An Overview of Internet of Vehicles Based on Blockchain

School of Computer Science and Technology
Shandong University
Qingdao, Shandong

***Abstract*—This paper mainly discusses the theoretical scheme of the Internet of Vehicles based on blockchain in the current academic circle, explores their physical architecture and methods for specific requirements, and hopes to help researchers who are new to this field to get familiar with the work done by predecessors more quickly.**

***Index Terms*—Blockchain, Internet of vehicle, Security, Efficiency**

I. Introduction

With the improvement of semiconductor technology, we have higher computing power chips, higher I/O speed and larger capacity memory. The maturity and application of communication technology represented by 5G has made the speed of information dissemination reach a qualitative leap. The door of the information age is slowly expanding to human beings.This is also the era of vehicle. The excellent vehicles and developed road system make us communicate more frequently in real life.When the information age meets the automobile age, the automobile networking comes into being. We install micro-private computers on the vehicle, set up private networks for them, record and exchange these rich data.These data have brought a new revolution in modern society: operation information generated by driving a car, road condition information generated by in-vehicle sensors, and various service information provided to the car, all of which make us advance to a smarter, more convenient and more human-oriented era.

According to a survey, in today's era of information explosion, there are 2.5 quintillion bytes of new data generated every day. However, in this process, we should realize that there are many urgent problems to be solved in the vehicle networking system.For example, how to solve the problem of privacy data in information sharing? how to solve the problem of information synchronization between vehicles in a large geographic range? how to solve the problem of data security and authenticity? If these problems cannot be solved, then our car networking system will always remain in the imagination. Fortunately, these problems have been largely solved by the introduction of blockchain technology.

In this article, we mainly investigate and compare the application schemes of blockchains in internet of vehicle (IOV). Because the technology of IOV and blockchain is a new computer technology, most of the current schemes of IOV + blockchain are in the initial stage of theoretical analysis and exploratory implementation.However, in the paper based on theoretical analysis, many articles have proposed a new and reasonable architecture of IOV + block chain, and introduced some more efficient and reasonable blockchain consensus algorithm ideas (such as POS, DPOS) into the architecture, which solved the trust, data privacy and efficiency problems in the vehicle networking system. Among the scenarios for specific applications, the electric vehicle charging system [49] [51] [61] [64] [87] [90] [95] [96] [110] [133] [143] [156] [186] and the Intelligent Transportation system are the most popular, and they have been improved several times to have high usability. Other applications such as insurance industry [40], traffic accident detection, smart city [52] [70] are still in a relatively early stage, which will have a great development space in the future. Next, we will analyze the development status of blockchain in the application of IOV one by one.

II. Background and Related Work

In this section, we provide background knowledge on blockchain.

A. Blockchain

The blockchain technology stems from Bitcoin, invented by an anonymous researcher named Satoshi Nakamoto Although the blockchain was initially designed to realize a decentralized cryptocurrency, it has been endowed with programmability to become a fully functional consensus computer. The blockchain capable running smart contracts has found tremendous applications in many areas.

A blockchain system consists of a group of participants called miners to maintain a distributed ledger, i.e. the blockchain, using a consensus algorithm (e.g.Proof-of-Work, PBFT). The blockchain is a special data structure formed by blocks chained together. A block is a container of transactions, which lead to state transition of the blockchain. E.g. a fund transfer transaction leads to state transition of relevant accounts. Each block is generated by a miner and added to the blockchain through the consensus algorithm.

The blockchain systems like Bitcoin are completely decentralized without any trusted parties. They are also unalterable because the blockchain is maintained by provably secure consensus algorithms. Thus the blockchain can be used to prove existence of valuable information, like intelligence property rights, property ownership certificates etc.

B. Internet of Vehicle

********** [46] [53] [69] [72] Buzachis A et al. [77] propose an effective system combining blockchain technology to support the communication and transaction between entities. In order to avoid the collision of the road intersection, the scheme combines the hypeleger fabric (HLF) and frfp algorithm to verify whether all automous vehicles have the same block version (such as the same priority list), so as to avoid the collision of road intersections; and in case of inconsistency, emergency measures are taken to avoid any accidents.

In [80], the energy ecosystem in the Ethereum blockchain network is designed to record all processes from power generation to end users. Participants in this scheme include energy producers, consumers, distributors, dealers, charging stations and electric vehicle users, and transactions between participants are completed on smart contracts. In applications developed using smart contracts, users can access information such as the location of the relevant charging station, price list, payment type, charging method, charging type, and plug type. In addition, the program uses PROMETHEE, a multi-criteria decision-making method, to provide quotations based on user characteristics. Erdin E et al. [105] design and implement a payment system based on bitcoin for EV charging network payment. The system establishes a payment network with permission and signature parallel to the main ledger, which eliminates the transaction cost in bitcoin payment.

III. Introduction

With the improvement of semiconductor technology, we have higher computing power chips, higher I/O speed and larger capacity memory. The maturity and application of communication technology represented by 5G has made the speed of information dissemination reach a qualitative leap. The door of the information age is slowly expanding to human beings.This is also the era of vehicle. The excellent vehicles and developed road system make us communicate more frequently in real life.When the information age meets the automobile age, the automobile networking comes into being. We install micro-private computers on the vehicle, set up private networks for them, record and exchange these rich data.These data have brought a new revolution in modern society: operation information generated by driving a car, road condition information generated by in-vehicle sensors, and various service information provided to the car, all of which make us advance to a smarter, more convenient and more human-oriented era. According to a survey, in today's era of information explosion, there are 2.5 quintillion bytes of new data generated every day. However, in this process, we should realize that there are many urgent problems to be solved in the vehicle networking system.For example, how to solve the problem of privacy data in information sharing? how to solve the problem of information synchronization between vehicles in a large geographic range? how to solve the problem of data security and authenticity? If these problems cannot be solved, then our car networking system will always remain in the imagination. Fortunately, these problems have been largely solved by the introduction of blockchain technology.

In this article, we mainly investigate and compare the application schemes of blockchains in internet of vehicle (IOV). Because the technology of IOV and blockchain is a new computer technology, most of the current schemes of IOV + blockchain are in the initial stage of theoretical analysis and exploratory implementation.However, in the paper based on theoretical analysis, many articles have proposed a new and reasonable architecture of IOV + block chain, and introduced some more efficient and reasonable blockchain consensus algorithm ideas (such as POS, DPOS) into the architecture, which solved the trust, data privacy and efficiency problems in the vehicle networking system. Among the scenarios for specific applications, the electric vehicle charging system and the Intelligent Transportation system are the most popular, and they have been improved several times to have high usability. Other applications such as insurance industry, traffic accident detection, automobile sales and maintenance are still in a relatively early stage, which will have a great development space in the future. Next, we will analyze the development status of blockchain in the application of IOV one by one.

IV. Several physical layer architectures of blockchain

Before talking about the Internet of vehicles + blockchain, let's take a look at how the common Internet of things is built. Based on the investigation of the blockchain architecture scheme of the Internet of things, three kinds of blockchain architectures are summarized in the schem of Reyna, A. et al. [18]. Ali et al. [6] on the basis of the previous, summarized the general structures of 4 Blockchains, which are as follows:

- IOV devices as transaction-issuers to the blockchain
- Gateway devices as end-points to the blockchain
- Interconnected edge devices as end-points to the blockchain
- Cloud-blockchain hybrid with the IoT edge

And the Internet of vehicles + blockchain solutions mostly follow these architectures.

A. IOV devices as transaction-issuers to the blockchain

Relatively speaking, "Devices as transaction - issuers to the blockchain" is the most easy architecture to implement in hardware and software, because it does not require additional infrastructure services. However, due to the limitations of on board unit(OBU) computing capacity and communication capacity, such an architecture is more suitable for application scenarios with low interactive data volume and low real-time requirements. In the scheme of Yang, Z., et al., [2], vehicles can form a cluster with vehicles with similar driving routes in their communication range, and vehicles in the cluster will directly interact with data. Each cluster will maintain a blockchain network independently, and the vehicles within the cluster will package the data interaction information into transactions, broadcast and verified within the cluster, and finally generate blocks through an improved PoW consensus

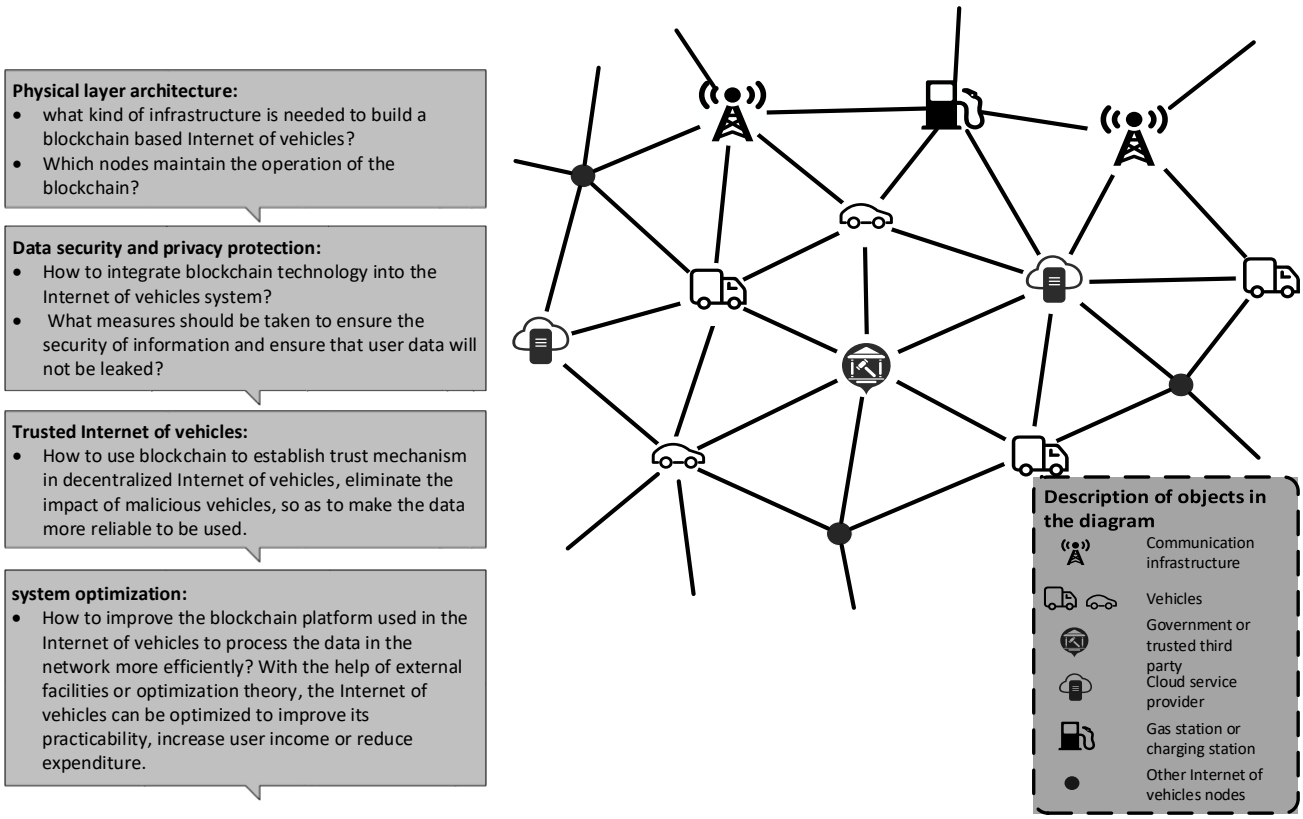


Fig. 1. Overview of Internet of Vehicles Based on Blockchain

algorithm. Although this scheme takes into account the limited communication capacity of cars and controls the communication range in a small cluster, it still has great usability and universality problems: One of the problems is whether on-board unit can meet PoW's demand for computing power. In addition, it is difficult to find a stable vehicle cluster for a long time. Clusters of unfamiliar cars will disintegrate within a few hours, with the Vehicles will enter different clusters. Moreover, the scope boundary of the cluster is difficult to determine. In such a scenario, two vehicles, perhaps only a few meters apart, would not be able to interact with data because they did not belong to the same cluster. In my opinion, this scheme can only be applied to the information records on a particular road or the information exchange records of the transport fleet, where the latter can use the private chain to avoid the onerous consensus process. Dorri, A. et al. [13] supposes that nodes in the Internet of vehicles (can be smart vehicles, OEMs (original Equipment manufacturers), Vehicle Assembly Lines, Software providers, Cloud Storage providers, And mobile devices of users such as smartphones, tablets) are directly responsible for the propagation and verification of transactions, the generation and verification of blocks and other blockchain functions. But the advantage of the scheme is that it maintains a blockchain of information about all vehicles and vehicle services in the Smart Vehicles system, and vehicles

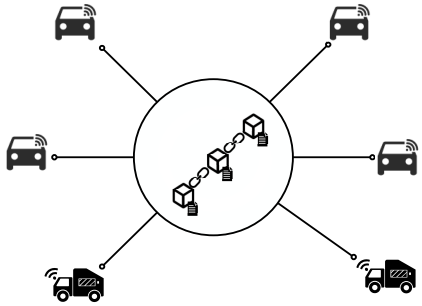


Fig. 2. IOV devices as transaction-issuers to the blockchain

do not have to switch between different blockchain networks. At the same time, in order to reduce the traffic in the network so as to expand the system scale, the scheme divides the nodes into smaller clusters. Each cluster chooses cluster head as overlay Block Managers (OBMs) to deal with the transactions within the cluster, and broadcasts them as transactions into the blockchain, and is also responsible for generating or verifying the blocks. Considering the location change of vehicles often, it also puts forward the soft handover method for dynamic partition clustering to reduce the network delay.

The same architecture is also adopted in the cheme of Demir, M.et al. [10], enabling individual drivers, business

organizations such as Insurance companies, and governments agencies and other participants to directly form a Blockchain network for storing and managing Vehicle Insurance information. Considering the high reliability of the participants and the low computing power, permissioned blockchain is adopted to avoid wasting time in reaching a consensus. In order to avoid the risk of information leakage caused by malicious behavior (such as the vehicle's itinerary and the owner's identity privacy information), the vehicle chooses a pair from several different asymmetric key pairs at a time to encrypt the uploaded information. This information is opened with the corresponding private key when it needs to be disclosed to a specific participant, such as insurance claims after an accident. This scheme takes advantage of the fact that the information recorded on the block chain could not be tamped, so as to ensure data integrity, and also proposes to add advanced cryptographic techniques such as the Zero Knowledge proofs and bilinear Pairings into the privacy protection in the future proofs.

Awais Hassan M et al. [199] present a warning message release system without any roadside units. The warning messages exchanged between vehicles include lane change warning, blind spot warning, frontal collision, intersection assistance, etc. In addition, each vehicle is assigned a reputation value stored in the blockchain to evaluate the sender (vehicle) of the warning message to distinguish malicious vehicles from honest vehicles

B. Gateway devices as end-points to the blockchain

Many solutions are adopted reasonable "Gateway devices as end - points to the blockchain" architecture, basic way is to use a fixed location computing facilities (such as RSU, Road Side Unit) as a Gateway to blockchain to transmit data and reach a consensus. On-board Unit responsible for data collection and transmission, it largely reduce the on-board Unit burden of computation and communication. For example: in the scheme of Yuan Y et al. [24], common vehicles and sensor-rich vehicles transmit information only via MECN (Mobile Edge Computing Node, similar to RSU). MECN stores the location information of landmark, collects the vehicles sent by Sense-rich vehicles corresponding to the location information of landmark, and sends the modified GPS data to all vehicles. At the same time, all these operations are written to the block. Finally, MECNs complete the consensus algorithm and validates it.The same framework applies to the scheme of Rathee G et al. [125].

On the basis of the scheme of Gandhi G M et al. [44], Jiang X et al. [42] proposes a novel distributed deep learning (DDL) framework supporting blockchain to improve the performance of automatic driving object detection. The vehicle will collect the driving information of a certain road section and send it to the MEC node (mobile edge computing) through transaction. MEC node is responsible for packing the data to the block (by completing the consensus algorithm), modeling the collected data through deep learning, and sharing the data model with the vehicle. In this framework, the author also proposes a model called YOLOv2 to train the model using distributed transfer learning.

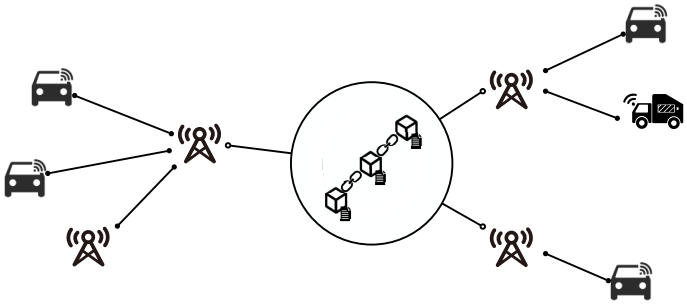


Fig. 3. Gateway devices as end-points to the blockchain

C. Interconnected edge devices as end-points to the blockchain

The difference with this architecture is that it allows direct communication between vehicles, rather than having to pass all the information through the blockchain. It is very effective in reducing communication delays between vehicles and reducing blockchain traffic, and data producers have some freedom to choose what data is broadcast. Therefore, it is suitable for those applications with frequent information exchange and low tolerance of communication delay, such as intelligent traffic systems, accident detection systems, etc. The architecture is used in the scheme of Leiding, B. et al. [21] and Ethereum is used on this basis to build a blockchain network suitable for various Application scenarios such as Traffic Regulation Application (TRA) and Vehicle Tax. Shrestha, R. et al. [15] basically also adopted such a framework, and proposes that the RSU can provide Proof-of-Locaiton (PoL), providing the location of nearby vehicles, to enhance the credibility of the data in the system (preventing malicious participants from fabricating data about a place when they have not arrived at all). The scheme is still at an early stage of exploration and therefore not feasible: it does not take into account possible attacks on Rsus or vehicles, and the disinformation dissemination and information leakage resulting from such attacks. In addition, it has no incentive for vehicles to share data, which may discourage owners from broadcasting real and valid data to the network. However, many researchers have proposed further solutions to privacy protection and data sharing incentives, which we will discuss later.

Leiding B et al. [83] proposes a blockchain based system to support manufacturer agnostic platform solutions, which allow VANET participants to provide and trade any type of services and goods. In the scheme, "vehicle to vehicle" and "vehicle to infrastructure" communication modes are supported in the blockchain system.

D. Cloud-blockchain hybrid with the IoV edge

This architecture combines the strengths of previous architectures in a more flexible way to build blockchains. Vehicles have a choice to use the blockchain for certain Interaction

Ref.	Design goal	Target	Physical layer architectures	Other features	Blockchain
[2]			1st	Divide vehicles into clusters	
[13]			1st	Divide nodes into clusters	
[10]	storing and managing Vehicle Insurance information	Insurance companies and governments agencies	1st	Vehicle can choose a pair from several different asymmetric key pairs at a time to encrypt information	permissioned blockchain
[199]	warning message release	Vehicle driver	1st	Reputation evaluation	
[24]	intelligent transportation systems	Vehicle driver	2nd		
[125]	online cab booking services	Connected vehicles	2nd	CV as a Service	
[42]	automatic driving object detection	Autonomous vehicle	2nd	Distributed deep learning	
[21]	Traffic Regulation Application (TRA) and Vehicle Tax	Governments agencies	3rd		Ethereum
[15]	message dissemination in VANET	VANET	3rd	Proof-of-Locaiton	
[83]	V2X economy	VANET	3rd	Use IPFS	Ethereum
[12]	vehicular services	vehicular edge computing and networks	4th	reputation-based data sharing scheme	blockchain and smart contract
[20]	data analysis and service delivery	Vehicle	4th		
[32]	carpooling	passenger and the driver	4th	conditional privacy, one-to-many proximity matching and data auditability	
[36]	develop collaboration between clouds of different automakers	different automakers and vehicle driver	4th		

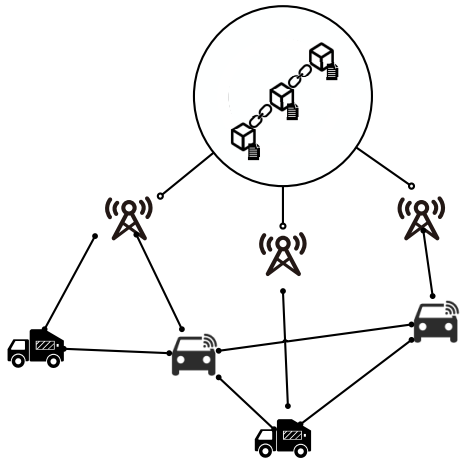


Fig. 4. Interconnected edge devices as end-points to the blockchain

Events, and the remaining Events occur directly between vehicle. At the same time, vehicles with high vehicle-mounted unit performance can serve as nodes in the blockchain network and directly participate in various transactions of the blockchain. However, and those vehicles with limited performance can generate transactions by transferring data to gatway devices. In addition, vehicles in the network can also use fog computing, high-performance database to overcome the performance bottleneck of some on-board computing units.

Nadeem, S. et al. [20] use the fog compute node between roadside unit's cloud and blockchain based distributed cloud. Each fog-based small Cloud covers a small associated network responsible for secure data analysis and service delivery with minimal latency.

using blockchain-assisted vehicular fog computing, Li M et al. [32] propose an efficient and privacy-preserving carpooling scheme with conditional privacy, one-to-many proximity matching, target matching and data auditability. In the scheme, fog computing nodes are introduced to enable local matching between passengers and drivers, and private blockchain is constructed by RSU. Through the private proximity test with

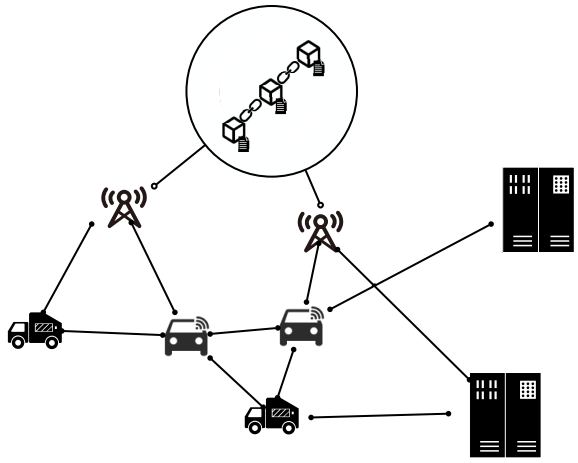


Fig. 5. Cloud-blockchain hybrid with the IoV edge

location tags, it achieves one-to-many proximity matching of the current location, and on this basis, establishes the only secret key between the passenger and the driver. In addition, the scheme divides the carpooling area into grids, and effectively realizes the matching of the drop-off locations through range query technology. Vehicles from different automakers have their own private clouds, and the collaboration between them is poor, resulting in inefficient collaboration between heterogeneous vehicles. Therefore, it is an inevitable trend to develop collaboration between clouds. Yin B et al. [36] propose a multi-vehicle cloud collaboration framework called JointCloud, introduce the coordination mechanism established by the blockchain, and describes in detail the vehicle cloud service standardization method and service composition method. Finally, it designs a distributed cloud service evaluation method based on blockchain to provide users with an effective cloud service evaluation solution.

In the IOV based on blockchain, data will flow among different participants to help the vehicle or system managers make decisions.During blockchain generation, miners verify the validity of transactions broadcast on the network and verify blocks after the consensus algorithm generates them, which ensures that the data on blockchain is in conformity with the norms. However, this is not enough to meet our needs. Blockchain is a decentralized, distributed system in which data is generated and uploaded by multiple parties.In most of the blcokchain + IOV scheme based on public chain, there is no way to ensure that all participants are honest and correct, in other words, malicious participants may upload false data in the correct format (such as For example, a vehicle broadcasts the traffic jam information that does not exist on its own route to the blockchain network in order to facilitate its travel, so that other vehicles receiving the information will choose other routes) to reduce the credibility of information in the blockchain. In order to solve the credibility problem of data on the platform, some schemes put forward the credibility evaluation scheme, which evaluates the credibility of the data producer (vehicle) or data processor (such as RSU), so that the decision maker of the vehicle or system can make the most correct decision based on the information.

E. Classification based on trust value generation hierarchy

Due to the differences in infrastructure and application scenarios in the Internet of Vehicles, the trust problem is very complex and the solutions are various. According to the level of trust value generation, Trust Management Models can be divided into three categories: Entity-oriented Trust Model, data-oriented Trust Model, and combined Trust Model.

1) **Entity-oriented trust model:** :

This model focuses on predicting the likelihood that the vehicle will behave honestly based on its historical experience, rather than on the reliability of the transactions or information submitted. Yang, Z., et al. [2] and Lu, Z., et al., [3] proposed that the credit value stored on the block chain is only for vehicles, and the credit value is evaluated and updated by the history of the vehicle.Taking Lu, Z., et al., [3] as an example, there exists A reliable and highly secure law enforcement authority (LEA) in the system to collect information related to the credibility of blockchain networks. The vehicle improves its credit when sending authentic messages, and reduces its credit when sending the wrong forged messages to deceive other vehicles. Besides, it also improves its credit when testifying for correct messages or reporting wrong messages on the network. When the vehicle's credit value is reduced to zero, the RSU node responsible for block chain maintenance will no longer broadcast the message sent by the vehicle.

Cui J et al. [113] proposes a reputation system managed by TA to reduce untrusted messages in 5G-enabled vehicular networks. The reputation system consists of three modules: feedback collection module, reputation calculation module and reputation update module. The solution uses a weighted sum method and set the user's reputation value as the initial score of the vehicle to solve the cold start problem, and on this basis uses multi-weighted to accurately update the reputation of different messages and vehicle conditions in the RSMA. Those vehicles whose reputation scores are lower than the threshold cannot participate in communication. Khelifi H et al. [195] propose a secure NDN caching scheme based on a blockchain network. Each cache store is assigned a reputation value, which increases/decreases according to the content provided.

2) **Data-oriented trust model:** : This model focuses on the credibility of the event or information and is not interested in the participants of the event or the sender of the information. To some extent, this model improves the workload and complexity of the credibility evaluation system: the amount of data in the network is much more than the number of vehicles, and data has no historical information for reference. But it can improve the utilization of information, so that the information submitted by dishonest vehicles can also be used. At the same time, it also reduces the risk of system attack: the original honest vehicle may submit wrong data due to accidental error or attack, and the system will not be disturbed by the vehicle history when evaluating the information. Pu Y, et al. [73] proposes an efficient, reliable, and privacy-protected

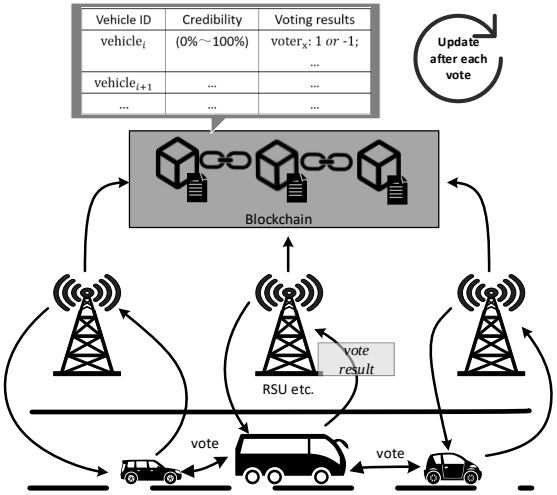


Fig. 6. Entity-oriented trust model

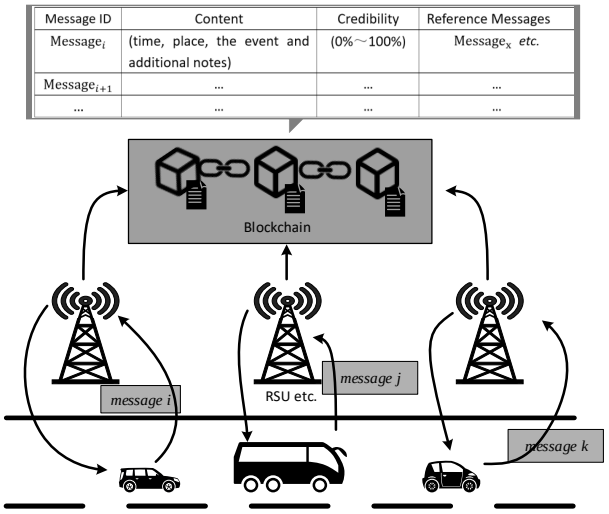


Fig. 7. Data-oriented trust model

blockchain-based solution for vehicular social networks. The scheme uses a pseudonym mechanism to achieve personal anonymity by hiding the identity of the vehicle. In addition, in order to encourage vehicles to report credible information, an incentive and punishment mechanism is proposed. At the same time, the papaer propose an evaluation mechanism based on multi-factor and single-factor weight to evaluate the reliability of the message. In addition, practical Byzantine fault-tolerant technology (PBFT) and blockchain are used to achieve consensus and store records respectively to prevent malicious entities from manipulating the reward score and credit score of the vehicle. In order to defend the CV-based traffic signal control system from malicious data attacks, Li W et al. [106] design a blockchain-based decentralized architecture. The architecture uses the Hyperledger Fabric framework as a development platform, and introduces a customized blockchain network for connected vehicles and a consensus protocol design for verifying source data. For the consensus protocol, the authors designed a new mechanism to prevent attackers from sending deception source information to the blockchain network. In the scheme, roadside units (RSUs) and witness vehicles are used as references for other nodes in the network to verify each vehicle information and then permanently record it in the blockchain network.

3) **combined trust model:** :

This model combines the two approaches described earlier. It uses the credibility of the entity that generates the data as a reference for data credibility evaluation, or evaluates the credibility of the corresponding entity according to the data credibility that the entity generates. In the scheme of Luo B. et al. [11], because k-anonymity is used as a tool to prevent information leakage, K mutual trusted vehicles need to cooperate with each other and mix their messages with each other. If there are malicious participants involved in the process, it is easy to cause information leakage, so vehicles must choose vehicles with high reputation to cooperate. In order to prevent malicious vehicles from quickly disguised as trusted vehicles before destructive behaviors, or on-off attacks by maintaining high reputation in the network, this scheme gives the same weight to historical trust information and the current behaviors evaluation.

F. Classification based on trust value generation role

1) **Credibility of vehicle or vehicle service provider:** :

In Yang Z. et al. [2], the vehicle will vote for the information generated by the on-board sensors on other vehicles according to the information it has. If it is correct, the vote for the information is 1, otherwise the vote is - 1. In addition, trusted authority (TA) will score the performance (accuracy, range) of sensor units loaded on the vehicle, and give higher probability to those vehicles with higher sensor performance when selecting miner nodes in the vehicle cluster. When the vehicle node is selected as the miner, it will package its voting results on other vehicles in the cluster in the block and send them to all other vehicles in the cluster. Other vehicles will check the miner's qualification, the signature of the block, and accept the updated rating results in the case of ratings recorded in the block do not conflict with their local ratings. This scheme relies on the performance score of vehicle sensors made by TA. Malicious nodes may attack TA or forge sensor performance, which will affect the information reliability of the whole system.

Yang Z. et al. [14] have made some modifications on the basis of the scheme of Lu Z. et al. [3]: vehicles are only the producers of data (from onboard sensors) and rating, and RSUs are added to collect vehicle voting information and evaluate vehicle reputation value, and respond to queries on other vehicle reputation values sent by vehicles. RSU is also responsible for collecting and broadcasting sensor information

and rating results uploaded by vehicles, and generating blocks through consensus algorithm. Considering that if the RSU with more information is used to generate blocks, more information will be confirmed earlier, which will improve the efficiency of the whole system, this paper proposes a PoW(proof of work) + PoS(proof of stake) consensus algorithm, which takes the sum of absolute values of offsets in the candidate block as the stage, and the nodes with more stages have lower PoW difficulty. This paper also analyzes several risks faced by the reputation management system of the Internet of vehicles:

- **malicious vehicles:**
  - Message spoofing attack
  - Bad mouthing and ballot stuffing attack.
- **Compromised RSU.**

Chai H. et al. [19] follow the basic idea of the scheme of Yang Z. et al [14] and provide a solution for the sharing of computing resources between vehicles in the blockchain based Internet of vehicles: task owners (TOS) vehicle intend to offload their computing tasks to an advanced resource providers (RPs) vehicle to implementation cooperative computing. During this process, the TOs will use a digital cryptocurrency called Resource Coins to pay the RP for the resources it provides. Each vehicle determines its role (Tos or RPs) according to its service requirements and resource availability, and sends these information to the blockchain network in the form of transactions to trigger smart contracts to seek matches. After completion of the transaction, TOs will check the integrity and correctness of the RPs' operating results, and generate reputation for RPs in the form of a transaction. Each time the RSU collects a certain number of transactions, a block is automatically generated and the reputation sum of all transactions in the block is recorded. PoR consensus algorithm requires all nodes to select the block with the highest total reputation in the current slot to join the block chain, so as to ensure that transactions with high credibility are confirmed in priority. Malik N. et al. [25] also use the way of Yang Z. et al. [14] for vehicles to evaluate each other and stores credit information in Interplanetary File systems (IPFS) , and vehicles can quickly get credit information through the lightweight blockchain.

Singh M. et al. [26] no longer uses the method of voting evaluation to generate credit value, but uses an encrypted credential similar to Bitcoin – Trust Bit to establish Trust in the system. Each Trust bit has a unique ID issued by the vehicle's dealer or Authorized Dealer and is earned by the vehicle after completing a certain amount of computing in group Communication. Bit Trust increases with the amount of computation completed by the vehicle, indicating that the vehicle has higher respect and honor. The assumption of this scheme is that when vehicles contribute more to the system, they will also obtain higher profits, so the cost of taking malicious actions is higher, and rational participants will be more inclined to participate in the communication between vehicles honestly. This is consistent with the reality. Li L. et al. [16] also adopts A similar digital currency, CreditCoin. When the vehicle initiates and uploads A correct information, it will invite other witnesses to sign the information together. Correct uploads will make the initiators and participants get rewards. Otherwise, they will be punished. Singh M et al. [123] [128] [135] and [178] propose a reward-based IV (intelligent vehicle) communication based on blockchain technology. The program uses crypto IV-TP to protect the privacy of IV. In addition, IV-TP provides an efficient communication channel between IVs and also helps to detect the detailed history of IV communication. IV's communication history and reputation will be stored on the VC and will be available to authorized institutions for inspection if necessary.

Lu Z. et al. [7] uses Law Enforcement Authority (LEA) to monitor vehicle behavior and evaluate the reputation value of each vehicle. Besides rewarding good and evil behaviors. It also encourages the reporting of malicious behaviors.In this scenario, vehicle information is divided into three levels according to importance:

- LV.1 Emergency (vehicle loss of control, etc.) broadcast.
- LV.2 State of vehicle operation (braking, turning).
- LV.3 Broadcast poor road Conditions.

The influence of information within The network was also taken into account: D_r is The relative density of vehicles, D_r=D/D_aver, D_aver is set to 20 vehicles per Km. Compared with simple mutual voting, it has certain superiority to choose the reward and punishment intensity of the vehicle's good or bad behavior from the importance degree and influence range of information. However, the use of a centralized node LEA as a supervisor and evaluator may lead to a potential risk of being targeted. Kandah F et al. [48] use the design in the scheme of Ying Z. et al. [45] and Yang Z. et al. [2] ,and establish novel vehicle reputation evaluation system. When a vehicle enters a geographical area within the RSU's jurisdiction, the vehicle sends a beacon message (Mbeacon) indicating its availability and willingness to participate in the system. After receiving the beacon information, RSU will start to form a platoon according to the availability and proximity of vehicles, and send the latest information of blockchain to it. After the anonymous identity is generated, the vehicle completes information interaction and the proof of interaction (POI) update in the platoon. After a set of interactions, the members of the platoon will select a miner who is responsible for creating blocks in the platoon blockchain (PB) as specified in the mining and validation of the platoon section. When a platoon block is formed and mined on the blockchain, each vehicle will update the trust value of its neighboring vehicles according to the response received by the previous context. Finally, after generating a specified number of blocks in the platoon, or based on the RSU's request to mine in the global blockchain, the platoon members will select a miner to send the platoon blockchain into the global blockchain for mining.

Based on the permissioned blockchain technology, Su Z. et al. [50] propose a secure electric vehicle charging framework. In this framework, pre-selected electric vehicles can publicly audit and share transaction records without relying on trusted

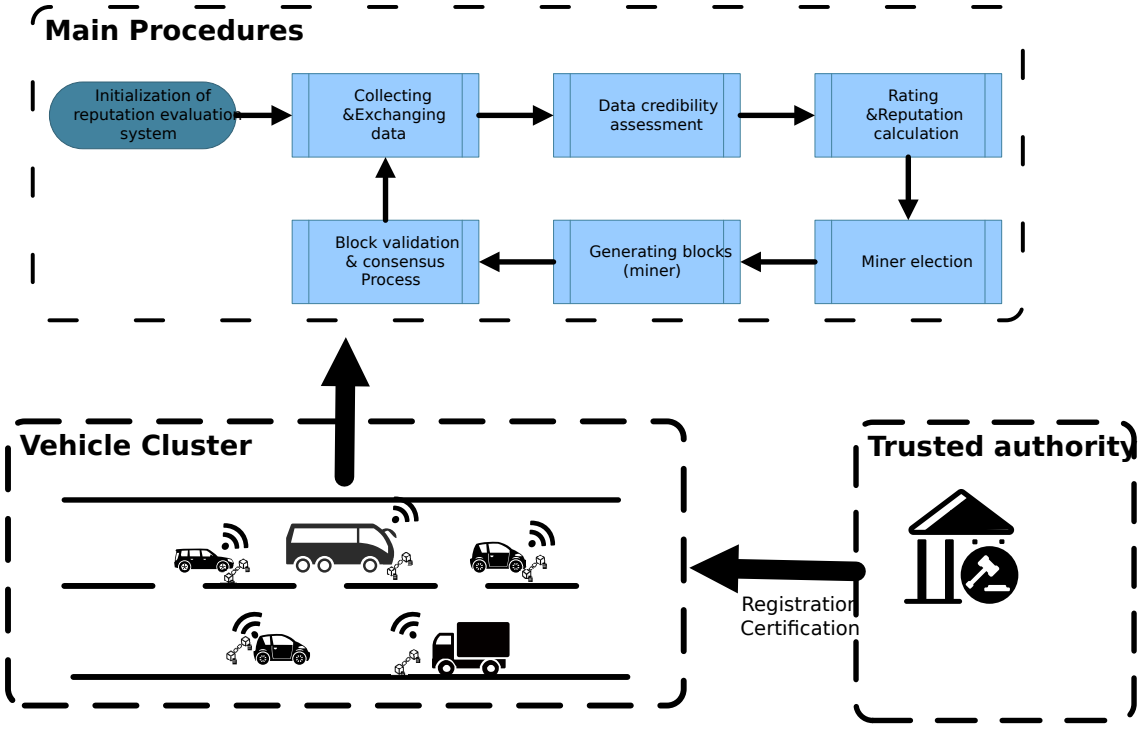


Fig. 8. Reputation evaluation system used in [2]

intermediaries. In order to reduce the cost of building a blockchain in an electric vehicle with limited energy, they propose a reputation-based DBFT consensus algorithm.

In order to evaluate the credibility of electric vehicle owners, PCP(private charging pile) owners and LAG(Local Aggregators) operators, Wang Y et al. [59] proposes a reputation model based on the ratings recorded in the blockchain. The sheme calculate the reputation value of each participant through transaction records, social relations, energy supply or demand, etc. All valid transactions are ordered by timestamps and packaged into a local block by each LAG. LAGs should compete with each other to solve a proof-of-work (PoW) puzzle with a certain difficulty. For each consensus node , the difficulty of PoW puzzle it need to solve is adjusted dynamically and inversely proportional to its reputation value.

Wang Y et al. [89] proposes a blockchain-based secure incentive scheme to optimize the charging and discharging of electric vehicles in the VEN system and achieve regional energy balance. A reputation proof consensus protocol is proposed in the scheme: a higher reputation value means a higher probability of participating in the consensus process and getting rewards. Therefore, every energy node in the network will strive to improve its charging and discharging services for electric vehicles to increase its reputation value. After each charge and discharge, the electric vehicle will score the service provider, that is, the energy node. The trust evaluation is derived from the historical transactions between electric vehicle users and energy nodes, which is related to the service level, energy transaction volume and the time of each interaction, and the evaluation results are revised through some information of electric vehicle users.

Almost similar to Wang Y et al. [89],A. S. Yahaya et al. [91] propose a reputation-based search and matching scheme between electric vehicle charging demanders and suppliers. The scheme adopts partial homomorphic encryption in local communication based on reputation calculation, and provides a privacy protection method that hides the location of EVs users. A private blockchain is used in the system to verify and allow energy security transactions between electric vehicle demanders and suppliers.

Ji Y. et al. [102] proposes a plan for updating the platoon leader in vehicular networks based on blockchain technology and reputation management mechanism to ensure that the most trusted platoon member serves as the platoon leader. In this scheme, according to the traffic incident information received, each platoon member evaluates the reputation of others in the form of offset. Miners use the reputation blockchain and the Delegated Proof of Stake (DPoS) consensus scheme to select several reputable platoon members to form a miner group, and the leader acts as a miner to generate blocks in turn and wait for others to verify it. If a block successfully passes the consensus process, it will be officially added to the blockchain, which can reflect the current reputation value of all platoon members. Xie L. et al. [108] constructs a SDN-enabled 5G-VANET and designs a trust management system combined with blockchain. In order to ensure that the vehicle cannot fabricate road information, when a vehicle uploads a video, it must also upload a traffic status tag for broadcasting and sharing with other vehicles. In addition, nearby vehicles will evaluate the authenticity of these uploaded traffic information.

RSU will calculate the trust value of the tag based on the distance between these nearby vehicles and the tag sending vehicle, and pack the trust value into a block. The sheme uses a combination of proof-of-work and proof-of-stake to regularly elect miners, in order to retain broadcasts that meet the actual conditions and block malicious vehicles (vehicles that broadcast a large amount of wrong road information)

2) **Credibility of RSU:** :

In the blockchain network with RSUs as miners' nodes, RSUs are not only responsible for meeting the information service needs of vehicles, but also need to complete complex affairs such as blockchain consensus algorithm. As the data processor, RSUs may perform malicious acts or be attacked by hackers. Therefore, credibility is needed as an evaluation index to ensure that vehicles can obtain more reliable data. In addition, if a consensus algorithm like PoW is adopted in the blockchain, which consumes a lot of computing power, the delay of information exchange in the network will be greatly increased, and there will also be potential problems of blockchain divergence caused by poor communication quality. Therefore, an algorithm based on DPoS with RSU credibility as the eligibility criteria for miners was proposed: Vehicles are evaluated by the RSU's performance to assess RSUs' level of credibility. After paying a deposit, The RSU which has high credibility can be a candidate for miner. The candidates are divided into two parts: The candidate miners with higher credit score are active miners. Each active miner acts as block manager for a period of time, completing block generation, broadcasting, verification and so on. Those with low credit value will serve as spare miners and cooperate with active miners to complete blockchain verification, so as to ensure that block managers are not bribed. Each time all active miners complete a dig, the system reevaluates the RSU's credibility and re-elects candidates.

3) **combined trust model:** : Wang Y. et al. [43] proposes a blockchain based framework for AVSNs (autonomous vehicular social networks) in content transmission. In this framework, the unforgeable ledger, cryptocurrency and asymmetric encryption can ensure the security of content transaction and reputation value, as well as the identity privacy of CAV (connected autonomous vehicles). Then, according to the user's social characteristics and user behavior, two reputation evaluation models are established to encourage the legitimate behavior of CAV and RSU, and improve the content reliability. Finally, the author designs a proof of reputation (POR) consensus protocol to effectively deploy the blockchain network into the avsn composed of RSU and CAV.

G. Other methods to ensure the authenticity of data

Kulathunge A S et al. [29] This research proposes a communication framework for VANET to explore blockchain functions. It meets the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication requirements in the Internet of Vehicles. It includes an intelligent toll payment (ITP) system (V2I communication) and automatic tracking of vehicles, called goose tracking (V2V and V2I communication), and meets the main communication needs. In addition, a simulator called SimulatorZ is implemented to model the "goose tracking". The simulator supports multi-vehicle simulation and can obtain the data requirements of the master and slave vehicles and the communication schedule. The communication framework provides the trustworthiness of vehicle behavior, cashless secure transactions between two untrusted parties, and rewards and punishments for vehicle behavior. Liu H et al. [107] mainly discusses the security of information and energy interaction in evce computing, and proposes the security scheme of cloud computing and edge computing. In the scheme, data currency and energy currency inspired by blockchain are defined to reward the participants who contribute to the system, and promote the consumption of various services by electric vehicles.

Deshpande V et al. [68] propose a smart vehicle framework SaFe based on blockchain and security elements (SE) to solve the reliability problem of electronic control units (ECU) in smart vehicles in intelligent transportation systems (ITS). Electronic control units (ECUs) need to be able to complete complex operations and ensure that smart vehicles can operate reliably even in emergency situations. However, these ECUs do not have a trusted execution/storage environment (TEE/TSE), which makes it vulnerable to many security issues. The solution uses SE in the TEE and TSE of the ECU, which is a small security microcontroller that can be used as an additional module of the hardware security module (HSM) to store critical keys to authenticate or encrypt key data/actions of smart vehicles. The solution also demonstrates how the blockchain can safely promote application management on the SE when the ECU needs change, to prove the rationality of using the blockchain.

Aiming at the problem of identity authentication, Liu H et al. [88] used a secret sharing mechanism based on a dynamic proxy mechanism to design a route hash-chain data tracking method based on the vehicle driving route. The solution also uses blockchain to achieve trust management: multiple proxy vehicles coordinately maintain the trust blockchain through V2V interaction to obtain the trust value of the vehicle, and then select one of the proxy vehicles as a miner to generate a new block to write proxy vehicles' trust value and authentication transaction records.

Hua S et al. [112] proposes a blockchain-based decentralized solution to solve the problem of trust between transaction participants during the refueling process, especially during the battery replacement process. All operations of the battery during its service life are stored in the blockchain network, and based on these constant battery information, its quality can be automatically evaluated through smart contracts. The solution not only considers the degradation of battery performance over time, but also considers its depreciation in each charging cycle, thereby ensuring a fair transaction between untrusted EV drivers and the station grid.

For cognitive Internet of Vehicles (CIoV), Qian Y. et al. [153] propose a privacy aware content caching architecture,

which processes transactions between content requesters and content providers through blockchain. In this scheme, all content providers authenticate and audit the process to solve the problem of mutual distrust in content transaction.

V. Data security and privacy protection

The traditional Internet of vehicles (IOV) system has not only poor security (vulnerable to DDoS and other malicious attacks, or privacy information disclosure) but also low efficiency due to its personalized identity registration, verification and cancellation mechanism. However, as a powerful tool generated by the combination of distributed technology and cryptography, blockchain can upload, verify and save data through consensus algorithm, hash chain and other technologies. When honest nodes are in the majority, the blockchain can ensure the availability, traceability and non repudiation of data, which greatly increases the difficulty and cost of malicious attacks. Therefore, in recent years, many schemes for accident recording and illegal detection in vehicle networks have combined blockchain: Kuhn M. et al. [37] use the traceability of the blockchain system to monitor the production process of vehicles, and allow understanding and tracing of the product history of safety critical products and all relevant processing steps. Blockchain provides complete and continuous data sets, which can be used to improve product quality, prevent failures and predict reliability, promote production line collaboration, and provide reliable evidence for responsibility allocation, fault accountability and product recall. Li C. et al. [27] recommend the use of vehicle sensors to help improve the accuracy of GPS (Global Positioning System) and save the vehicle location information to the blockchain, so that the authenticity of the location information can be judged by its historical submission records. Song Y et al. [147] [155] propose a framework of blockchain-enabled Internet of Vehicles (IoV) with cooperative positioning (CP) to improve vehicle GPS positioning accuracy, system robustness and safety. The solution uses multitraffic signs as benchmarks, realizes the self-positioning correction of intelligent vehicles through the deep neural network (DNN) algorithm, and share information to common vehicles (CoVs) in the same segment or area. In Cebe M. et al. [9], Ugwu M.C. et al. [4] and other articles, blockchain-based Internet of Vehicles is used in criminal investigations and accident determination. The owner's information of the vehicle (including name, age and even place of residence and work), driving route, insurance information, etc. will be recorded. Guo H et al. [34] proposes an automatic vehicle event recording system based on blockchain. In order to solve the problem that the traditional POW algorithm cannot update data in real time, they propose the mechanism of Proof of Event with Dynamic Federation Consensus to record the incident in new block. In the event of an accident, the vehicle directly involved broadcasts an "event generation" request , and only those vehicles within communication range can receive and respond. The vehicle directly associated with the accident and the vehicle receiving the request will then generate the event and broadcast it to a "vehicle network" defined based on the existing cellular network infrastructure. Within the vehicle network, a random federated group is formed to validate event data and save it in a new block by using a multi-signature scheme.Finally, the resulting new block is sent and stored in the Department of Motor Vehicles (DMV) for permanent recording. Davydov V et al. [192] introduce two blockchain-based accident detection models, aimed at reducing the difficulty of illegal detection and related measures. In particular, the authors introduce a new technology called "offline-detection", which involves detecting accidents without communication and Internet access. However, when the blockchain is introduced into the Internet of vehicles system, there are still some data security problems. The reason is that as a distributed ledger, blockchain is designed to be open and transparent, take the classic proof-of-work as an example: transactions are broadcast in the whole blockchain network, and miners need to complete the competition to obtain the right of generating blocks and corresponding rewards, and the blocks are accepted only after the verification of other nodes. Moreover, all nodes keep a complete copy of the blockchain information (or a full copy after a certain time). Malicious nodes can pretend to be ordinary nodes to apply for sharing blockchain information on the network, or directly attack ordinary nodes to obtain blockchain information. In fact, almost all IOV solutions have more or less considered information security or privacy protection. In IOV, there will be a large amount of data interaction between nodes, and these data may involve users' private or confidential data. The parties involved in the data certainly do not want to allow unrelated people to access the data, so identity authentication and encryption are required to ensure the confidentiality of the data. Since the data of the vehicle Internet is related to traffic safety, the solution requires that the data of the vehicle sensors cannot be tampered with, that is, the integrity of the data needs to be verified through message verification. In most cases, it is also necessary to anonymize the user's identity and take some measures to ensure that his true identity will not be tracked (unlinkability). In addition, many aspects such as the scalability of the authentication scheme and the consumption of resources (computing power and communication volume) have also been considered. Next, we will illustrate the current research status of the academic community in this field from the aspects of framework and cryptography technology.

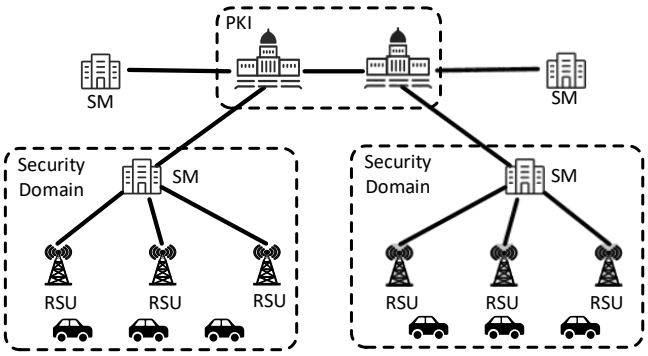
A. Key management scheme of Internet of vehicles based on blockchain

Lei A et al. [76] introduce blockchain technology to the key management scheme used in VCS scenarios, thereby removing the third party (central administrator). The verification and authentication in the key transfer process are completed by the network composed of SMs, which simplifies the process of key transfer and dynamic key management between two heterogeneous networks to reduce the key transfer time. The records of these processes are packaged into blocks for SMs to create a public ledger, achieving immutability and supervisability. In addition, SM will dynamically modify the collection period

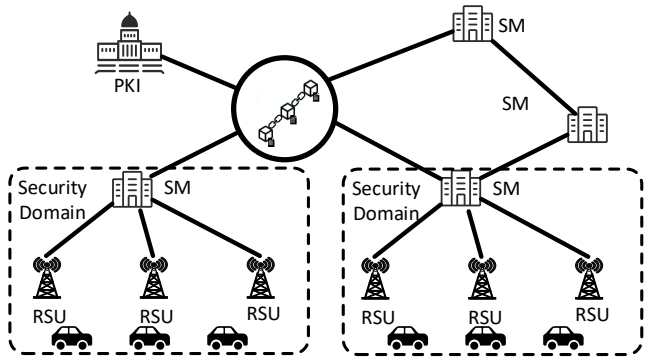
of transactions according to various traffic levels, making the solution more efficient in actual scenarios. Liu J et al. [210] adopt the same structure, and on this basis enable the vehicle to autonomously generate multiple pseudonyms to ensure unlinkability and traceability. Based on Lei A et al. [76], Lei A et al. [104] proposes a certificate revocation scheme that can prevent internal attacks in VCS networks. The program uses the Certificate Revocation List (CRL) to distribute the revocation information of the vehicle pseudonym. However, to ensure safety and privacy, the vehicle will use each set of pseudonyms and frequently switch to the new pseudonym. Therefore, this paper uses the PKI to track the ownership of the pseudonym set by combining the blockchain. Moreover, the scheme reduces the size of the CRL and the communication overhead by combining the group key management scheme. The provision of vehicle fog services (VFS) requires the support of data centers. However, high-speed moving vehicles will span the service range of multiple distributed data centers, so cross-data center identity verification needs to be considered. This paper proposes a blockchain-assisted lightweight anonymous authentication mechanism (BLA) to meet the privacy protection and performance requirements of distributed VFS. The program allows vehicles to be anonymous and change their pseudonyms at any time to prevent malicious tracking. Blockchain technology realizes the non-interactivity between the vehicle and the service manager (SM), so that the SM needn't communicate during the authentication process, which reduces the amount of communication in the network.

Zheng D. et al. [115] propose a blockchain-based privacy protection mechanism for intelligent vehicle communication in VANET. The mechanism is composed of four participants: certification authority (CA), vehicles, roadside units and cloud servers. CA generates a public-private key pair in elliptic curve cryptography for each registered vehicle, and provides vehicles' public key to the RSU for signature verification in the ledger. RSU is responsible for broadcasting the messages and transactions sent by vehicles and recording them in the blockchain that it maintains, which provides a way for identity verification and transaction verification between vehicles. In addition, the real identity corresponding to the pseudonym of the vehicle is also recorded in the blockchain to maintain the credibility of the CA.

Baldini G et al. [71] proposes a new authorization ticket distribution scheme, which can be seen as an improvement to the existing PKI-based standardized security framework, so as to better provide the basic services required for integrity and authentication. The solution uses the Zone Key concept and blockchain to solve the scalability problem of the existing revocation mechanism, and minimizes the risk of privacy by minimizing the number of AT (Authorization Ticket).



(a) Traditional Centralization Structure



(b) Distributed Structure in the Internet of Vehicles Based on Blockchain

SM: Security Manager
PKI: Public Key Infrastructure
RSU: Road Side Unit

Fig. 9. Network structures

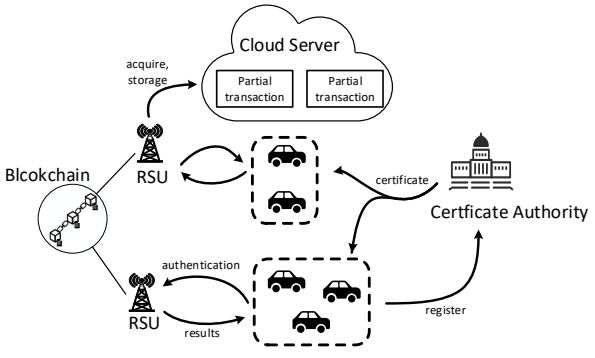


Fig. 10. A key management structure using RSU to maintain blockchain

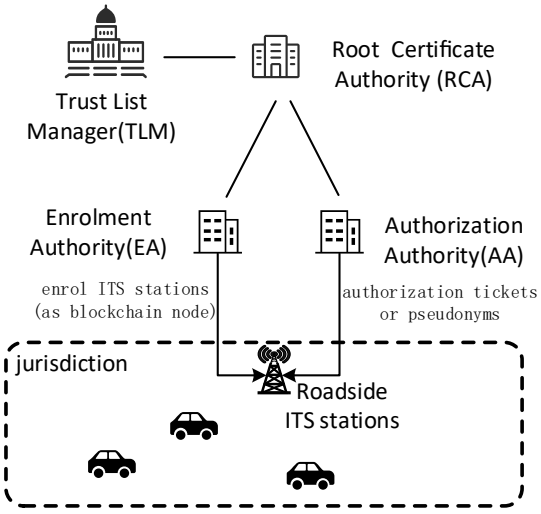


Fig. 11. A scheme of C-ITS PKI deployment

B. Key Distribution Scheme

In Arora A et al. [117], each vehicle must submit its identification details to the registration authority (RA), such as name, address, electronic license plate (ELP) number, etc. to complete the registration. RA is responsible for assigning pseudo identity (PID) to vehicles using elliptic curve Diffie Hellman key agreement protocol and generating public and private key pairs from PID.

C. Public-Key Cryptography

1) Public-Key Encryption:

a) Hybrid Encryption: Although asymmetric encryption algorithms are powerful and difficult to replace, their efficiency is far lower than that of symmetric encryption algorithms. Therefore, the hybrid encryption method combining the advantages of symmetric encryption and asymmetric encryption shows its high practicability. In Alam M S U et al. [119], many functions in the vehicle system are completed by a variety of ECU (electronic control unit). The potential safety hazard is that the vehicle ECU is connected through multiple communication buses. Any ECU connected to the bus can read data or send data to other ECU. If one ECU is manipulated by an attacker, the data of other important ECUs will also be leaked. This paper suggests using symmetric key encryption and elliptic curve based public key encryption (PKE) to ensure confidentiality, and digital signature to ensure the integrity and authenticity of data. In addition, the scheme uses identity based access control to allocate bus communication permissions, and block chain inspired mechanism to protect the data stored in ECU. In Brousmiche K L et al. [57],the authors designed a novel consortium blockchain to manage the life cycle information and data of vehicles, so as to realize the cooperation and data sharing among automobile manufacturers, insurance companies and service providers. In order to ensure the data confidentiality, the authors design and implement a hybrid encryption protocol, which can dynamically add and delete authorized users, so that the vehicle owner can grant temporary access to external users.

b) El Gamal Encryption:

c) RSA Encryption:

d) Elliptic Curve Encryption: When vehicle nodes share data with other nodes, VANET will be affected by issues such as identity validity and message reliability. The method used to allow vehicle nodes to upload sensor data to a trusted center for storage is vulnerable to security risks, such as malicious tampering and data leakage. In order to cope with these security challenges, Zhang X et al. [30] propose a data security sharing and storage system based on consortium blockchain (DSSCB) applied in vehicular ad-hoc network (VANET). In this scheme, a digital signature algorithm based on the elliptic curve bilinear pair property is used to sign the message in the data sharing stage to ensure the non-repudiation and integrity of the message. The use of the consortium blockchain solves the scalability problem and improves the overall system efficiency.

Malik N et al. [35] propose an identity authentication technology based on a private blockchain to ensure the privacy and security of vehicles in VANET. The revocation authority (RA) and CA have all the ledger control rights, and only RSU is granted with read permission, but not OBU. In addition, the framework no longer uses CA or RSU to distribute CRLs, but modifies the status of the vehicle's revocation flag to reduce dependence on CA and improve node revocation efficiency.

In order to solve the hidden safety hazards in the system, Kim M H et al. [79] propose a blockchain-based safe charging system for electric vehicles. The charging system ensures the security of keys, secure mutual authentication, anonymity and forward secrecy, and improves operational efficiency. The Burrows-Abadi-Needhamlogic used in the program can provide secure mutual authentication. The program also uses automatic verification of Internet security protocols and application simulation tools to prevent replay and man-in-the-middle attacks.

e) Paillier Encryption Scheme: Charging stations need to schedule and match in advance according to the route of EV, but this process may reveal sensitive information about users (such as driving habits, route information, etc.). In order to solve this problem, Yucel F et al. [101] proposes a privacy-preserving distributed stable matching between electric vehicles and suppliers (i.e. public/private gas stations, V2V chargers), using a preference list formed by distance calculation based on partial homomorphic encryption, while hiding the location. Jiao Liu et al. [210] propose a blockchain-based VANET protocol called BUA. The main purpose of this protocol is to realize the unlinkable vehicle identity authentication. The architecture of the system is shown in fig. 10. The vehicle uses homomorphic encryption to generate a number of pseudonyms to achieve non linkability. Each SM covers a certain area and maintains a blockchain that stores information such as vehicle registration data, so as to verify the validity and ownership of pseudonyms used by vehicles

Ref.	Security	Privacy	Anonymity	unlink-ability	entity auth.	message auth.	nonrepu-diation	scalable	low overhead or high efficiency	account-ability
[119]	✓				✓	✓	✓			
[57]	✓	✓			✓	✓				

locally.

2) Digital Signature Schemes:

a) multi-signature: In order to achieve conditional privacy in vehicles, Zhang L et al. [82] proposes a method based on fair blind signature and threshold secret sharing. Using this method, the vehicle can anonymously sign the notification message. When a forged or malicious message is found in the system, multiple regulatory agencies can cooperate to track the true identity of the message sender. Writers also designed a mechanism to implement pre- and post-event countermeasures, which use threshold technology (and multi-signature scheme) to implement a priori confrontation (and a posteriori confrontation). If and only if the number of message generators (signers) reaches the threshold, the announcement message is considered a trusted message. For posterior countermeasures, notification messages should be signed using a multi-signature scheme, thereby reducing the number of messages that should be stored. If the announcement message is later found to be fake/fake, then the conditional privacy property of the system can be used to retrieve the true identity of the message sender. Wang Y et al. [59] propose a scheme to optimize the scheduling of charging and sharing between EV and PCP in PCPSN (private charging pipe sharing networks) based on blockchain. In the scheme, a secure PCP sharing protocol based on reputation is used, which guarantees effective consensus in the blockchain through BLS multi signature.

b) ring signature: Wang H et al. [111] propose a system model and security model that uses blockchain to provide anonymous rewards to V2G networks. The authors studied the anonymity of CAG(Central Aggregator) and BV, and realized the unlinkability between the payer address and the payee address by combining the aggregate signature and ring signature. Therefore, no one can establish a relationship between the two parties when the reward is executed. This scheme is the first BBARS scheme with available cryptographic primitives, and it has been proven safe in the random oracle model. Calvo J A L et al. [38] present a security protocol based on consensus strength (blockchain) for exchanging messages between vehicles. In this paper, the authors use platoon formation which is the most ideal arrangement method with high security and road efficiency, and use the ring signature scheme combined with blockchain to verify the identity of vehicles in platoon. When the vehicle completes the initialization of joining a platoon, the vehicle in the platoon can confirm whether the other party is in the same platoon through the vehicle identification value, so as to prevent malicious vehicles from sending messages under the condition of privacy.

c) group signature: Bai H et al. [39] propose a lightweight protocol for the communication of the Internet of vehicles. The edge nodes in the group provide efficient authentication services as group managers. First, edge node creates public-private key pair, broadcasts public key to all vehicles in range, and completes initialization of parameters. Then, the vehicles carry out blind signature, submit the authentication information to the edge node, to obtain the group certificate. Finally, the vehicles can sign the status information through the certificate and group public key, and communicate with other vehicles within the service scope of the edge node. If necessary (in case of accident or malicious behavior), the manager can identify the corresponding vehicle from the private key in the group signature. In the scheme, adding group members to edge nodes will not change the group public key, nor change the signature length and computation of the open algorithm, which reduces the time-space cost in authentication.

Zhang X et al. [94] applie the distributed blockchain structure to intelligent traffic signal control to improve the robustness of the system and prevent information asymmetry. This paper uses an efficient batch verification algorithm based on BLS (Boneh-Lynn-Shacham) group signature and an ElGamal encryption algorithm that can ensure the confidentiality and integrity of the message. The OBU uses the private key to sign the traffic information and submit it to the RSU. After receiving the message, the RSU uses the group public key for verification. The calculated Dif-Dell-Hellman problem guarantees the security of the group signature, so that the attacker cannot forge a new signature through eavesdropping, and cannot distinguish the signature without opening the signature. The Chinese Remainder theorem used in the scheme guarantees that newly joined group members can no longer use the previous group public key to verify signatures, and the new group public key cannot be used to verify the signatures of group members who have left the group, thereby ensuring forward and Backward security to facilitate rapid joining and withdrawal of group members.

d) elliptic curve digital signature algorithm: Gao F et al. [98] propose a decentralized anonymous payment mechanism that enables electric vehicles in the V2G network to share privacy-protected data, and combines the registration process to achieve design goals. In order to prevent internal attackers from inferring the identity of the pseudonym by analyzing the transaction data in the global ledger, the RA in the scheme only provides identity information when transaction disputes occur, so it does not frequently participate in the payment execution process. In addition, users can register multiple accounts in one registration process and use different accounts for each transaction. This one-time account strategy can disperse the user's transaction rules into different accounts, thereby suppressing attacks based on transaction data analysis.

Ref.	Security	Privacy	Anonymity	unlink-ability	entity auth.	message auth.	nonrepu-diation	scalable	low overhead or high efficiency	account-ability
[101]	✓	✓	fi	fi	✓	fi	fi	fi	fi	fi
[210]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

In order to help autonomous vehicles make decisions and investigate crimes or traffic violations. Narbayeva S et al. [146] developed a vehicle behavior tracking system based on exonum platform, which can transmit state parameters between adjacent vehicles safely and reliably. In this paper, ECDSA is used for data input and transaction confirmation.

e) Other Signature Methods: For the verification process of blocks in the blockchain used by electric vehicles and distribution networks, Sheikh A et al. [86] proposes a Byzantine-based consensus algorithm for energy trading between EVs and DN. The algorithm points out that a successful attack requires 33% of information is maliciously manipulated, which reduces the probability of attacks threatening the security of the system. In addition, to ensure data security, the transmitted data includes plain text and corresponding signatures. In the data signing stage, the author first generates a message digest (MD) of plaintext through the secure hash algorithm (SHA), and then uses the private key to encrypt the MD into a digital signature. In the verification phase, the hash result of the plaintext is compared with the decryption result of the public key of the digital signature. When the two are the same, it can be considered that the information has not been tampered with and the sender's identity is confirmed.

3) The scheme of applying multiple encryption methods: [206] implements blockchain-based privacy-preserving authentication (BPPA) on the Hyperledger Fabric (HLF) platform. It uses the blockchain to record Semi-TA activities to achieve the transparency of certificates and revocation, and uses the Merkle Patricia tree (MPT) to expand the blockchain. The scheme designs a distributed identity verification scheme, so that the receiver can verify the status of the sender's certificate through multiple hash calculations, thereby saving time and storage requirements for CRL. In order to protect conditional privacy, the scheme allows vehicles to have multiple certificates at the same time. The linkability between the certificate and the real identity has been encrypted and stored in the blockchain, and the real identity of the vehicle will be disclosed to authorized institutions when necessary.

D. zero-knowledge proof

Baza M et al. [67] uses two cryptographic tools, attribute-based encryption and zero-knowledge succinct non-interactive knowledge argumentation to ensure data security. Attribute-based encryption (ABE) is an encryption scheme that allows access control to encrypted data. In this scheme, each user will be assigned a set of secret keys according to his attribute set. Then, the message that needs to be transmitted is encrypted under the access policy formed by the system attribute set, so that the message can only be decrypted by users with attributes that satisfy the policy. In our solution, ABE is used to enable distributor AVs to identify neighboring AVs that have the functions required to download firmware updates. The second tool used, zk-SNARK, is a proof structure, in which the prover can prove to the verifier that he possesses a specific piece of information without revealing the information. The program uses it to exchange updates in return for a proof of distribution in a untrustworthy environment. Li M et al. [159]'s scheme uses Merkle hash tree and smart contract to implement proof-of-ad-receiving (PoAR) to alleviate the "free riding" attack, and achieves anonymity and conditional linkability based on zero-knowledge-proof technology. At the same time, the proposed scheme can send advertisements to specific vehicles many times to ensure that malicious vehicles will not abuse anonymity to obtain additional rewards.

E. K-Anonymity

In Firoozjaei M D et al. [63], the authors introduced a credit sharing solution for a blockchain-based EV charging system called EVChain. EVChain is a hybrid blockchain composed of a MaBC (main blockchain) for charging applications and several SuBC (subnetwork blockchains) for credit sharing groups. Among them, MaBC is responsible for completing user-to-server (U2S) transactions, and its members can publicly access data related to charging credit. In SuBC, the user-to-user (U2U) transaction between EVs is completed, and the private data of the credit sharing group is stored. The solution uses a component called bridge between SuBC and MaBC to separate U2U and U2S transactions, and hides the activities of the credit sharing group based on k-anonymity, thereby protecting user privacy. In Li H et al. [198], the authors use dynamic (m,r) threshold encryption to define "The identity privacy protection algorithm". Vehicles need to upload SBM (Safety Beacon Messages) by using the unified sub-identity of r vehicles. When the vehicle enters a different group, it will regenerate r sub-identities with the help of CAserver. The authors also use k-anonymity to define "The location privacy protection algorithm". When a vehicle uploads SBM, the vehicle will upload k locations in conjunction with other K-1 selected vehicles. Therefore, it can blur the connection between vehicles and their locations. In Luo B. et al. [11], the authors improved the application of the K-anonymity method in VANET, so that vehicles can rate the reputation of other vehicles, ensuring that requesters and partners only cooperate with vehicles they trust. The authors put forward a method for evaluating the credibility of vehicle behavior by analyzing the various needs of the request vehicle and the cooperative vehicle to prevent malicious vehicles from stealing sensitive vehicle information in the process of K-anonymity.

Ref.	Security	Privacy	Anonymity	unlink-ability	entity auth.	message auth.	nonrepu-diation	scalable	low overhead or high efficiency	account-ability
[67]	✓				✓	✓	✓	✓	✓	✓
[159]	✓	✓	✓	✓	✓	✓	✓			

Ref.	Security	Privacy	Anonymity	unlink-ability	entity auth.	message auth.	nonrepu-diation	scalable	low overhead or high efficiency	account-ability
[63]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[198]	✓	✓	✓	✓	✓	✓	✓		✓	✓
[11]	✓	✓	✓	✓	✓	✓	✓		✓	✓

F. Other encryption methods

Javaid U et al. [116] proposes a PUF and blockchain-based solution called DrivMan used in VANET to realize trust management and data sharing. PUF provides a unique encrypted fingerprint (cID) for each IV to establish the data source, and the RSU is responsible for issuing certificates to protect the privacy of the vehicle. Cheng L et al. [141] propose an auxiliary traffic control system using attribute-based blockchain in IoV. Drivers can use control-by-vehicle methods to control traffic lights to improve traffic efficiency while balancing system availability and privacy safety. Before starting communication, Users are grouped their attributes (such as location and direction), and then users can interact with each other to determine the status of traffic lights without leaking privacy. When necessary, the system also supports the responsibility investigation of history through ciphertext-policy attribute-based encryption (CP-ABE) and blockchain technology. Based on the consortium blockchain, Liu D et al. [100] propose a cross-domain authentication scheme against security threats in V2G networks. A trust model and system architecture are designed in the article, and an encryption algorithm based on SM9 identity is used for signature and authentication. By using a hash algorithm to verify the certificate, the scheme can effectively reduce the number of public key algorithm signatures and verifications, thereby making the solution efficient and scalable.

G. Other ways to protect privacy

Xu C et al. [33] propose a remote attestation security model based on privacy preserving blockchain, called RASM. In order to provide evidence of a credible identity and integrity, the model proposes two core steps: first, use trusted platform module (TPM) to complete remote attestation, then use calculation node to make decision, and use accounting node to write data block. The model is mainly oriented to judge the qualification of new nodes when they are added to the network and fast remote verification when two nodes communicate.

Knirsch F et al. [78] point out that in a liberalized market, different energy suppliers and charging station operators will provide energy at different prices according to demand and supply. While customers can benefit from this, this dynamic pricing example is subject to privacy issues: information such as the customer's location, itinerary, and transaction records may be analyzed. Therefore, based on the blockchain technology, the authors present a reliable, automatic and privacy protection scheme, which can select the charging station according to the price and the distance from the electric vehicle. Electric vehicles send out demand signals, and charging stations offer similar auctions. Then, the EV owner chooses a charging station based on the price quoted by the supplier. This paper shows that the use of blockchain improves the reliability and transparency of this method, while protecting the privacy of electric vehicle owners.

VI. System optimization

In order to make the system of "Internet of Vehicles + blockchain" achieve more powerful functions and better meet our needs for convenience and comfort under the current hardware development level, optimizing the performance of the system is also a research field that we cannot ignore. With the help of some targeted system design concepts, the efficiency indexes of various aspects of the vehicle networking scheme, such as communication efficiency, storage efficiency and computing efficiency, can be improved without changing the hardware configuration. Researchers have made a lot of efforts in this area, and some of their scheme use more effective methods to reduce the delay in the system, improve the transaction throughput of the system, and so on. In addition, some researches are devoted to improving the usability of the system, that is, encouraging users to submit real and useful data to enhance the authenticity and richness of data in the system, so that users can obtain useful information from it.

A. Optimization efficiency

The construction of the Internet of Vehicles is often based on a large geographical range, providing information exchange services for tens of millions of constantly moving vehicles. A large number of users will bring massive data traffic, which is a great challenge to computing power, communication bandwidth and storage space. Next, we will analyze each solution to these problems one by one.

1) Stratify and partition: One of the classical methods to effectively reduce the traffic on the whole network and improve the efficiency of the blockchain is stratify or partition the

Internet of vehicles. For most application scenarios, vehicles only care about the events in their vicinity (such as intelligent transportation system, electric vehicle charging system, accident recording system, etc.), neither need spread the information to the whole system, nor need to get the information of whole system from time to time. Therefore, we can divide the Internet of vehicles into relatively independent clusters according to geographical locations just like administrative regions [161] [170], so as to realize the transaction autonomy within cluster and the concise interaction between clusters. Another method is to allocate data to different blockchains according to the content and source, so as to improve the efficiency of transaction processing, as proposed by Jiang T et al. [54].

Dorri A., et al [13] do not rely on RSUs and other infrastructure to communicate, but directly form a cluster of geographically close vehicles to achieve efficient data interaction within the cluster, with no message exchange between the clusters. van der Heijden, R.W., et al. [8] adopt Permissioned Blockchain method and divides the vehicles and Rsus in a certain area into clusters. After the consensus algorithm is completed internally, the cluster heads of each cluster will complete the consensus of the whole network together. Sharma V. et al. [65] also adopt an almost similar structure, optimizing the number of transactions through distributed clusters, in order to reduce the burden of a large number of blockchain data transmissions in the power transaction network, and maximize energy saving at the same time. The scheme proposed by Gao J et al. [129] standardize the message transmission mode of the cluster model and adds the credibility evaluation of the message. The solution proposed in Jameel F et al. [181] improve the original clustering method, and formulates the mining task offloading problem according to the transmission rate of the vehicle and the computing resources available in the mining cluster. Due to the limited local vision of offloading vehicles, the feasibility of the mining task is ensured. In addition, the article proposes a game theory solution to balance the computational load of mining clusters to promote fair participation of all vehicles in the process.

The blockchain communication scheme proposed by Oham C. et al. [1] is divided into two layers: the information senders at the first layer include smart cars, vehicle technicians and manufacturers, and they will exchange relevant information to facilitate the forensic process and make responsible decisions. At the same time, there are also validators on the first layer, including: car manufacturers, insurance companies and automotive technicians, used to verify the authenticity of information and track changes in the state of the blockchain. In the second tier, the senders are insurance companies and smart car manufacturers, and the verifiers are law enforcement and transportation. In actual situations, the smart vehicle generates a transaction and stores the witness's perception, and sends the transaction to the first-level verifier. After the authenticator verifies the authenticity of the intelligent vehicle and the correctness of the transaction, it is included in the blockchain. After the accident, the insurance company sends a request transaction to the second layer of validators. The transportation management agency will retrieve the transaction data (time and place of the incident) after receiving the request. Once retrieved, it will query the nearest roadside unit and work with law enforcement to decrypt the user's encrypted account in the transaction data sent by the insurance company. Law enforcement authorities and transportation authorities will cross-validate all collected evidence to determine the responsible party. This structure is also adopted by Cebe M. et al. [9].

Liang H. et al. [17] propose a micro-blockchain architecture to build a reliable intrusion strategy for the GDID paradigm. The architecture includes a macro blockchain and several micro blockchains. Local intrusion samples and intrusion detection strategies can be quickly stored, prepaid and propagated through the micro-blockchain architecture deployed and running in specific areas. Multiple micro-blockchains can build a larger micro-blockchain, providing a spatiotemporal dynamic intrusion detection strategy for vehicles moving in large areas. All data collected by the micro-blockchain will be stored in the macro-blockchain to verify the legitimacy of the collected data and generate cryptocurrencies for data providers.

Guo S et al. [28] establish a layered architecture including the vehicle network layer, the blockchain edge layer and the blockchain network layer. It implements trusted access to vehicles and collaborative sharing between different vehicle networks. As a result, it enhances network functions, reduces delivery delays and increases authentication speed.At the same time, this article proposes an edge caching scheme based on many-to-many matching. By dynamically optimizing the caching strategy, the average delay can be minimized and the collaborative sharing performance can be improved.

Ying Z et al. [45] propose a scheme of Autonomous Vehicle Platoon (AVP), which divides vehicles with similar geographical location and driving track into a platoon, and constructs a semi closed communication space for each platoon. PMS can communicate with each other in the same platoon, and only PL (platoon leader) can communicate with facilities or vehicles outside the platoon. The authentication and data transmission between PMs (platoon members) are recorded on the private blockchain and uploaded to the public blockchain after the journey.The scheme also implements a dynamic AVP management protocol on Ethereum. Vehicles who want to join or leave the platoon must communicate with the platoon leader, and all messages will be delivered in the form of transaction in the smart contract. This method can significantly reduce inter platoon interference and effectively improve the safety of platoon. Of course, a fixed platoon leader may face targeted attacks, so Ji Y et al. [102] propose a scheme to achieve a credible and efficient platoon leader update method. Chen C et al. [150] introduce a scheme of selecting PH by reputation value to motivate vehicles to become PH and keep the platoon updated dynamically

Masoud M Z et al. [47] propose a blockchain-based distributed vehicle history reporting system called CarChain. The system builds an overlay network that can be shared among

ordinary customers, auto dealers, auto mechanics, insurance companies, and the government. In order to reduce the complexity and scale of CarChain, a hierarchical design module is used to build a different coverage network for each country.

Wang Q et al. [74] propose a two-layer architecture of a traffic chain, which includes a local chain for each road section and a global chain. For each local chain, "local miners" are miners who wish to participate in the collection of traffic status of nearby road sections. Each block on the local chain contains all the reports of the corresponding road section and is only multicast to the corresponding local miners. For global chains, all miners in the city can become "global miners" participating in its construction. Each block on the global chain contains a summary report of the traffic status of each road segment and broadcasts it to all global miners. When a vehicle needs to find a route to a certain location, it can retrieve the necessary traffic status from the global chain. A similar approach is also adopted by Zhang L et al. [82].

Yahiatene Y et al. [97] propose a software-defined vehicular network(SDVN) oriented framework, which uses three levels of controllers: aprincipal controller (PC), roadside unit (RSU) and local controller. PC can see the global view of vehicular social networks(VSN) topology. RSU is an intermediate between PC and miners. In terms of security, the local controller not only acts as a miner, but also acts as a relayer.

In Chai H et al. [200], a new cache scheme based on transactions in blockchain network is proposed. According to the influence range of SI, it is divided into low range SI and high range SI: for the former, the audit process is relatively simple, while for the latter, the scheme first audits it in a small range, and then verifies it in a larger range by the superior peer. In addition, in order to reduce the overall consensus delay, this paper proposes a new hierarchical blockchain to maintain SI messages. Mining nodes need to reach consensus in different layers, and cache various Si messages in different level ledgers according to the scope of Si influence, so as to meet the high-speed transmission and low latency requirements of IOV applications.

2) Faster transaction confirmation: Michelin R.A. et al. [22] adopt a customized blockchain, which relies on the block identified by its public key generated by each vehicle to store signed transactions to solve the problem through a consensus algorithm. High latency and computational power consumption caused by verification transactions. This type of blockchain allows data to be appended directly to existing blocks by hashing the previous information and signing newly created information. The vehicle collects data from the sensor, signs and generates a new transaction, and sends it to the nearest RSI for verification. RSI can access the vehicle public key stored in the block header of the blockchain. When the transaction is authenticated as valid, it will be immediately attached to the current block of the vehicle (if this is a newly added vehicle, a GenesisBlock will be created). In order to ensure the privacy of the vehicle, the asymmetric key pair used for communication will be changed after a certain period of time (called KUI). Due to the limited resources of vehicles, they only need to maintain a block of Merkle tree instead of maintaining the entire blockchain.

In order to use the bidirectional energytrading capabilities of electric vehicles (EVs) to reduce the level of mismatch between supply and demand, Zhou Z et al. [41] proposes a safe and effective V2G(vehicle-to-grid) energy trading framework by integrating blockchain and edge computing. The author proposes consortium blockchain-based energy trading mechanism for V2G: The computational resource allocation problem is modeled as a two-stage Stackelberg leader-follower game, and the optimal strategy is obtained by using the backward induction approach.The author also developed a task offloading mechanism based on edge computing for LEAGs to improve the probability of success when producing blocks.

3) Efficient consensus algorithm: In Jiang X et al. [42], Ji Y et al. [102], Niyato D et al. [114] and Su Z et al. [149], the Delegated Proof of Stake (DPoS) consensus algorithm is used to establish a blockchain-enabled vehicle network (BEVEN), which can effectively ensure the security and traceability of data sharing. Miners in DPoS include active miners and standby miners: Active miners are responsible for block generation and block verification. Standby miners can verify and review newly generated blocks to prevent infected active miners from colluding with each other to generate maliciously manipulated block verification results.

Wang Y. et al. [81] use a reputation-based delegated Byzantine fault tolerance (DBFT) consensus algorithm to effectively reach consensus in the energy blockchain. Electric vehicles have two roles in the V2V network: the original node and the consensus node. Ordinary nodes only relay, transmit, exchange, and receive ledger data, while consensus nodes are authorized to execute the consensus process.When a smart contract is made between the EV and the aggregator, the EV will broadcast this event to the network. All transactions within a certain period of time are collected and verified by consensus nodes, and then sorted by timestamp and packed into blocks. In order to coordinate the large number of energy transactions in the electric vehicle (EV) charging network system and prevent excessive power load and attacks, Liu C et al. [85] proposes a proof-of-benefit consensus mechanism with online benefit generating (ONPoB) algorithm on the blockchain platform. This solution improves the processing rate of EV charging/discharging loads, effectively smoothing the overall power load fluctuations. Hu W. et al. [142] use the Byzantine consensus algorithm based on time sequence and gossip protocol in the blockchain-based IoV architecture to complete information communication and consensus authentication, which improves the efficiency of consensus while ensuring security, and improves the tolerance of failures. Chai H. et al. [154] use a light-weight Proof-of-Knowledge (PoK) consensus mechanism to enable the vehicle with the most knowledge to generate a blockchain.

Sun G. et al. [165] propose a local vehicle-to-vehicle (V2V) energy transaction architecture based on fog computing in social hotspots, and solves some problems in transaction security and privacy protection by using a consortium blockchain.

The paper combines the Delegated Proof of Stake (DPOS) algorithm with the practical Byzantine fault tolerance (PBFT) algorithm, and proposes a new consensus algorithm called DPOSP, which greatly reduces resource consumption and improves consensus efficiency. In the scheme of Yang YT et al. [172], authors propose a proof of event consensus concept for vehicle networks, which can identify selfish or malicious behaviors and prevent the propagation of false traffic warning messages. This method divides the transaction into two consecutive stages: synchronizing the local blockchain, and then synchronizing to the global blockchain, thereby reducing the transmission load on the network. A distributed secure content caching framework is proposed in Dai Y. et al. [193]. In this framework, the vehicle performs content caching while the base station maintains the permissioned blockchain to ensure intelligent and secure content caching. Similar to DPoS, this paper uses the utility of base station to select delegates. The base stations do not directly participate in content transmission and coin payment in the process of content caching, which means that they can't cheat in the caching process to gain profits, so they are ideal delegation candidates. In the scheme of Javaid U. et al. [158], a smart contract based IOV protocol using physical unclonable functions (PUF) and dynamic proof of work (DPoW) consensus algorithm is proposed, which provides a secure framework for registering trusted vehicles and preventing malicious vehicles. PUF is used to assign a unique identity to each trusted vehicle, while the dpow consensus allows the protocol to expand based on the incoming traffic generated by the vehicle.

Ref.	consensus algorithm	Application scenarios
[42]	Delegated Proof of Stake	Object detection for autonomous driving
[102]	Delegated Proof of Stake	Universally applicable to various applications of IOV
[114]	Delegated Proof of Stake	Universally applicable to various applications of IOV
[149]	Delegated Proof of Stake	secure data sharing in disaster rescue
[81]	Reputation-based Delegated Byzantine Fault Tolerance	secure electric vehicles charging
[85]	Proof of Benefit	secure electric vehicles charging
[142]	Byzantine consensus algorithm	intelligent transport
[154]	Proof of Knowledge	Artificial intelligence algorithm in IOV
[165]	The combination of DPoS and PBFT	Energy Sharing
[172]	Proof of Event	intelligent traffic management
[193]	Proof of Utilization	content caching in vehicular edge computing and networks
[158]	Dynamic Proof of Work	Universally applicable to various applications of IOV

B. Data storage methods of the Internet of Vehicles

Cebe M. et al. [9] roughly follow the structure of Oham C. et al. [1]. But it also observes that the server provider is not interested in the information uploaded regularly by the on-board unit EDR (event data recorders), and the capacity of the on-board unit is limited, therefore, this article uses a fragmented ledger. Instead of storing all the forensic data in a shared ledger, each participant will save data different from other participants. In order to ensure correctness, the hash of the data will be submitted to the blockchain jointly maintained by the participating parties. After the accident, the hash value on the public chain can be compared with the records inside the vehicle to verify the integrity of the data. [4] also follows the basic structure of this article, and adds monitoring of Proof of vehicle state, Proof of interaction, Proof of BlockChain state to improve the robustness of the system. The DSSCB scheme proposed by Zhang X. et al. [30] is optimized for large-scale data storage in VANET, and distributed security is used to solve the security challenges caused by centralized databases [27]. In DSSCB, RSU is PSN (pre-selected node), and vehicle is SN (sensing node). PSN is granted the right to write data and participate in consensus. SN can access and synchronize copies, but does not participate in consensus. The local storage device in the PSN is responsible for collecting sensor data uploaded by the SN and obtaining data shared by other PSNs, and automatically organize and analyze the data using the originally deployed smart contract.

Kang J. et al. [126] point out that due to the limited resources of vehicles, it is necessary to rely on the massive storage resources provided by vehicular edge computing and networks(VECONs) in certain scenarios, but the RSU as the vehicle edge computing server cannot be fully trusted Therefore, in this scheme, each vehicular edge cluster will reward the edge nodes that contribute the most storage space by using the vehicle coin (the cryptocurrency in VECON) according to the records of the local controller. This method is called Proof-of-Storage consensus algorithm.

Lasla N. et al. [58] discuss and adopt a variety of technologies to save the storage space of the scheme. (1) Multiple blockchains: different types of data such as vehicle registration, access, and misconduct are stored in different blockchains. In this case, the vehicle will only use admission and withdrawal blockchains because they are sufficient to verify the origin of any security messages received. (2) Pruning: Deleting useless information is an effective way to reduce the size of the blockchain. For example, an entry about an old vehicle that has been revoked can be deleted from the vehicle's blockchain copy. But these useless transactions can only be deleted from the vehicle copy, and need to be

completely stored in the validator node to ensure the security of the blockchain. (3) Encrypted accumulator: The idea is to accumulate a group of valid vehicles into a single digital object, where each vehicle will have another member to prove that it has been registered in the accumulator. Only the accumulator will be stored on the blockchain, and the vehicle only needs to include their witnesses in its security message so that the recipient can check membership by applying a simple function.

In Jeong B. G. et al. [120] , a method called data-owner-based attribute-based encryption (DO-ABE) is used. Compared with the traditional ABE, it better realizes message level-based granular control over the encrypted content. The original data is encrypted and stored in off-chain (external) storage, and the metadata used for transaction processing is stored on the blockchain. When the data requester purchases the right to use original data, he needs to prove to the data owner that he is a legitimate user through access property set S. When the identity verification is successful, the data owner transmits the key SK and the address of the external memory to the data requester. Finally, the data requester can download the encrypted original data by provided address, and obtain the original data through SK and the predefined DO-ABE decryption function on blockchain.

a) Interplanetary File System (IPFS): In the scheme of Malik, N. et al. [25], the authors use Interplanetary File System (IPFS), a way of storing and sharing data that could replace HTTP. In this scheme, THE RSU is only responsible for maintaining the basic functions of the blockchain and processing various information uploaded by the vehicle (road condition and reputation evaluation), while the data storage is completed by IPFS. When the vehicle sends a request for query information to the RSU, the RSU will request the corresponding data from the IPFS system. Jiang X et al. [42] propose a blockchain-enabled object detection framework for automatic driving. In this paper, the authors train the adaptive domain YOLO model to generate cross-domain object detector according to the data uploaded by vehicles to nearby MEC nodes. Among them, the uploaded data uses the interplanetary file system (IPFs), which can store and share data using content addressable and peer-to-peer (P2P) methods.

In order to facilitate the vehicles to make decisions based on the information from other vehicles and RSUs in IOV, Ramaguru R et al. [191] propose a real-time blockchain scheme to complete identity authentication and ensure the communication security between vehicles. There are two parts in the storage system: firstly, BigchainDB is used as a blockchain database to store vehicle details and communication transactions between vehicles. Then, the InterPlanetary File System (IPFs) is used to store large files, such as vehicle logs. The content-address hash from IPFS is referenced in the blockchain transaction stored in bigchaindb, so as to improve the storage efficiency and reduce the space occupation of the blockchain.

C. Maximizes benefit

Su Z et al. [50] contract games to simulate the decision-making process between aggregators and electric vehicles in the case of asymmetric information. In the proposed contract game, the aggregator designs a contract menu that includes its trading strategies for all types of electric vehicles.Within the proposed framework, electric vehicles can choose traditional energy, clean energy, or their hybrid energy to meet their own energy needs while maximizing the utility of operators. In addition, the author propose a dynamic optimal contract allocation and energy allocation algorithm to realize the optimal contract, and solve the problem that the optimal strategy of all electric vehicles may not be satisfied due to the intermittent and instability of power supply problem.

Zhou Z et al. [55] proposes a secure and efficient V2G energy trading framework. Firstly, the authors developed a V2G secure energy trading mechanism based on consortium blockchain, and proposed an effective incentive mechanism based on contract theory considering the information asymmetry. The framework combines edge computing to improve the success probability of block creation, and divides the computing resource allocation problem into two stages: 1) Stackelberg leader follower game; 2) using backward induction to get the optimal strategy. The same game strategy is also applied to Zhou Z et al. [41], Liu K et al. [66], Zhou Z et al. [84] and Lin X et al. [160], to maximize the benefits of both parties to the transaction.

Zhou Z et al. [84] develope a secure energy trading mechanism supported by the consortium blockchain. All transactions are created, disseminated and validated by authorized local energy aggregators (leags). According to the characteristics of each kind of electric vehicle, under the constraints of individual rationality IR, incentive compatibility (IC) and monotonicity, the scheme maximizes the profits of both parties.

Liu H et al. [60] propose a decentralized electricity trading model based on blockchain and smart contract technology to realize peer-to-peer (P2P) trading between electric vehicles (EVS) in the vehicle grid (V2G) network through information equivalence and process disclosure. In order to solve the randomness and uncertainty of electric vehicle charging and discharging, the reverse auction mechanism based on dynamic pricing strategy is adopted to complete the transaction matching, which can not only improve the interests of the seller with weak competitiveness, but also reduce the cost of the buyer. Similarly, Xia S. et al. [62] propose a vehicle to vehicle (V2V) electricity trading scheme based on Bayesian game pricing. This scheme obtains the optimal pricing which maximizes the utility of the buyer and the seller under the linear strategic equilibrium. In Jin R. et al. [93], taking into account the various random factors faced by the charging station load, this scheme uses the Monte Carlo model to determine the future charging demand of the charging station. In Kang J. et al. [103] and Chen C. et al. [130], an iterative double auction mechanism using consortium blockchains is used to ensure

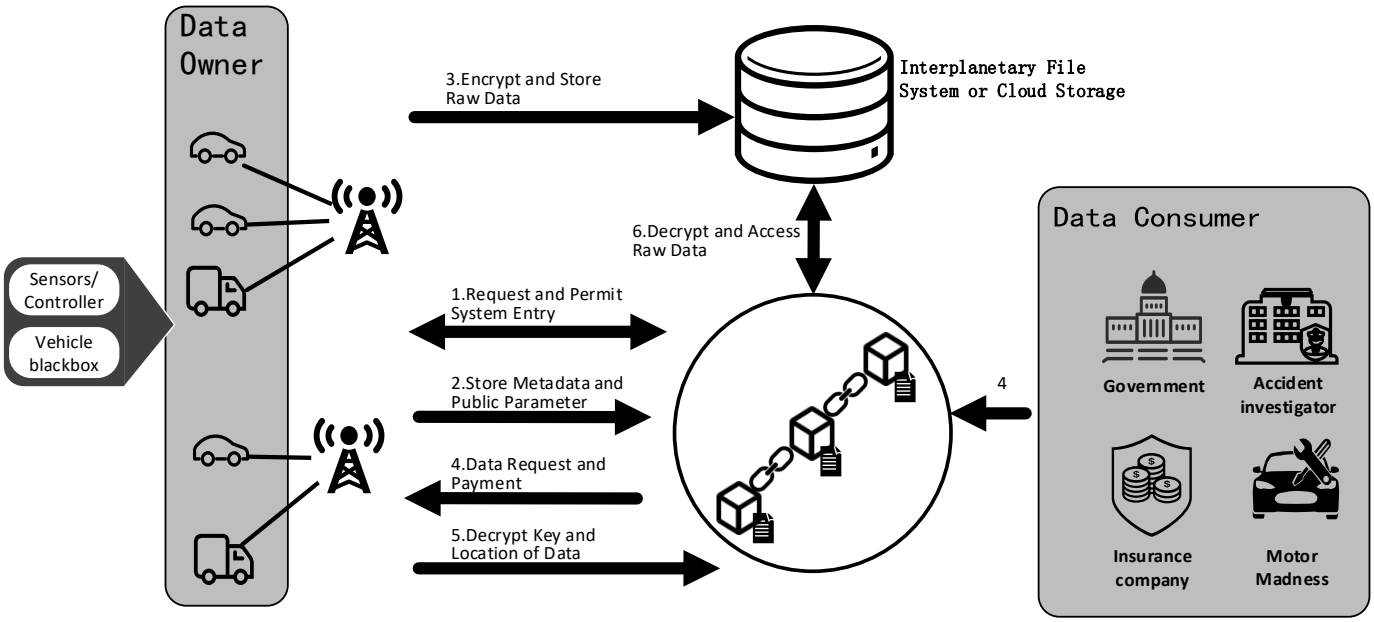


Fig. 12. An example of a blockchain based Internet of vehicles with external storage devices

maximum revenue.

In order to reduce the power fluctuation level in the power grid and the total charging cost of electric vehicles, Liu C. et al. [56] propose a new charging scheme for electric vehicles based on the blockchain distributed smart grid system. Considering the battery capacity, charging rate and charging behavior of EV users, the power fluctuation level is formulated in the scheme. Then, they propose a blockchain based electric vehicle participation (AdBEV) scheme, which uses iceberg order execution algorithm to obtain an improved charging and discharging scheduling scheme for electric vehicles. Huang X. et al. [194] propose a scheme for assisting vehicular fog computing through smart contracts, which can automatically organize and verify request release, workload commitment, task evaluation and reward distribution. The scheme also uses the Stackelberg game framework to optimize the design of smart contracts to minimize user costs.

D. Encourage users to participation

To accurately predict traffic conditions and avoid further congestion, Hassija V et al. [75] propose an advanced blockchain-based secure crowdsourcing model and an incentive model to increase the enthusiasm of users to participate in the crowd sourcing model of crowding probability estimation. When an abnormal situation is found on the road, users can share the incident on the network. The shared information will include some basic parameters such as road type, road conditions, observed events or incidents or any other relevant details. The smart contract deployed on the network verifies the events shared by users, and confirms the authenticity of the event by submitting the results of the same event data by different users. In order to ensure that users will not repeatedly submit information to obtain monetary benefits, only the first user to share information about a certain event will receive tokens to encourage users to share information accurately as soon as possible.

E. Other optimization methods

When the machine learning model learns the data in the vehicle network, it can significantly improve the performance of the vehicle network system in all aspects: faster traffic, less accident rate, and even more comfortable travel planning. Some problems in machine learning have been solved through the combination with blockchain technology: as the complexity of on-board sensor systems increases, A large amount of raw data that can be used for machine learning may bring a huge communication burden and data security issues to the Internet of Vehicles. For example, to reduce communication costs and improve the accuracy of machine learning while retaining data from Connected and Autonomous Vehicles (CAV), Fu Y. et al. [131] propose a BCL framework for AI-enabled CAVs. This framework enables distributed CAVs to train ML models locally and then upload them to the blockchain network, avoiding a large amount of data transmission, and has high security. Liu M. et al. [31] propose a new performance optimization framework based on deep reinforcement learning (DRL) for blockchain-based IoV, which maximizes transactional throughput while ensuring the decen-

Ref.	Design goal	Target	Machine learning methods used	consensus algorithm	Blockchain
[31]	select block producers and adjust the block size and block interval	IOV	deep reinforcement learning	practical Byzantine fault tolerant	
[92]	Match the two sides of the transaction	charging stations and electric vehicles	k-nearest neighbor	practical Byzantine fault tolerant	Consortium blockchain
[131]	reduce communication costs and improve the accuracy of machine learning	Connected and Autonomous Vehicles (CAV)	Blockchain-based Collective Learning (Deep neural networks)	Fault Tolerance-Delegated Proof of Stake (BFT-DPoS)	
[134]	evaluate the credibility of vehicle	autonomous vehicles	federated learning	practical Byzantine fault tolerant	private Blockchain
[140]	evaluate the credibility of vehicle	IOV	federated learning	Delegated Proof of Stake	permissioned blockchain
[148]	Provide information analysis service for vehicles	autonomous vehicles	federated learning	proof-of-work	permissioned blockchain
[151]	detecting driver's behavior	smart vehicles	Convolution Neural Network	proof-of-work	Ethereum
[154]	knowledge sharing	IOV	Federated Learning	proof-of-work	Ethereum
[193]	content caching	vehicular edge computing and networks	Deep reinforcement learning	Proof of Utility (PoU)	permissioned blockchain

tralization, delay and security of the underlying blockchain system Throughput. In this framework, it first analyze the performance of the blockchain system in terms of scalability, decentralization, latency and security. Then, DRL technology is used to select block producers and adjust the block size and block interval to adapt to the dynamic changes of the IoV scene. This framework can effectively improve the throughput of IoV systems supporting blockchain without affecting other attributes. T. Ashfaq et al. [92] use k-nearest neighbor to match charging stations and electric vehicles. Besides, federated learning (FL) has become a powerful privacy-aware decentralized computing approach, which can use distributed training data sets and powerful local learning capabilities of vehicles to analyze personalized data with higher privacy in a network of nodes [148] [154]. Pokhrel S R. [134] designes a lightweight multi-layer blockchain framework to improve the end-to-end reliability of FL system in the Internet of Vehicles (IoV). The sheme is mainly integrated by credibility and reputation modules, which can learn and jointly evaluate the credibility of vehicle observations during the data collection process, and can also perform timely block verification at the blockchain layer. Lu Y et al. [140] propose a blockchain-based federated learning architecture to reduce transmission load while protecting the privacy of data providers. The solution uses a hybrid blockchain architecture, consisting of a permissioned blockchain and a local directed acyclic graph (DAG). The article uses Deep Reinforcement Learning (DRL) to select nodes, and uses an asynchronous federated learning scheme to improve learning efficiency. The learned model will be uploaded to the blockchain, and then two-stage verification will be performed to ensure the reliability of shared data. Khan M Z et al. [151] use deep learning based on convolutional neural network to analyze the driver's behavior in the car, and transmit the verified video data inside the car through blockchain technology.

Jindal A et al. [99] construct a blockchain-based edge-as-a-service framework for secure energy transactions in a V2G environment that supports SDN. The edge node is responsible for providing energy transaction processing for its surrounding EVs, and uses the blockchain consensus algorithm for protection. The communication architecture supporting SDN is used to provide communication for the entire intelligent transportation field. By improving the response speed of information transfer between various nodes, the overall throughput of the network is increased. Similarly, Chaudhary R et al. [157] propose a scheme using SDN architecture to minimize network delay and improve the quality of service (QoS) in the network.

In the scheme of Pajic J et al. [109], a scheduling system named EVA is proposed, which distributes the power demand of electric vehicles in a certain geographical range to the period of low load of power grid, so as to avoid the cost increase caused by the low utilization efficiency of power infrastructure. EVA is based on smart contracts running on the Ethereum blockchain, combined with off-chain computational nodes, which performing schedule calculations using Alternating Direction Method of Multipliers (ADMM) to achieve high transparency and verifability while maintaining high efficiency. In Kamal M et al. [136], the author uses the channel characteristics of wireless network to generate link fingerprints in V2V communication, and adopts the data sharing mechanism based on blockchain, which can realize

real-time data authentication between vehicles. In addition, the scheme uses a simple coding mechanism to provide a lightweight solution for V2V communication in IOV networks.

In Tan H et al. [162], a Certificateless authentication scheme for cloudassisted VANETs is proposed, which uses a new VANET infrastructure with edge computing functions to achieve effective V2R transmission. Data from heterogeneous vehicles is processed and stored in distributed cloud servers, while nearby RSUs act as edge clusters for data caching and necessary local data processing. In addition, a group key dynamic update mechanism is designed in this scheme, and Chinese remainder theorem is applied. In which, complex pair calculation is completed on the side of RSU and TA, while relatively lightweight tasks for authentication and key management are completed by vehicles, which can meet the practical requirements of VANET occasions with limited resources. In order to solve the problem of secure routing in vehicular ad hoc networks, Busygin A et al. [190] introduces a blockchain with floating genesis blocks in the storage and distribution of routing and authentication information to solve the problems related to blockchain size growth.

REFERENCES

[1] Oham, C., et al., A blockchain based liability attribution framework for autonomous vehicles. arXiv preprint arXiv:1802.05050, 2018.

[2] Yang, Z., et al., A blockchain-based reputation system for data credibility assessment in vehicular networks. 2017, IEEE. p. 1–5.

[3] Lu, Z., et al., A privacy-preserving trust model based on blockchain for VANETs. IEEE Access, 2018. 6: p. 45655–45664.

[4] Ugwu, M.C., et al., A tiered blockchain framework for vehicular forensics. International Journal of Network Security & Its Applications (IJNSA) Vol, 2018. 10.

[5] Yin, B., et al., An Efficient Collaboration and Incentive Mechanism for Internet of Vehicles (IoV) With Secured Information Exchange Based on Blockchains. IEEE Internet of Things Journal, 2019. 7(3): p. 1582–1593.

[6] Ali, M.S., et al., Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2018.21(2): p. 1676–1717.

[7] Lu, Z., et al., Bars: a blockchain-based anonymous reputation system for trust management in vanets. 2018, IEEE. p. 98–103.

[8] van der Heijden, R.W., et al., Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication. 2017. p. 1–5.

[9] Cebe, M., et al., Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Communications Magazine, 2018. 56(10): p. 50–57.

[10] Demir, M., O. Turetken and A. Ferworn, Blockchain Based Transparent Vehicle Insurance Management. 2019, IEEE. p. 213–220.

[11] Luo, B., et al., Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Transactions on Vehicular Technology, 2019.69(2): p. 2034–2048.

[12] Kang, J., et al., Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 2018. 6(3): p. 4660–4670.

[13] Dorri, A., et al., Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 2017. 55(12): p.119–125.

[14] Yang, Z., et al., Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 2018. 6(2): p. 1495–1505.

[15] Shrestha, R., R. Bajracharya and S.Y. Nam, Blockchain-based message dissemination in VANET. 2018, IEEE. p. 161–166.

[16] Li, L., et al., Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems, 2018. 19(7): p. 2204–2220.

[17] Liang, H., et al., MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X. IEEE Communications Magazine, 2019.57(10): p. 77–83.

[18] Reyna, A., et al., On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 2018. 88: p. 173–190.

[19] Chai, H., et al., Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. IEEE Access, 2019. 7: p.175744–175757.

[20] Nadeem, S., et al., Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2019. 10(1): p. 288–295.

[21] Leiding, B., P. Memarmoshrefi and D. Hogrefe, Self-managed and blockchain-based vehicular ad-hoc networks. 2016. p. 137–140.

[22] Michelin, R.A., et al., SpeedyChain: A framework for decoupling data from blockchain for smart cities. 2018. p. 145–154.

[23] Kang, J., et al., Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory.IEEE Transactions on Vehicular Technology, 2019. 68(3): p. 2906–2920.

[24] Yuan Y, Wang F Y. Towards blockchain-based intelligent transportation systems[C]//2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016: 2663-2668.

[25] Malik, N., et al., Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach. 2019, IEEE. p. 34–41.

[26] Singh, M. and S. Kim, Trust bit: Reward-based intelligent vehicle commination using blockchain paper. 2018, IEEE. p. 62–67.

[27] Li, C., et al., Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework. IEEE Transactions on Intelligent Transportation Systems, 2020.

[28] Guo S, Hu X, Zhou Z, et al. Trust access authentication in vehicular network based on blockchain[J]. China Communications, 2019, 16(6): 18-30.

[29] Kulathunge A S, Dayarathna H. Communication framework for vehicular ad-hoc networks using Blockchain: Case study of Metro Manila Electric Shuttle automation project[C]//2019 International Research Conference on Smart Computing and Systems Engineering (SCSE). IEEE, 2019: 85-90.

[30] Zhang X, Chen X. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network[J]. IEEE Access, 2019, 7: 58241-58254.

[31] Liu M, Teng Y, Yu F R, et al. Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.

[32] Li M, Zhu L, Lin X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing[J]. IEEE Internet of Things Journal, 2018, 6(3): 4573-4584.

[33] Xu C, Liu H, Li P, et al. A remote attestation security model based on privacy-preserving blockchain for v2x[J]. IEEE Access, 2018, 6: 67809-67818.

[34] Guo H, Meamari E, Shen C C. Blockchain-inspired event recording system for autonomous vehicles[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 218-222.

[35] Malik N, Nanda P, Arora A, et al. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks[C]//2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018: 674-679.

[36] Yin B, Mei L, Jiang Z, et al. Joint cloud collaboration mechanism between vehicle clouds based on blockchain[C]//2019 IEEE International Conference on Service-Oriented System Engineering (SOSE). IEEE, 2019: 227-2275.

[37] Kuhn M, Giang H, Otten H, et al. Blockchain Enabled Traceability–Securing Process Quality in Manufacturing Chains in the Age of Autonomous Driving[C]//2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD). IEEE, 2018: 131-136.

[38] Calvo J A L, Mathar R. Secure blockchain-based communication scheme for connected vehicles[C]//2018 European Conference on Networks and Communications (EuCNC). IEEE, 2018: 347-351.

[39] Bai H, Wu C, Yang Y, et al. A Blockchain-Based Traffic Conditions and Driving Behaviors Warning Scheme in the Internet of Ve-

hicles[C]//2019 IEEE 19th International Conference on Communication Technology (ICCT). IEEE, 2019: 1160-1164.
[40] Brousmiche K L, Heno T, Poulain C, et al. Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned[C]//2018 9th IFIP international conference on new technologies, mobility and security (NTMS). IEEE, 2018: 1-5.
[41] Zhou Z, Tan L, Xu G. Blockchain and edge computing based vehicle-to-grid energy trading in energy internet[C]//2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2018: 1-5.
[42] Jiang X, Yu F R, Song T, et al. Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach[J]. IEEE Internet of Things Journal, 2020, 7(5): 3681-3692.
[43] Wang Y, Su Z, Zhang K, et al. Challenges and Solutions in Autonomous Driving: A Blockchain Approach[J]. IEEE Network, 2020.
[44] Gandhi G M. Artificial Intelligence Integrated Blockchain For Training Autonomous Cars[C]//2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM). IEEE, 2019, 1: 157-161.
[45] Ying Z, Ma M, Yi L. BAVPM: Practical Autonomous Vehicle Platoon Management Supported by Blockchain Technique[C]//2019 4th International Conference on Intelligent Transportation Engineering (ICITE). IEEE, 2019: 256-260.
[46] Sang-Oun L E E, Hyunseok J, Han B. Security Assured Vehicle Data Collection Platform by Blockchain: Service Provider's Perspective[C]//2019 21st International Conference on Advanced Communication Technology (ICACT). IEEE, 2019: 265-268.
[47] Masoud M Z, Jaradat Y, Jannoud I, et al. CarChain: A Novel Public Blockchain-based Used Motor Vehicle History Reporting System[C]//2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE, 2019: 683-688.
[48] Kandah F, Huber B, Altarawneh A, et al. BLAST: Blockchain-based Trust Management in Smart Cities and Connected Vehicles Setup[C]//2019 IEEE High Performance Extreme Computing Conference (HPEC). IEEE, 2019: 1-7.
[49] AlJabri O, AlDhaheri O, Mohammed H, et al. Facilitating Electric Vehicle Charging Across the UAE Using Blockchain[C]//2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE, 2019: 1-4.
[50] Su Z, Wang Y, Xu Q, et al. A secure charging scheme for electric vehicles with smart communities in energy blockchain[J]. IEEE Internet of Things Journal, 2018, 6(3): 4601-4613.
[51] Huang X, Xu C, Wang P, et al. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem[J]. IEEE Access, 2018, 6: 13565-13574.
[52] Sharma P K, Moon S Y, Park J H. Block-VN: A distributed Blockchain based vehicular network architecture in smart city[J]. Journal of information processing systems, 2017, 13(1).
[53] Pustišek M, Kos A, Sedlar U. Blockchain based autonomous selection of electric vehicle charging station[C]//2016 international conference on identification, information and knowledge in the Internet of Things (IIKI). IEEE, 2016: 217-222.
[54] Jiang T, Fang H, Wang H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis[J]. IEEE Internet of Things Journal, 2018, 6(3): 4640-4649.
[55] Zhou Z, Wang B, Dong M, et al. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 50(1): 43-57.
[56] Liu C, Chai K K, Zhang X, et al. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform[J]. IEEE Access, 2018, 6: 25657-25665.
[57] Brousmiche K L, Durand A, Heno T, et al. Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1281-1286.
[58] Lasla N, Younis M, Znaidi W, et al. Efficient distributed admission and revocation using blockchain for cooperative its[C]//2018 9th IFIP international conference on new technologies, mobility and security (NTMS). IEEE, 2018: 1-5.
[59] Wang Y, Su Z, Zhang K. A Secure Private Charging Pile Sharing Scheme with Electric Vehicles in Energy Blockchain[C]//2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2019: 648-654.
[60] Liu H, Zhang Y, Zheng S, et al. Electric vehicle power trading mechanism based on blockchain and smart contract in V2G network[J]. IEEE Access, 2019, 7: 160546-160558.
[61] Akın Y, Dikkollu C, Kaplan B B, et al. Ethereum Blockchain Network-based Electrical Vehicle Charging Platform with Multi-Criteria Decision Support System[C]//2019 1st International Informatics and Software Engineering Conference (UBMYK). IEEE, 2019: 1-5.
[62] Xia S, Lin F, Chen Z, et al. A Bayesian Game based Vehicle-to-Vehicle Electricity Trading Scheme for Blockchain-enabled Internet of Vehicles[J]. IEEE Transactions on Vehicular Technology, 2020.
[63] Firoozjaei M D, Ghorbani A, Kim H, et al. EVChain: A Blockchain-based Credit Sharing in Electric Vehicles Charging[C]//2019 17th International Conference on Privacy, Security and Trust (PST). IEEE, 2019: 1-5.
[64] Javed M U, Javaid N. Scheduling Charging of Electric Vehicles in a Secured Manner using Blockchain Technology[C]//2019 International Conference on Frontiers of Information Technology (FIT). IEEE, 2019: 351-3515.
[65] Sharma V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV)[J]. IEEE Communications Letters, 2018, 23(2): 246-249.
[66] Liu K, Chen W, Zheng Z, et al. A Novel Debt-Credit Mechanism for Blockchain-Based Data-Trading in Internet of Vehicles[J]. IEEE Internet of Things Journal, 2019, 6(5): 9098-9111.
[67] Baza M, Nabil M, Lasla N, et al. Blockchain-based firmware update scheme tailored for autonomous vehicles[C]//2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019: 1-7.
[68] Deshpande V, George L, Badis H. Safe: A blockchain and secure element based framework for safeguarding smart vehicles[C]//2019 12th IFIP Wireless and Mobile Networking Conference (WMNC). IEEE, 2019: 181-188.
[69] Saranti P G, Chondrogianni D, Karatzas S. Autonomous vehicles and blockchain technology are shaping the future of transportation[C]//The 4th conference on sustainable urban mobility. Springer, Cham, 2018: 797-803.
[70] Orecchini F, Santiangeli A, Zuccari F, et al. Blockchain technology in smart city: A new opportunity for smart environment and smart mobility[C]//International conference on intelligent computing & optimization. Springer, Cham, 2018: 346-354.
[71] Baldini G, Hernández-Ramos J L, Steri G, et al. Zone keys trust management in vehicular networks based on blockchain[C]//2019 Global IoT Summit (GIoTS). IEEE, 2019: 1-6.
[72] Sharma S, Ghanshala K K, Mohan S. Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture[C]//2019 IEEE 2nd 5G World Forum (5GWF). IEEE, 2019: 452-457.
[73] Pu Y, Xiang T, Hu C, et al. An efficient blockchain-based privacy preserving scheme for vehicular social networks[J]. Information Sciences, 2020.
[74] Wang Q, Ji T, Guo Y, et al. TrafficChain: A Blockchain-Based Secure and Privacy-Preserving Traffic Map[J]. IEEE Access, 2020, 8: 60598-60612.
[75] Hassija V, Gupta V, Garg S, et al. Traffic Jam Probability Estimation Based on Blockchain and Deep Neural Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020.
[76] Lei A, Cruickshank H, Cao Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems[J]. IEEE Internet of Things Journal, 2017, 4(6): 1832-1843.
[77] Buzachis A, Filocamo B, Fazio M, et al. Distributed Priority Based Management of Road Intersections Using Blockchain[C]//2019 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2019: 1159-1164.
[78] Knirsch F, Unterweger A, Engel D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions[J]. Computer Science-Research and Development, 2018, 33(1-2): 71-79.
[79] Kim M H, Park K S, Yu S J, et al. A secure charging system for electric vehicles based on blockchain[J]. Sensors, 2019, 19(13): 3028.
[80] Akın Y, Dikkollu C, Kaplan B B, et al. Ethereum Blockchain Network-based Electrical Vehicle Charging Platform with Multi-Criteria Decision Support System[C]//2019 1st International Informatics and Software Engineering Conference (UBMYK). IEEE, 2019: 1-5.
[81] Wang Y, Su Z, Xu Q, et al. Contract based energy blockchain for secure electric vehicles charging in smart community[C]//2018 IEEE 16th

Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). IEEE, 2018: 323-327.

[82] Zhang L, Luo M, Li J, et al. Blockchain based secure data sharing system for Internet of vehicles: A position paper[J]. Vehicular Communications, 2019, 16: 85-93.

[83] Leiding B, Vorobev W V. Enabling the vehicle economy using a blockchain-based value transaction layer protocol for vehicular ad-hoc networks[C]//Proc. Medit. Conf. Inf. Syst.(MCIS). 2018: 1-31.

[84] Zhou Z, Wang B, Guo Y, et al. Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2019, 3(3): 205-216.

[85] Liu C, Chai K K, Zhang X, et al. Proof-of-Benefit: A Blockchain-Enabled EV Charging Scheme[C]//2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, 2019: 1-6.

[86] Sheikh A, Kamuni V, Urooj A, et al. Secured Energy Trading Using Byzantine-Based Blockchain Consensus[J]. IEEE Access, 2019, 8: 8554-8571.

[87] Asfia U, Kamuni V, Sheikh A, et al. Energy trading of electric vehicles using blockchain and smart contracts[C]//2019 18th European Control Conference (ECC). IEEE, 2019: 3958-3963.

[88] Liu H, Zhang P, Pu G, et al. Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4221-4232.

[89] Wang Y, Su Z, Zhang N. BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3620-3631.

[90] Chen X, Zhang T, Ye W, et al. Blockchain-based Electric Vehicle Incentive System for Renewable Energy Consumption[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020.

[91] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran and N. Naseer, "A Blockchain based Privacy-Preserving System for Electric Vehicles through Local Communication," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149129.

[92] T. Ashfaq, N. Javaid, M. U. Javed, M. Imran, N. Haider and N. Nasser, "Secure Energy Trading for Electric Vehicles using Consortium Blockchain and k-Nearest Neighbor," 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 2235-2239, doi: 10.1109/IWCMC48107.2020.9148494.

[93] Jin R, Zhang X, Wang Z, et al. Blockchain-Enabled Charging Right Trading Among EV Charging Stations[J]. Energies, 2019, 12(20): 3922.

[94] Zhang X, Wang D. Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain[J]. IEEE Access, 2019, 7: 97281-97295.

[95] Jeong S, Dao N N, Lee Y, et al. Blockchain based billing system for electric vehicle and charging station[C]//2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2018: 308-310.

[96] Kirpes B, Becker C. Processing electric vehicle charging transactions in a blockchain-based information system[J]. 2018.

[97] Yahiatene Y, Rachedi A, Riahla M A, et al. A blockchain-based framework to secure vehicular social networks[J]. Transactions on Emerging Telecommunications Technologies, 2019, 30(8): e3650.

[98] Gao F, Zhu L, Shen M, et al. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks[J]. IEEE network, 2018, 32(6): 184-192.

[99] Jindal A, Aujla G S, Kumar N. SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment[J]. Computer Networks, 2019, 153: 36-48.

[100] Liu D, Li D, Liu X, et al. Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid[C]//2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2018: 1-5.

[101] Yucel F, Bulut E, Akkaya K. Privacy Preserving Distributed Stable Matching of Electric Vehicles and Charge Suppliers[C]//2018 IEEE 88th Vehicular Technology Conference (VTC-Fall). IEEE, 2018: 1-6.

[102] Ji Y, Hou R, Lui K S, et al. A Blockchain-Based Vehicle Platoon Leader Updating Scheme[C]//ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020: 1-6.

[103] Kang J, Yu R, Huang X, et al. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains[J]. IEEE Transactions on Industrial Informatics, 2017, 13(6): 3154-3164.

[104] Lei A, Cao Y, Bao S, et al. A blockchain based certificate revocation scheme for vehicular communication systems[J]. Future Generation Computer Systems, 2020, 110: 892-903.

[105] Erdin E, Cebe M, Akkaya K, et al. Building a private bitcoin-based payment network among electric vehicles and charging stations[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1609-1615.

[106] Li W, Nejad M, Zhang R. A blockchain-based architecture for traffic signal control systems[C]//2019 IEEE International Congress on Internet of Things (ICIOT). IEEE, 2019: 33-40.

[107] Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing[J]. IEEE Network, 2018, 32(3): 78-83.

[108] Xie L, Ding Y, Yang H, et al. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs[J]. IEEE Access, 2019, 7: 56656-56666.

[109] Pajic J, Rivera J, Zhang K, et al. Eva: Fair and auditable electric vehicle charging service using blockchain[C]//Proceedings of the 12th ACM International Conference on Distributed and Event-based Systems. 2018: 262-265.

[110] Gorenflo C, Golab L, Keshav S. Mitigating trust issues in electric vehicle charging using a blockchain[C]//Proceedings of the Tenth ACM International Conference on Future Energy Systems. 2019: 160-164.

[111] Wang H, Wang Q, He D, et al. BBARS: Blockchain-based anonymous rewarding scheme for V2G networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 3676-3687.

[112] Hua S, Zhou E, Pi B, et al. Apply blockchain technology to electric vehicle battery refueling[C]//Proceedings of the 51st Hawaii International Conference on System Sciences. 2018.

[113] Cui J, Zhang X, Zhong H, et al. RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(4): 6417-6428.

[114] Niyato D, Kim D I, Kang J, et al. Incentivizing Secure Block Verification by Contract Theory in Blockchain-Enabled Vehicular Networks[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-7.

[115] Zheng D, Jing C, Guo R, et al. A traceable blockchain-based access authentication system with privacy preservation in VANETs[J]. IEEE Access, 2019, 7: 117716-117726.

[116] Javaid U, Aman M N, Sikdar B. DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts[C]//2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, 2019: 1-5.

[117] Arora A, Yadav S K. Block chain based security mechanism for internet of vehicles (IoV)[C]//Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT). 2018: 26-27.

[118] Sharma R, Chakraborty S. Blockapp: using blockchain for authentication and privacy preservation in iov[C]//2018 IEEE Globecom Workshops (GC Wkshps). IEEE, 2018: 1-6.

[119] Alam M S U, Iqbal S, Zulkernine M, et al. Securing vehicle ECU communications and stored data[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.

[120] Jeong B G, Youn T Y, Jho N S, et al. Blockchain-Based Data Sharing and Trading Model for the Connected Car[J]. Sensors, 2020, 20(11): 3141.

[121] Kwame O B, Xia Q, Sifah E B, et al. V-Chain: A Blockchain-Based Car Lease Platform[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1317-1325

[122] Singh M, Kim S. Branch based blockchain technology in intelligent vehicle[J]. Computer Networks, 2018, 145: 219-231.

[123] Singh M, Kim S. Blockchain based intelligent vehicle data sharing framework[J]. arXiv preprint arXiv:1708.09721, 2017.

[124] Rowan S, Clear M, Gerla M, et al. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels[J]. arXiv preprint arXiv:1704.02553, 2017.

[125] Rathee G, Sharma A, Iqbal R, et al. A blockchain framework for

securing connected and autonomous vehicles[J]. Sensors, 2019, 19(14): 3165.

[126] Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2018, 6(3): 4660-4670.

[127] Wang X, Zeng P, Patterson N, et al. An improved authentication scheme for internet of vehicles based on blockchain technology[J]. IEEE access, 2019, 7: 45061-45072.

[128] Singh M, Kim S. Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain[J]. arXiv preprint arXiv:1707.07442, 2017.

[129] Gao J, Agyekum K O B O, Sifah E B, et al. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks[J]. IEEE Internet of Things Journal, 2019, 7(5): 4278-4291.

[130] Chen C, Wu J, Lin H, et al. A secure and efficient blockchain-based data trading approach for Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2019, 68(9): 9110-9121.

[131] Fu Y, Yu F R, Li C, et al. Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles[J]. IEEE Wireless Communications, 2020, 27(2): 197-203.

[132] Iqbal R, Butt T A, Afzaal M, et al. Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions[J]. International Journal of Distributed Sensor Networks, 2019, 15(1): 1550147719825820.

[133] Pedrosa A R, Pau G. ChargeItUp: On blockchain-based technologies for autonomous vehicles[C]//Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. 2018: 87-92.

[134] Pokhrel S R. Towards efficient and reliable federated learning using blockchain for autonomous vehicles[J]. Computer Networks, 2020: 107431.

[135] Singh M, Kim S. Introduce reward-based intelligent vehicles communication using blockchain[C]//2017 International SoC Design Conference (ISOCC). IEEE, 2017: 15-16.

[136] Kamal M, Srivastava G, Tariq M. Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020.

[137] Kim S. Blockchain for a trust network among intelligent vehicles[M]//Advances in Computers. Elsevier, 2018, 111: 43-68.

[138] Ahmad F, Kerrache C A, Kurugollu F, et al. Realization of blockchain in named data networking-based internet-of-vehicles[J]. IT Professional, 2019, 21(4): 41-47.

[139] Hu J, He D, Zhao Q, et al. Parking management: A blockchain-based privacy-preserving system[J]. IEEE Consumer Electronics Magazine, 2019, 8(4): 45-49.

[140] Lu Y, Huang X, Zhang K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4298-4311.

[141] Cheng L, Liu J, Xu G, et al. SCTSC: A semicentralized traffic signal control mode with attribute-based blockchain in IoVs[J]. IEEE Transactions on Computational Social Systems, 2019, 6(6): 1373-1385.

[142] Hu W, Hu Y, Yao W, et al. A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles[J]. IEEE Access, 2019, 7: 139703-139711.

[143] Liu C, Chai K K, Lau E T, et al. Blockchain based energy trading model for electric vehicle charging schemes[C]//International Conference on Smart Grid Inspired Future Technologies. Springer, Cham, 2018: 64-72.

[144] Yao Y, Chang X, Mišić J, et al. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775-3784.

[145] Bonadio A, Chiti F, Fantacci R, et al. An integrated framework for blockchain inspired fog communications and computing in internet of vehicles[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(2): 755-762.

[146] Narbayeva S, Bakibayev T, Abeshev K, et al. Blockchain technology on the way of autonomous vehicles development[J]. Transportation Research Procedia, 2020, 44: 168-175.

[147] Song Y, Fu Y, Yu F R, et al. Blockchain-Enabled Internet of Vehicles With Cooperative Positioning: A Deep Neural Network Approach[J]. IEEE Internet of Things Journal, 2020, 7(4): 3485-3498.

[148] Pokhrel S R, Choi J. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges[J]. IEEE Transactions on Communications, 2020.

[149] Su Z, Wang Y, Xu Q, et al. LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue[J]. IEEE Transactions on Dependable and Secure Computing, 2020.

[150] Chen C, Xiao T, Qiu T, et al. Smart-Contract-Based Economical Platooning in Blockchain-Enabled Urban Internet of Vehicles[J]. IEEE Transactions on Industrial Informatics, 2019, 16(6): 4122-4133.

[151] Khan M Z, Khan M U G, Irshad O, et al. Deep learning and blockchain fusion for detecting driver's behavior in smart vehicles[J]. Internet Technology Letters, 2019: e119.

[152] Mendiboure L, Chalouf M A, Krief F. Survey on blockchain-based applications in internet of vehicles[J]. Computers & Electrical Engineering, 2020, 84: 106646.

[153] Qian Y, Jiang Y, Hu L, et al. Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles[J]. IEEE Network, 2020, 34(2): 46-51.

[154] Chai H, Leng S, Chen Y, et al. A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020.

[155] Song Y, Yu R, Fu Y, et al. Multi-Vehicle Cooperative Positioning Correction Framework Based on Vehicular Blockchain[C]//Proceedings of the 9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications. 2019: 23-29.

[156] Umoren I A, Jaffary S S A, Shakir M Z, et al. Blockchain-Based Energy Trading in Electric Vehicle Enabled Microgrids[J]. IEEE Consumer Electronics Magazine, 2020.

[157] Chaudhary R, Jindal A, Aujla G S, et al. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system[J]. Computers & Security, 2019, 85: 288-299.

[158] Javaid U, Aman M N, Sikdar B. A Scalable Protocol for Driving Trust Management in Internet of Vehicles with Blockchain[J]. IEEE Internet of Things Journal, 2020.

[159] Li M, Weng J, Yang A, et al. Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11): 11248-11259.

[160] Lin X, Wu J, Mumtaz S, et al. Blockchain-based On-Demand Computing Resource Trading in IoV-Assisted Smart City[J]. IEEE Transactions on Emerging Topics in Computing, 2020.

[161] Shrestha R, Nam S Y. Regional blockchain for vehicular networks to prevent 51% attacks[J]. IEEE Access, 2019, 7: 95021-95033.

[162] Tan H, Chung I. Secure Authentication and Key Management With Blockchain in VANETs[J]. IEEE Access, 2019, 8: 2482-2498.

[163] Syed T A, Siddique M S, Nadeem A, et al. A Novel Blockchain-Based Framework for Vehicle Life Cycle Tracking: An End-to-End Solution[J]. IEEE Access, 2020, 8: 111042-111063.

[164] Rawat D B, Doku R, Adebayo A, et al. Blockchain enabled Named Data Networking for Secure Vehicle-to-Everything Communications[J]. IEEE Network, 2020.

[165] Sun G, Dai M, Zhang F, et al. Blockchain Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles[J]. IEEE Internet of Things Journal, 2020.

[166] Deng X, Gao T. Electronic Payment Schemes Based on Blockchain in VANETs[J]. IEEE Access, 2020, 8: 38296-38303.

[167] Kandah F, Huber B, Skjellum A, et al. A blockchain-based trust management approach for connected autonomous vehicles in smart cities[C]//2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2019: 0544-0549.

[168] Rahman M A, Rashid M M, Barnes S J, et al. A Blockchain-based Secure Internet of Vehicles Management Framework[C]//2019 UK/China Emerging Technologies (UCET). IEEE, 2019: 1-4.

[169] Hu W, Yao W, Hu Y, et al. Collaborative optimization of distributed scheduling based on blockchain consensus mechanism considering battery-swap stations of electric vehicles[J]. IEEE Access, 2019, 7: 137959-137967.

[170] Shrestha R, Bajracharya R, Shrestha A P, et al. A new type of blockchain for secure message exchange in VANET[J]. Digital Communications and Networks, 2020, 6(2): 177-186.

[171] Li Y, Hu B. An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain[J]. IEEE Transactions on Smart Grid, 2019, 11(3): 2627-2637.

[172] Yang Y T, Chou L D, Tseng C W, et al. Blockchain-based traffic event validation and trust verification for VANETs[J]. IEEE Access, 2019, 7: 30868-30877.

[173] Mollah M B, Zhao J, Niyato D, et al. Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey[J]. arXiv preprint arXiv:2007.06022, 2020.
[174] Zielińska A, Skowron M, Bień A. The concept of the blockchain technology model use to settle the charging process of an electric vehicle[C]//2019 Applications of Electromagnetics in Modern Engineering and Medicine (PTZE). IEEE, 2019: 271-274.
[175] Salem M, Mohammed M, Rodan A. Security approach for in-vehicle networking using blockchain technology[C]//International Conference on Emerging Internetworking, Data & Web Technologies. Springer, Cham, 2019: 504-515.
[176] Cho S Y, Chen N, Hua X. Developing a Vehicle Networking Platform Based on Blockchain Technology[C]//International Conference on Blockchain. Springer, Cham, 2019: 186-201.
[177] Velliangiri S, Kumar G K L, Karthikeyan P. Unsupervised Blockchain for Safeguarding Confidential Information in Vehicle Assets Transfer[C]//2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2020: 44-49.
[178] Singh M, Kim S. Crypto trust point (cTp) for secure data sharing among intelligent vehicles[C]//2018 International Conference on Electronics, Information, and Communication (ICEIC). IEEE, 2018: 1-4.
[179] Silva F C, A Ahmed M, Martínez J M, et al. Design and implementation of a Blockchain-Based energy trading platform for electric vehicles in smart campus parking lots[J]. Energies, 2019, 12(24): 4814.
[180] Buzachis A, Celesti A, Galletta A, et al. A secure and dependable multi-agent autonomous intersection management (MA-AIM) system leveraging blockchain facilities[C]//2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion). IEEE, 2018: 226-231.
[181] Jameel F, Javed M A, Zeadally S, et al. Efficient Mining Cluster Selection for Blockchain-based Cellular V2X Communications[J]. arXiv preprint arXiv:2007.01052, 2020.
[182] Thakur S, Breslin J G. Electric vehicle charging queue management with blockchain[C]//International Conference on Internet of Vehicles. Springer, Cham, 2018: 249-264.
[183] Kohlbrenner F, Nasirifard P, Löbel C, et al. A Blockchain-based Payment and Validity Check System for Vehicle Services[C]//Proceedings of the 20th International Middleware Conference Demos and Posters. 2019: 17-18.
[184] Kaur K, Garg S, Kaddoum G, et al. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure[C]//2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2019: 1-6.
[185] Noh J, Jeon S, Cho S. Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles[J]. Electronics, 2020, 9(1): 74.
[186] Chen X, Zhang X. Secure Electricity Trading and Incentive Contract Model for Electric Vehicle Based on Energy Blockchain[J]. IEEE Access, 2019, 7: 178763-178778.
[187] Mostafa A. VANET Blockchain: A General Framework for Detecting Malicious Vehicles[J]. J. Commun, 2019, 14(5): 356-362.
[188] Saini A, Sharma S, Jain P, et al. A secure priority vehicle movement based on blockchain technology in connected vehicles[C]//Proceedings of the 12th International Conference on Security of Information and Networks. 2019: 1-8.
[189] Oham C, Michelin R, Kanhere S S, et al. B-FERL: Blockchain based Framework for Securing Smart Vehicles[J]. arXiv preprint arXiv:2007.10528, 2020.
[190] Busygin A, Konoplev A, Kalinin M, et al. Floating Genesis Block Enhancement for Blockchain Based Routing Between Connected Vehicles and Software-defined VANET Security Services[C]//Proceedings of the 11th International Conference on Security of Information and Networks. 2018: 1-2.
[191] Ramaguru R, Sindhu M, Sethumadhavan M. Blockchain for the Internet of Vehicles[C]//International Conference on Advances in Computing and Data Sciences. Springer, Singapore, 2019: 412-423.
[192] Davydov V, Bezzateev S. Accident Detection in Internet of Vehicles using Blockchain Technology[C]//2020 International Conference on Information Networking (ICOIN). IEEE, 2020: 766-771.
[193] Dai Y, Xu D, Zhang K, et al. Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4312-4324.
[194] Huang X, Ye D, Yu R, et al. Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design[J]. IEEE/CAA Journal of Automatica Sinica, 2020, 7(2): 426-441.
[195] Khelifi H, Luo S, Nour B, et al. Reputation-based blockchain for secure NDN caching in vehicular networks[C]//2018 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2018: 1-6.
[196] Zachary C L. Method and system using a blockchain database for data exchange between vehicles and entities: U.S. Patent Application 15/605,677[P]. 2018-11-29.
[197] Guo C, Huang X, Zhu C, et al. Distributed Electric Vehicle Control Model Based on Blockchain[C]//IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2019, 486(1): 012046.
[198] Li H, Pei L, Liao D, et al. Blockchain meets VANET: An architecture for identity and location privacy protection in VANET[J]. Peer-to-Peer Networking and Applications, 2019, 12(5): 1178-1193.
[199] Awais Hassan M, Habiba U, Ghani U, et al. A secure message-passing framework for inter-vehicular communication using blockchain[J]. International Journal of Distributed Sensor Networks, 2019, 15(2): 1550147719829677.
[200] Chai H, Leng S, Zeng M, et al. A Hierarchical Blockchain Aided Proactive Caching Scheme for Internet of Vehicles[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.
[201] Hassija V, Chamola V, Han G, et al. Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4182-4191.
[202] Zhang X D, Li R, Cui B. A security architecture of VANET based on blockchain and mobile edge computing[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 258-259.
[203] Alvarez I, Bowman M. Trusted vehicle telematics using blockchain data analytics: U.S. Patent 10,284,654[P]. 2019-5-7.
[204] Hassija V, Chamola V, Garg S, et al. A blockchain-based framework for lightweight data sharing and energy trading in V2G network[J]. IEEE Transactions on Vehicular Technology, 2020.
[205] Ou W, Deng M, Luo E. A decentralized and anonymous data transaction scheme based on blockchain and zero-knowledge proof in vehicle networking (workshop paper)[C]//International Conference on Collaborative Computing: Networking, Applications and Worksharing. Springer, Cham, 2019: 712-726.
[206] Lu Z, Wang Q, Qu G, et al. A blockchain-based privacy-preserving authentication scheme for vanets[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2792-2801.
[207] Yang Y, He D, Wang H, et al. An efficient blockchain-based batch verification scheme for vehicular ad hoc networks[J]. Transactions on Emerging Telecommunications Technologies, 2019.
[208] Bagga P, Sutrala A K, Das A K, et al. Blockchain-based batch authentication protocol for Internet of Vehicles[J]. Journal of Systems Architecture, 2020: 101877.
[209] El Sayed A I, Megahed M H, Azeem M H A. Design New Collision Resistant Hash Function for Blockchain in V2V Communication[C]//2019 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE, 2019: 1-8.
[210] Liu J, Li X, Jiang Q, et al. BUA: A Blockchain-based Unlinkable Authentication in VANETs[C]//ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020: 1-6.