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] 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, automobile sales 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]

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: Vehicle position correction: A vehicular blockchain Nets-based GPS error sharing Framework [27], 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. 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.

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'scloud 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.

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. For various reasons, there is currently no blockchain-based vehicle networking scheme using this model.

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:** :

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.**

Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles[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. The Trust and Reputation in Vehicular Networks: A Smart contract-based Approach[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.

Trust bit: Reward-based intelligent Vehicle commination using Blockchain Paper [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. CreditCoin A privacy-blockchain-based Incentive Announcement Network for Communications of Smart Vehicles[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.

Bars: A blockchain-based Anonymous Reputation system for Trust Management in Vanets [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.

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.

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 Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework [], 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. In Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles[9], A tiered blockchain framework for vehicular forensics[] 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.

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, Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain[] 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.

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.

[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.

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.

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. 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.

[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.

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 theprobability of success when producing blocks.

3) Efficient consensus algorithm: [42] DPOS [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.

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.

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.

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. and F. Wang, Towards blockchain-based intelligent transportation systems. 2016, IEEE. p. 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.