An Overview of Internet of Vehicles Based on Blockchain

Zhao xin
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] [92] [95] [96] [110] [133] 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] [77] proposes 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. [105] designs and implements 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.

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. For example, [92] uses 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] . [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. [140] proposes 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. [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 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. To reduce communication costs and improve the accuracy of machine learning while retaining data from Connected and Autonomous Vehicles (CAV), [131] proposes 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.

III. 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. On blockchain and its integration with IOT. Challenges and opportunities[18] Based on the investigation of the blockchain architecture scheme of the Internet of things, three kinds of blockchain architectures are summarized. The Applications of Blockchains in the Internet of Things: A Comprehensive Survey[6] on the basis of the previous, summarized the general structures of 4 Blockchains, which are as follows:

- Gateway devices as end-points to the blockchain
- Devices as transaction-issuers 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 A blockchain-based reputation system for data credibility Assessment in Vehicular Networks [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 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. In the BlockChain: A Distributed Solution to Automotive Security and Privacy[13] supposed 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 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 Blockchain Based Transparent Vehicle Insurance Management[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.

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: [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 [125].

On the basis of [44], [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.

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 "self-managed and blockchain based Ad-Hoc networks[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. "Blockching-Based Message Dissemination in VANET" [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. [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 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.

In the Trust and Reputation in Vehicular Networks: A Smart Plant-based Approach[12],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. In [42], the proposer of the scheme also uses IPFS to store data. Securing Cognitive Radio Vehicular Ad Hoc Network with Fog Node based Distributed Blockchain Cloud Architecture[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, [32] propose an efficient and privacy-preserving carpooling (FICA) 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 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. [36] proposes a multi-vehicle cloud collaboration framework called JointCloud, introduces 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.

IV. A TRUSTED PLATFORM FOR INTERNET OF VEHICLES

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.

A. 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.A privacy-preserving trust model based on blockchain for VANETS[3], A blockchain-based reputation system for data credibility assessment in vehicular networks[2] 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 A privacy-preserving trust model based on blockchain for VANETS[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. [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.

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. [73] proposes an efficient, reliable, and privacy-protected 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, we 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.

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 blockchain enabled trust based location privacy protection scheme in VANET [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.

B. Classification based on trust value generation role

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

In "a blockchain based reporting system for data reliability assessment in vehicular networks [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.

Blockchain based decentralized trust management in vehicular networks [14] has made some modifications on the basis of [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.**

[19] follows the basic idea of [14] and provides 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. [25] also uses the way vehicles evaluate each other of [14] and stores credit information in Interplanetary File systems (IPFS) , and vehicles can quickly get credit information through the lightweight blockchain.

[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. [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. [123] [128] and [135] 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.

[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.

[48] uses the design in [45] and [2] ,amd establishes 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, [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 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, [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.

[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 [89], [91] proposes 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.

[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. [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:** : [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.

C. Other methods to ensure the authenticity of data

[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. [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.

[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, [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.

[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.

V. Data security and privacy protection

As a powerful cryptography tool, blockchain completes data uploading and verification through hash chain, consensus algorithm and other technologies, so it has excellent performance in reliability, availability, non-repudiation and other aspects. [37] uses the traceability of the blockchain system to monitor the production process of vehicles, and allows 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. Although the data stored in the blockchain has strong tamper-proof capability, it is weak in leak-proof. The reason is that as a distributed ledger, blockchain is designed to be open and transparent: transactions are broadcast throughout the blockchain network and verified by nodes in the network. In most scenarios, all nodes keep a complete copy of blockchain information (not necessarily starting from the creation block, but starting at a certain time or before a fixed number of blocks). Malicious nodes can pretend to be normal nodes in the network to apply for sharing blockchain information, or directly attack normal nodes to obtain blockchain information. In the Internet of vehicles, a large number of data interactions will take place among the nodes of all parties involved, and these interactions often involve the privacy of users or confidential data in some laws and regulations. The relevant parties of the data must not want to let irrelevant people have access to the data, that is, the confidentiality of the data needs to be realized. In addition, in some application scenarios (such as intelligent transportation systems), the data from vehicle sensors are required to be untampered with, namely the integrity of the data, which requires the transformation of the blockchain-based vehicle network with the help of additional cryptography methods.

In [27], it is proposed to use vehicle sensors to assist in improving the accuracy of GPS (Global Positioning System), and vehicle position information will be transmitted to the blockchain. [147] 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 [9], [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. In this case, ensuring that information can be transmitted in the car network in a secret and safe manner has become the most important concern in the solution. In fact, in almost all IOV solutions, information security or privacy protection issues are more or less considered. Some researchers apply relatively mature secure transmission solutions to the Internet of Vehicles based on blockchain. Below, let's summarize the implementation of various solutions.

[35] proposed a blockchain-based framework to ensure the privacy and security of vehicles in decentralized networks. Here, a private blockchain is used to provide selective access to the ledger, in which Revocation Authority (RA) and Certificate Authority (CA) have complete control over the ledger, and only give RSUs the right to read, OBUs The information needs to be obtained through RSU, thus avoiding any exposure to untrusted entities. The hash table and ledger entry pointers located in the CA support the traceability of the vehicle to prevent any suspicious behavior. CA is an ECC-based PKI to establish a system by setting up system parameters, which are stored in the vehicle during registration together with the public hash function. In addition, RSU also provides the public key generated by the private key of the CA for signature verification in the ledger. The blockchain network between CA, RA, and rsu is established by their public keys. They use the public key to address and verify each other when storing and retrieving transactions, and securely generate blocks for identity verification and revocation of the ledger. [104] proposes a blockchain-based certificate revocation scheme to prevent internal attacks in the VCS network and reduce the CRL size and broadcast message overhead. The proposed blockchain structure enables PKI to keep tracking the ownership of pseudonym sets and distribute CRLs in an efficient manner. A part of CRL distribution is used in conjunction with the group key management scheme to minimize the message overhead of certificate revocation. The program discussed the two scenarios of CRL, namely infrastructure level and vehicle

level, and studied the CRL size of different programs, proving that the blockchain-based program can significantly reduce the size of CRL. Secondly, the authors analyzed the message handshake process between infrastructures and vehicles, and proved that the scheme has higher efficiency and robustness compared with the traditional structure. Finally, the message overhead results of the experimental simulation show that the blockchain-based scheme releases the communication volume by reducing the total number of messages, thereby reducing the communication burden.

As we all know, although asymmetric encryption algorithms are powerful and difficult to replace, their efficiency is far lower than that of symmetric encryption algorithms. In order to improve efficiency, [57] designed and implemented a hybrid encryption protocol (using symmetric encryption scheme S and asymmetric encryption scheme A), which can dynamically add and delete authorized User. The key pair in A consists of two key pairs, one for encryption and the other for signature. The verification adopts the signed output. If the signature is valid, the signed message is returned, otherwise an error is returned.

[59] developes a reputation-based secure PCP(private charging piles) sharing protocol using BLS multi-signature to effectively reach consensus in the blockchain.

BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV[]

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, [30] proposed a data security sharing and storage system based on Consortium Blockchain (DSSCB). This digital signature technology based on the bilinear pairing properties of elliptic curves can be used to ensure the reliability and integrity of data transmission to nodes. Similarly, the RA in [117] uses the elliptic curve Diffie-Hellmankey protocol to assign pseudo-identities (PID) and generates a private key from the public key pair according to the PID. The vehicle-based architecture in [119] uses elliptic curve-based PKE. And [146] uses a blockchain system based on the Exonum platform to develop a car motion tracking system that uses an elliptic curve digital signature algorithm (ECDSA) to enter data and confirm its acceptance of transactions.

[33] proposes a remote proof security model based on privacy-protecting blockchain, called RASM. The two core steps of the remote proof security model based on the privacy-protecting blockchain are realized: The first is reliable identity authentication. The second is to use computing nodes to make decisions and use accounting nodes to write data blocks.

[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, we 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.

[38] proposes a security protocol based on consensus strength (blockchain) for exchanging messages between vehicles. It uses the scheme based on ring-signature to verify the identity of the vehicle joining the network, and uses the secure communication channel created by multi-party smart contract to verify through the blockchain based mechanism. The protocol satisfies the strict delay requirements of vehicle networks by instantaneous communication, and provides anonymous security system for network members who rely on cryptographic primitives.

[39] uses a group signature-based identity verification protocol to ensure privacy and security, while also ensuring identity traceability. Compared with the traditional signature method, the authentication time based on the group signature changes less with the increase of the number of vehicles, and the communication time is more stable.

[11] and [63] use K-anonymity to provide privacy protection for users information in Internet of vehicles. K-anonymity is a simple, effective and widely used privacy protection method. It ensures that in a group of K similar objects, the target object is no different from other K-1 objects. Therefore, the probability of user information being leaked is 1 / K.

[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.

[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).

[76] proposes a key management scheme suitable for vehicular communication systems (VCS) scenarios, including key transmission and dynamic key management schemes between two heterogeneous networks to reduce key transmission time. In the proposed scheme, a new blockchain concept is introduced to simplify the key transmission handshake process to obtain better efficiency. The third-party authority (central manager) is deleted from the scheme, and the key transmission process is verified and authenticated by the security manager (SM) network. The records of these processes (mining blocks) are shared on the network so that SMs can create a public ledgers.

[78] pointed 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 put forward 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 cars 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.

In order to solve the hidden safety hazards in the system, [79] proposes 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.

In order to achieve conditional privacy in vehicles, [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. We also designed a mechanism to implement pre- and post-event countermeasures. In our system, we 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 our system can be used to retrieve the true identity of the message sender.

For the verification process of blocks in the blockchain used by electric vehicles and distribution networks, [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, in order to emphasize the security of the system, the article also considers various attack scenarios that may appear on different nodes of the system to illustrate the security performance of the Byzantine blockchain consensus.

[94] proposes a blockchain-based trusted mechanism for traffic departments to adjust signal lights, and control the state of traffic vehicles through smart contracts to effectively prevent vehicles from broadcasting false information and malicious requests, thereby improving the credibility of vehicles. In order to protect the privacy and safety of vehicles from threats, the ElGamal encryption and group signature algorithm are used in the scheme to ensure the confidentiality, privacy and non-repudiation of any information. Anonymity is the simplest and most effective means to protect user privacy. [98] proposes 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. [118] also uses pseudo-identity to achieve its purpose.

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, [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. In order to defend the CV-based traffic signal control system from malicious data attacks, [106] designed 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. For the vital security and privacy issues of the V2G network in the smart grid, [111] proposes the concept of an blockchain-based anonymous rewarding scheme(BBARS) for the V2G network with available cryptographic primitives. The sheme studied thee CAG anonymity andBV anonymity simultaneously, and realized the unlinkability between the payer's address and the payee's address. Two different PKCs are used in the BBARS scheme: it uses PKCs in PKI to use aggregate signatures to improve efficiency, and use another different PKC when performing operations on the blockchain.

In [115], a blockchain-based access authentication system in VANET environment is proposed. The system not only provides a trusted communication environment for smart vehicles, but also uses anonymity to hide the real identity of users. The authors also designed a secure and distributed transaction storage scheme based on blockchain to prevent internal vehicles from distributing forged messages, and ensure the correctness of transaction information while tracking malicious vehicles. [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.

[126] 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. In [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. [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 attributebased encryption (CP-ABE) and blockchain technology.

Vehicle-mounted Fog services (VFS) need to span multiple geographically distributed data centers, which results in cross-data center authentication. Therefore, [144] proposes a Blockchain-assisted Lightweight Anonymous authentication mechanism (BLA) for distributed VFS to realize flexible cross-data center authentication, enabling vehicles to decide whether to re-authenticate when entering a new vehicle fog data center (VFD). The BLA also eliminates communication between the vehicle and the service managers (SM) and between SM during authentication, thereby reducing communication delays and transport burdens.

VI. Internet of Vehicles system optimizationn

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, 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 [54]

Blockchain: A distributed solution to automotive security and privacy[13] does not rely on RSUs and other infrastructure to communicate, but directly forms a cluster of geographically close vehicles to achieve efficient data interaction within the cluster, with no message exchange between the clusters. Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication[8] adopts 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. [65] also adopts 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 [129] standardizes the message transmission mode of the cluster model and adds the credibility evaluation of the message.

The blockchain communication scheme proposed by "A Blockchain Based Liability Attribution Framework for Autonomous Vehicles[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 "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles[9]".

MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X[17] proposes 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.

[28] established 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.

[45] proposes 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 [102] proposes a scheme to achieve a credible and efficient platoon leader update method. [150] introduced a scheme of selecting PH by reputation value to motivate vehicles to become PH and keep the platoon updated dynamically

[47] proposes 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.

[74] proposes 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 [82].

[97] proposes 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.

2) Faster transaction confirmation: SpeedyChain: A framework for decoupling data from blockchain for smart cities[22] adopts 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, [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 [42] [102] [114] and [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. [31] proposed a new performance optimization framework based on deep reinforcement learning (DRL) for blockchain-based IoV, which maximizes transactional throughput while ensuring the decentralization, 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.

[81] uses 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, [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. [142] uses 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. [154] use a light-weight Proof-of-Knowledge (PoK) consensus mechanism to enable the vehicle with the most knowledge to generate a blockchain

B. Storage space savings

"Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles[9]" roughly follows the structure of" A Blockchain Based Liability Attribution Framework for Autonomous Vehicles[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. "A tiered blockchain framework for vehicular forensics[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 [30] proposed 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.

[58] discusses and adoptes 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. [120] propose a data sharing scheme based on a blockchain-based data-owner-based attribute-based encryption(DO-ABE) for a vehicle data marketplace platform. The system uses consortium Blockchain to store metadata on blockchain and store encrypted raw data on off-chain storage, thereby safely and effectively processing large-capacity and privacy-sensitive black box video data. Data owners can use the blockchain-based DO-ABE and owner-defined access control lists (ACL) to control the data they own.

C. Other optimization methods

[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.

[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 [41] [66] [84], and maximizes the benefits of both parties to the transaction.

[84] developes 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.

[60] proposes 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, [62] proposes 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 [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 [103] and [130], an iterative double auction mechanism using consortium blockchains is used to ensure maximum revenue.

In order to reduce the power fluctuation level in the power grid and the total charging cost of electric vehicles, [56] proposes 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.

To accurately predict traffic conditions and avoid further congestion, [75] proposes 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.

[99] constructs 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.

Based on the consortium blockchain, [100] proposes 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.

In [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.

VII. Conclusion

This paper summarizes some schemes of the Internet of vehicles based on the blockchain, and briefly introduces some methods used in the scheme to ensure the credibility and improve the availability. I hope that in the future, researchers in this field can learn from the methods summarized in this paper to build a more efficient and complete vehicle networking system.

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 Vehicles[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 Net-

works[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. ChargeltUp: 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]
[208]
[209]
[210]
[211]
[212]