreidl, P.; Dutta, A.; Bölöni, L. Energy efficient merkle trees for blockchains. In Proceedings of the 20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 20–22 October 2021; pp. 1093–1099.
70. Han, J.; Song, M.; Eom, H.; Son, Y. An efficient multi-signature wallet in blockchain using bloom filter. In Proceedings of the 36th Annual ACM Symposium on Applied Computing, Virtual Event, Republic of Korea, 22–26 March 2021; pp. 273–281.
71. Chen, J.; Li, K.; Philip, S.Y. Privacy-Preserving Deep Learning Model for Decentralized VANETs Using Fully Homomorphic Encryption and Blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 11633–11642. [\[CrossRef\]](#)
72. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [\[CrossRef\]](#)
73. Esmat, A.; de Vos, M.; Ghiassi-Farrokhfal, Y.; Palensky, P.; Epema, D. A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. *Appl. Energy* **2021**, *282*, 116123. [\[CrossRef\]](#)
74. Xu, L.; Ge, M.; Wu, W. Edge server deployment scheme of blockchain in IoVs. *IEEE Trans. Reliab.* **2022**, *71*, 500–509. [\[CrossRef\]](#)
75. Ye, X.; Li, M.; Yu, F.R.; Si, P.; Wang, Z.; Zhang, Y. MEC and Blockchain-Enabled Energy-Efficient Internet of Vehicles Based on A3C Approach. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 01–06.
76. Ding, N.; Zhao, Y. Lightweight Blockchain Based on Storage Resource Optimization for Internet of Vehicles. In Proceedings of the 2021 IEEE International Intelligent Transportation Systems Conference (ITSC), Indianapolis, IN, USA, 19–22 September 2021; pp. 1063–1068.
77. Na, D.; Park, S. Lightweight blockchain to solve forgery and privacy issues of vehicle image data. In Proceedings of the 22nd IEEE Asia-Pacific Network Operations and Management Symposium (APNOMS), Tainan, Taiwan, 8–10 September 2021; pp. 37–40.
78. Philip, A.O.; Saravanaguru, R.K. Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 4031–4046. [\[CrossRef\]](#)
79. Sey, C.; Lei, H.; Qian, W.; Li, X.; Fiasam, L.D.; Kodjiku, S.L.; Adjei-Mensah, I.; Agyemang, I.O. VBlock: A Blockchain-Based Tamper-Proofing Data Protection Model for Internet of Vehicle Networks. *Sensors* **2022**, *22*, 8083. [\[CrossRef\]](#)
80. Wang, R.; Li, H.; Liu, E. Blockchain-based federated learning in mobile edge networks with application in internet of vehicles. *arXiv* **2021**, arXiv:2103.01116.
81. Zou, Y.; Shen, F.; Yan, F.; Lin, J.; Qiu, Y. Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IOV. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 9 March–1 April 2021; pp. 1–6.
82. Chen, C.; Wu, J.; Lin, H.; Chen, W.; Zheng, Z. A secure and efficient blockchain-based data trading approach for internet of vehicles. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9110–9121. [\[CrossRef\]](#)
83. Cui, J.; Ouyang, F.; Ying, Z.; Wei, L.; Zhong, H. Secure and efficient data sharing among vehicles based on consortium blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8857–8867. [\[CrossRef\]](#)

84. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J.* **2018**, *6*, 4660–4670. [\[CrossRef\]](#)
85. Ghimire, B.; Rawat, D.B. Secure, privacy preserving and verifiable federating learning using blockchain for internet of vehicles. *IEEE Consum. Electron. Mag.* **2021**, *11*, 67–74. [\[CrossRef\]](#)
86. Alam, I.; Kumar, S.; Kumar, M.; Kashyap, P.K. Blockchain Based Intelligent Incentive Enabled Information Sharing Scheme in Future Generation IoV Networks. 2021. Available online: <https://www.researchsquare.com/article/rs-714669/v1> (accessed on 5 February 2023).
87. Zhao, Y.; Du, K. An Application of the IoVs Information Sharing Scheme Based on Blockchain Technology. In Proceedings of the 2nd IEEE International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI), Nanjing, China, 23–25 September 2022; pp. 617–620.
88. Gao, L.; Wu, C.; Yoshinaga, T.; Chen, X.; Ji, Y. Multi-channel blockchain scheme for internet of vehicles. *IEEE Open J. Comput. Soc.* **2021**, *2*, 192–203. [\[CrossRef\]](#)
89. Wen, X.; Guan, Z.; Li, D.; Lyu, H.; Li, H. A Blockchain-based Framework for Information Management in Internet of Vehicles. In Proceedings of the 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Glasgow, UK, 21–22 August 2021; pp. 18–23.
90. Gao, L.; Wu, C.; Du, Z.; Yoshinaga, T.; Zhong, L.; Liu, F.; Ji, Y. Toward Efficient Blockchain for the Internet of Vehicles with Hierarchical Blockchain Resource Scheduling. *Electronics* **2022**, *11*, 832. [\[CrossRef\]](#)
91. Chen, C.; Quan, S. RSU Cluster Deployment and Collaboration Storage of IoV Based Blockchain. *Sustainability* **2022**, *14*, 16152. [\[CrossRef\]](#)
92. Zhang, D.; Shi, W.; St-Hilaire, M.; Yang, R. Multiaccess Edge Integrated Networking for Internet of Vehicles: A Blockchain-Based Deep Compressed Cooperative Learning Approach. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 21593–21607. [\[CrossRef\]](#)
93. Khan, A.A.; Laghari, A.A.; Shafiq, M.; Awan, S.A.; Gu, Z. Vehicle to Everything (V2X) and Edge Computing: A Secure Lifecycle for UAV-Assisted Vehicle Network and Offloading with Blockchain. *Drones* **2022**, *6*, 377. [\[CrossRef\]](#)
94. Gupta, M.; Patel, R.B.; Jain, S.; Garg, H.; Sharma, B. Lightweight branched blockchain security framework for Internet of Vehicles. *Trans. Emerg. Telecommun. Technol.* **2022**, e4520. Available online: <https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4520> (accessed on 5 February 2023).
95. Ni, W.; Asheralieva, A.; Maple, C.; Karim, M.M.; Niyato, D.; Yan, Q. Throughput-Efficient Blockchain for Internet-of-Vehicles. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021; pp. 1–6.
96. 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. [\[CrossRef\]](#)
97. Wang, S.; Huang, X.; Yu, R.; Zhang, Y.; Hossain, E. Permissioned blockchain for efficient and secure resource sharing in vehicular edge computing. *arXiv* **2019**, arXiv:1906.06319.
98. 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. [\[CrossRef\]](#)
99. Wang, N.; Yang, W.; Wang, X.; Wu, L.; Guan, Z.; Du, X.; Guizani, M. A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. *Digit. Commun. Netw.* **2022**. [\[CrossRef\]](#)
100. Kong, M.; Zhao, J.; Sun, X.; Nie, Y. Secure and efficient computing resource management in blockchain-based vehicular fog computing. *China Commun.* **2021**, *18*, 115–125. [\[CrossRef\]](#)
101. 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. [\[CrossRef\]](#)
102. Abishu, H.N.; Seid, A.M.; Yacob, Y.H.; Ayall, T.; Sun, G.; Liu, G. Consensus Mechanism for Blockchain-Enabled Vehicle-to-Vehicle Energy Trading in the Internet of Electric Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *71*, 946–960. [\[CrossRef\]](#)
103. Li, Z.; Chen, S.; Zhou, B. Electric vehicle peer-to-peer energy trading model based on smes and blockchain. *IEEE Trans. Appl. Supercond.* **2021**, *31*, 1–4. [\[CrossRef\]](#)
104. Khan, P.W.; Byun, Y.C. Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles. *Sustainability* **2021**, *13*, 7962. [\[CrossRef\]](#)
105. Firoozjaei, M.D.; Ghorbani, A.; Kim, H.; Song, J. EVChain: A blockchain-based credit sharing in electric vehicles charging. In Proceedings of the 17th IEEE International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 26–28 August 2019; pp. 1–5.
106. 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 89th IEEE Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
107. Alotaibi, J.; Alazzawi, L. PPIoV: A Privacy Preserving-Based Framework for IoV-Fog Environment Using Federated Learning and Blockchain. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 597–603.
108. Zhao, Y.; Wang, Y.; Wang, P.; Yu, H. PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV. *IEEE Syst. J.* **2021**, *16*, 3422–3432. [\[CrossRef\]](#)
109. Huang, D.; Tang, Z.Y.; Hu, W.Y.; Wu, Q.Z. Blockchain-based electric vehicle charging reputation management mechanism. In Proceedings of the 2021 IEEE International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), Xi'an, China, 28–30 May 2021; pp. 58–61.

110. Wu, Y.; Wu, L.; Cai, H. A Trusted Paradigm of Data Management for Blockchain-Enabled Internet of Vehicles in Smart Cities. *ACM Trans. Sens. Netw.* **2022**. Available online: <https://dl.acm.org/doi/abs/10.1145/3572841> (accessed on 5 February 2023).
111. Firdaus, M.; Rahmadika, S.; Rhee, K.H. Decentralized trusted data sharing management on internet of vehicle edge computing (IoVEC) networks using consortium blockchain. *Sensors* **2021**, *21*, 2410. [[CrossRef](#)] [[PubMed](#)]
112. Kumar, A.; Das, D. IntelligentChain: Blockchain and Machine Learning based Intelligent Security Application for Internet of Vehicles (IoV). In Proceedings of the 2022 IEEE 95th Vehicular Technology Conference (VTC2022-Spring), Helsinki, Finland, 19–22 June 2022; pp. 1–5.
113. Wang, Y.; Tian, Y.; Hei, X.; Zhu, L.; Ji, W. A novel IoV block-streaming service awareness and trusted verification scheme in 6g. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5197–5210. [[CrossRef](#)]
114. Wu, J.; Jin, Z.; Li, G.; Xu, Z.; Fan, C.; Zheng, Y. Design of vehicle certification schemes in IoV based on blockchain. *World Wide Web* **2022**, *25*, 2241–2263. [[CrossRef](#)]
115. 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](#)]
116. Kumar, A.; Das, D. EIoVChain: Towards Authentication and Secure Communication Based Blockchain for Internet of Vehicles (IoV). In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, VIC, Australia, 6–8 December 2021; pp. 47–54.
117. Shen, M.; Lu, H.; Wang, F.; Liu, H.; Zhu, L. Secure and Efficient Blockchain-Assisted Authentication for Edge-Integrated Internet-of-Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 12250–12263. [[CrossRef](#)]
118. Xu, G.; Bai, H.; Xing, J.; Luo, T.; Xiong, N.N.; Cheng, X.; Liu, S.; Zheng, X. SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles. *J. Parallel Distrib. Comput.* **2022**, *164*, 1–11. [[CrossRef](#)]
119. Liu, X.; Wang, L.; Li, L.; Zhang, X.; Niu, S. A Certificateless Anonymous Cross-Domain Authentication Scheme Assisted by Blockchain for Internet of Vehicles. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3488977. [[CrossRef](#)]
120. Feng, X.; Cui, K.; Wang, L. PBAG: A Privacy-Preserving Blockchain-based Authentication Protocol with Global-updated Commitment in IoV. *arXiv* **2022**, arXiv:2208.14616.
121. Gupta, M.; Kumar, R.; Shekhar, S.; Sharma, B.; Patel, R.B.; Jain, S.; Dhaou, I.B.; Iwendi, C. Game theory-based authentication framework to secure internet of vehicles with blockchain. *Sensors* **2022**, *22*, 5119. [[CrossRef](#)] [[PubMed](#)]
122. Abbes, S.; Rekhis, S. A blockchain-based solution for reputation management in IoV. In Proceedings of the 2021 IEEE International Wireless Communications and Mobile Computing (IWCMC), Harbin, China, 28 June–2 July 2021; pp. 1129–1134.
123. Golam, M.; Lee, J.M.; Kim, D.S. A UAV-assisted blockchain based secure device-to-device communication in Internet of military Things. In Proceedings of the 2020 IEEE International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 21–23 October 2020; pp. 1896–1898.
124. Chattaraj, D.; Bera, B.; Das, A.K.; Saha, S.; Lorenz, P.; Park, Y. Block-clap: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8092–8107. [[CrossRef](#)]
125. Vishwakarma, L.; Nahar, A.; Das, D. LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-enabled IoV. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5983–5994. [[CrossRef](#)]
126. Badshah, A.; Waqas, M.; Muhammad, F.; Abbas, G.; Abbas, Z.H.; Chaudhry, S.A.; Chen, S. AAKE-BIVT: Anonymous Authenticated Key Exchange Scheme for Blockchain-Enabled Internet of Vehicles in Smart Transportation. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 1739–1755. [[CrossRef](#)]
127. Elkhail, A.; Zhang, J.; Elhabob, R. An efficient heterogeneous blockchain-based online/offline signcryption systems for internet of vehicles. *Clust. Comput.* **2021**, *24*, 2051–2068. [[CrossRef](#)]
128. Liu, J.; Zhang, L.; Li, C.; Bai, J.; Lv, H.; Lv, Z. Blockchain-based secure communication of intelligent transportation digital twins system. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 22630–22640. [[CrossRef](#)]
129. Ye, X.; Li, M.; Si, P.; Yang, R.; Wang, Z.; Zhang, Y. Collaborative and Intelligent Resource Optimization for Computing and Caching in IoV With Blockchain and MEC Using A3C Approach. *IEEE Trans. Veh. Technol.* **2022**, *72*, 1449–1463. [[CrossRef](#)]
130. Alotaibi, J.; Alazzawi, L. Safiov: A secure and fast communication in fog-based internet-of-vehicles using sdn and blockchain. In Proceedings of the 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), Lansing, MI, USA, 9–11 August 2021; pp. 334–339.
131. Kumar, A.; Das, D. SIOVChain: Efficient and Secure Blockchain Based Internet of Vehicles (IoV). In Proceedings of the 23rd International Conference on Distributed Computing and Networking, Delhi, India, 4–7 January 2022; pp. 284–289.
132. Ahmed, M.; Moustafa, N.; Akhter, A.S.; Razzak, I.; Surid, E.; Anwar, A.; Shah, A.S.; Zengin, A. A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 19624–19633. [[CrossRef](#)]
133. Yaguchi, Y.; Wakazono, T. Flight Plan Management System for Unmanned Aircraft Vehicles Using Blockchain. In Proceedings of the 2021 IEEE International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 15–18 June 2021; pp. 1648–1652.
134. Azam, F.; Biradar, A.; Priyadarshi, N.; Kumari, S.; Almakhlles, D.; Tangade, S. A Framework for Secured Dissemination of Messages in Internet of Vehicle (IoV) Using Blockchain Approach. In Proceedings of the 2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNBC), Tumkur, Karnataka, India, 3–4 December 2021; pp. 1–6.
135. Liu, H.; Zhu, R.; Wang, J.; Xu, W. Blockchain-Based Key Management and Green Routing Scheme for Vehicular Named Data Networking. *Secur. Commun. Netw.* **2021**, *2021*, 3717702. [[CrossRef](#)]

136. Chen, Y.; Hao, X.; Ren, W.; Ren, Y. Traceable and authenticated key negotiations via blockchain for vehicular communications. *Mob. Inf. Syst.* **2019**, *2019*, 5627497. [\[CrossRef\]](#)
137. Kim, S.K.A. Enhanced IoV security network by using blockchain governance game. *Mathematics* **2021**, *9*, 109. [\[CrossRef\]](#)
138. Gupta, D.S.; Karati, A.; Saad, W.; da Costa, D.B. Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3255–3266. [\[CrossRef\]](#)
139. Baza, M.; Amer, R.; Rasheed, A.; Srivastava, G.; Mahmoud, M.; Alasmay, W. A blockchain-based energy trading scheme for electric vehicles. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–7.
140. Ayaz, F.; Sheng, Z.; Tian, D.; Nekovee, M.; Saeed, N. Blockchain-empowered AI for 6G-enabled Internet of Vehicles. *Electronics* **2022**, *11*, 3339. [\[CrossRef\]](#)
141. Chung, W.J.; Cho, T.H. A security scheme based on blockchain and a hybrid cryptosystem to reduce packet loss in IoV. *Int. J. Adv. Technol. Eng. Explor.* **2021**, *8*, 945. [\[CrossRef\]](#)
142. 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. [\[CrossRef\]](#)
143. 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, Fukushima, Japan, 30 January–2 February 2021; pp. 1–8.
144. Chai, H.; Leng, S.; He, J.; Zhang, K.; Cheng, B. CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-preserving Authentication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *71*, 4620–4631. [\[CrossRef\]](#)
145. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Kumar, N. P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 22571–22582. [\[CrossRef\]](#)
146. 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. [\[CrossRef\]](#)
147. Ren, Y.; Zhu, F.; Wang, J.; Sharma, P.K.; Ghosh, U. Novel vote scheme for decision-making feedback based on blockchain in internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 1639–1648. [\[CrossRef\]](#)
148. Xu, S.; Chen, X.; He, Y. EVchain: An anonymous blockchain-based system for charging-connected electric vehicles. *Tsinghua Sci. Technol.* **2021**, *26*, 845–856. [\[CrossRef\]](#)
149. 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. [\[CrossRef\]](#)
150. Guo, Y.; Wan, Z.; Cui, H.; Cheng, X.; Dressler, F. Vehicloak: A Blockchain-Enabled Privacy-Preserving Payment Scheme for Location-Based Vehicular Services. *IEEE Trans. Mob. Comput.* **2022**, 1–9. [\[CrossRef\]](#)
151. Knirsch, F.; Unterweger, A.; Engel, D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Comput.-Sci.-Res. Dev.* **2018**, *33*, 71–79. [\[CrossRef\]](#)
152. Lai, C.; Zhang, M.; Cao, J.; Zheng, D. SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates. *IEEE Internet Things J.* **2019**, *7*, 416–428. [\[CrossRef\]](#)
153. 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. [\[CrossRef\]](#)

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