Zheng *et al. Journal of Cloud Computing* (2023) 12:99
https://doi.org/10.1186/s13677-023-00478-8

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

IoV data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing

Tiange Zheng[1], Junhua Wu[1*] and Guangshun Li[1]

Abstract

Achieving efficient and secure sharing of data in the Internet of Vehicles (IoV) is of great significance for the development of smart transportation. Although blockchain technology has great potential to promote data sharing and privacy protection in the context of IoV, the problem of securing data sharing should be payed more attentions. This paper proposes an IoV data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing. Firstly, to improve protocol's efficiency, a dual-chain structure empowered by alliance chain is introduced as the model architecture. Secondly, for the space problem characterized by data storage and security, we adopt distributed storage with the help of edge devices. Finally, to both ensure the efficiency of consensus protocol and protect the privacy of vehicles and owners simultaneously, we improve DPoS consensus algorithm to realize the efficient operation of the IoV data sharing model, which is closer to the actual needs of IoV. The comparison with other data sharing models highlights the advantages of this model, in terms of data storage and sharing security. It can be seen that the improved DPoS has high consensus efficiency and security in IoV.

Keywords Edge computing, Blockchain, DPoS, Data sharing

Introduction

With the continuous innovation of intelligent transportation technology, basic safety information and application data can be transmitted between vehicles. The Internet of Vehicles can collect, store and send all working conditions, static and dynamic information of vehicles. The Internet of Vehicles generally has the real-time live view function, and the mobile network is used to realize the interaction between people and vehicles. Data sharing has become an important technical means to improve vehicle driving safety and travel efficiency. Data sharing technology can enhance the vehicle's ability to understand the current traffic environment and network state, and improve the vehicle's response speed to unknown scenes. The Internet of Vehicles technology will conduct real-time diagnosis on the vehicle, diagnose the fault problems existing in the vehicle, and inform the owner, greatly reducing the potential safety hazards. Although traditional mobile cloud computing (MCC) has more resources and larger storage space, and can migrate tasks to a remote cloud with strong computing power, vehicle transmission of large amounts of data to MCC will lead to huge energy costs and transmission delays [1]. It is unable to meet the local processing requirements of low latency, high bandwidth and large-scale mobile terminals and its emerging applications.

At the same time, the tension between resource constrained devices and computing intensive applications is difficult to provide satisfactory quality of service [2]. In addition, the security threat is an important problem in the cloud computing environment, and the resulting data security problem is becoming more and more serious [3]. Malicious vehicles often publish incorrect data or tamper

*Correspondence:
Junhua Wu
shdwjh@163.com
[1] School of Computer Science, Qufu Normal University, Rizhao, China

with others'shared data in the network, thus misleading vehicle driving judgment and even causing traffic accidents. Therefore, ensure the security in the process of data sharing, efficiently deploy edge nodes and schedule edge resources to meet application needs and improve service quality. It is very important to realize efficient data sharing between vehicles and improve the efficiency of transportation.

With the rapid development of mobile computing and mobile communication technology [4], Mobile Edge Computing (MEC) proposes to sink computing, storage, processing and other functions from cloud servers to the edge of wireless networks, providing mobile users with adjacent real-time computing and localized processing capabilities, so as to reduce network delay and improve user experience. In mobile edge computing, users can migrate computing intensive and delay sensitive applications from local to edge servers to solve problems such as limited computing resources and battery capacity [5].

The Internet of Vehicles (IoV) is one of the main application scenarios of MEC, which is computationally intensive, time-delay sensitive, real-time and large data volume. At the same time, the IoV is an important sub-class of the IoT, which is used to connect vehicles intelligently. Its essence is an interactive network composed of information such as vehicle location, speed, route and surrounding traffic conditions. Vehicles in the IoV environment are equipped with advanced onboard sensors and intelligent electronic devices and are further equipped with wireless communication On Board Unit(OBU) [6], which can effectively complete the interactive communication between the internal members of the IoV [7]. Data information is transmitted and shared mainly through Vehicle to Vehicle (V2V), Vehicle to Road (V2R) and Road to Road (R2R) as show in Fig. 1. Encryption technology is used to process the sensitive data in the vehicle node locally. At the same time, the non-sensitive information is transmitted through the Internet to realize the information interaction based on the Vehicle and the Road Side Unit (RSU).

In the IoV, mobile vehicles will constantly generate many different data types, including additional data such as mobile tracks, traffic information and multimedia data. Vehicles communicate, interact with information, and jointly collect and share data [8]. Data sharing between vehicles play a crucial role in improving driving safety and enhancing onboard services. IoV uses different communication types to conduct information interaction, provide safe and effective traffic information for traffic participants, and create a comfortable and safe driving environment. If some criminals release false information or communication information, and let other participants make the wrong driving decisions, it is easy to cause traffic congestion or even traffic accidents, resulting in serious consequences [9]. Therefore, how to efficiently and safely use large amounts of available data to improve the driving experience, and provide a wide range of high-quality services in the IoV, has become an urgent problem.

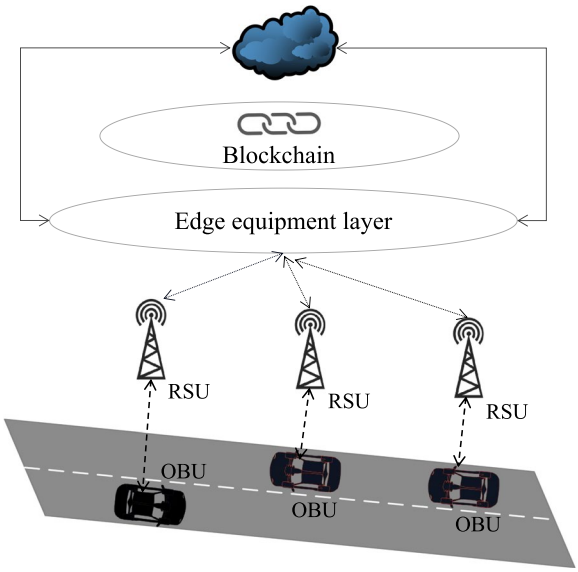

Fig. 1 Application scenario

Data sharing in the IoV is facing three key challenges. Firstly, there are centralized server single-point faults. Secondly, privacy protection is a practical and critical issue [10]. Data providers pay more and more attention to data security and privacy issues, and do not take any effective measures for data upload and storage, which is easy to cause privacy information disclosure. In addition, there is no effective incentive mechanism for data sharing [11] which aims to encourage participants to collect and share data and ensure the quality of data; These challenges hinder data sharing between vehicles and hinder the development of IoV.

Rehman et al. [12] combined cloud computing with blockchain technology to provide security services for cloud based Internet of Things applications. At the same time, it effectively prevents the attack of the malicious edge server, making the data sharing in the system more secure. However, the system is not well adapted for large-scale data sharing. Xu et al. [13] proposed an online electric vehicle charging system based on anonymous blockchain, which eliminates the third-party platform through blockchain technology and meets the requirements for user anonymity, information authenticity and system security. Kang et al. [14] proposed to use alliance chain and smart contract technology to realize the safe storage and sharing of data and calculate the credibility

of vehicles based on the weight subjective logic model, effectively preventing unauthorized data sources from ensuring high-quality data sharing between vehicles. However, the privacy protection of data is difficult to achieve. Ma et al. [15] proposed a blockchain-based data security sharing scheme for IoV, which realizes efficient and secure data sharing of IoV through smart contracts. The PBFT consensus mechanism is adopted to ensure that the network nodes quickly reach the consensus and maintain the ledger's consistency, but the resource consumption is relatively large. Wang et al. [16] proposed a safe and effective encrypted data retrieval and sharing scheme to ensure the security of data sharing while the keywords are retrieved and sorted to achieve accurate retrieval. Sharma et al. [17] proposed a blockchain-based data sharing scheme that relies heavily on third-party centralized institutions for traditional data sharing, which improves trust, but lacks fine-grained data access control and data privacy protection mechanism.

Currently, many scholars in the IoV field are trying to combine blockchain technology with the MEC. First, utilizing the characteristics of blockchain decentralization and each node backing up complete data information can make up for a single point of fault defects in centralized servers [18]. Second, using blockchain privacy, immutability and traceability ensures privacy, security, and integrity of data sharing. Moreover, using the consensus mechanism in blockchain and smart contracts is important to promote data sharing and ensure data quality between vehicles. To this end, this paper proposes an IoV data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing, with the following two aspects:

1. This paper gives full play to the advantages of blockchain and edge computing, embeds edge computing devices in roadside units and vehicles, which can transform the traditional cloud data interaction form into cloud-edge, and uses the dual chain mode based on the alliance chain to isolate the vehicle condition analysis results from the private data. At the same time, it encrypts the data before the chain, stores the real ciphertext in the edge device, and places the data summary and storage location on the blockchain. It enhances the protection of vehicle data security and privacy, and solves the problem of safe storage and sharing of system data.
2. In view of the problems of malicious nodes and voting enthusiasm in the consensus process, this paper improves the voting model and optimizes the reward and punishment mechanism on the basis of the dpos consensus mechanism, and solves the problems in the dpos algorithm, such as the untimely handling of malicious nodes and the low voting enthusiasm of nodes. The participants in the Internet of vehicles can reach consensus efficiently and reduce the impact of malicious nodes on the consensus process.

Related work

Blockchain

Blockchain is a distributed ledger system with a specific data structure that combines data blocks in a chain manner and ensures that it cannot be tampered with and forged. The blockchain, with its essential characteristics of decentralization, persistence, anonymity, and auditability [19]. As a peer-to-peer distributed ledger, each node stores complete ledger information, effectively avoiding data loss caused by single-node failure [20]. Blockchain mainly has three application types: Public Block Chains, Consortium Block Chains, and Private Block Chains. Blockchain uses encryption [21] chain block structure to verify and store data, using P2P, consensus mechanism [22, 23] implement distributed node verification, communication, and trust relationship. Using intelligent contract [24] automated execution of some pre-defined rules and terms, realize data automation to form a new data recording, storage, and sharing method [25].

Centralized servers mainly handle traditional data sharing, but enormous challenges. First, if the central server fails, the entire network server is at risk of paralysis, such as a denial of service attack on a centralized server that causes a single point of failure. Second, users have limited control over how and who personal data is used, and data stored in a centralized server may leak personal privacy. Finally, data stored in centralized servers lack reliability and traceability. Centralized IoT infrastructure requires third parties to trust for data processing, while data stored on centralized servers risk tampering with [26]. Blockchain technology has been widely concerned due to its decentralized autonomy, tamper-proof, and traceability. Blockchain technology is considered a critical decentralized technology to streamline and simplify network management and improve 6G network performance. The data stored on the blockchain needs to be jointly maintained by the whole network, effectively transferring value [27] between nodes that lack trust. In the past, the data sharing of the Internet of things could only be carried out through a trusted third-party platform. Now, using blockchain technology can run decentralized [28]. However, IoT data sharing research based on blockchain technology still faces many challenges.

The primary application types of blockchain are divided into Public Block Chains, Consortium BlockChain, and Private Block Chains. The comparative analysis of the

three basic blockchain application types is shown in Table 1.

Because the Public Blockchains and the Private Blockchains face different objects, their structure and characteristics differ. All the members of the public blockchain have the same permissions, and all the transaction records are open and transparent, which determines the credibility of the public blockchain, which is extremely difficult and difficult to achieve. However, the public blockchain transaction process requires all member certification, so the transaction speed is prolonged, and the transaction cost is high, so it does not apply to IoV.

The private chains are just the opposite. The private blockchain has a back-stage for managers. Some essential managers can modify and restore transactions appropriately and restrict access to users, and only authorized users can join. Although the transaction speed of the private blockchain is fast, the number of nodes in the private blockchain is limited. Also, because its transaction authentication has no lower limit requirements for the number of users, and its credibility is not high, there are significant problems for IoV.

The consortium blockchain combines the two advantages. It not only has the private blockchain fast processing speed and access control mechanism but also maintains a specific decentralized nature, making the transaction certification highly credible. Therefore, the consortium blockchain can adapt to the extremely high safety and fast speed response requirements of the data management of the IoV. The consortium blockchain can also realize cross-department sharing within the company and external data sharing through data desensitization processing.

Edge computing

Cloud computing is a kind of distributed computing technology. Its system structure includes organization, unified resources, platform, and application layer [29]. As an extension of cloud computing, edge computing is a highly virtualized platform that provides network services such as computing and storage between terminal devices and the cloud. The objects of edge computing operations are to downlink data from the cloud and uplink data from intelligent machines. Various devices are around, with considerable computing capacity and idle resources [30]. If the system can handle some simple edge devices in a low latency way, it can have low latency as it takes real-time tasks. Due to the limitation of computing, storage resources, and battery capacity of IoT devices, some tasks need to be unloaded to the edge server for processing [31, 32]. On the IoV, the vehicle's interior space has been dramatically improved, and more and more electronic devices with high processing, storage, and computing capabilities are equipped on the vehicle [33]. At the same time, to better serve vehicles, a large number of high-performance roadside equipment are deployed on both sides of the road. The above results show that the performance of IoV system will be improved if such on-board equipment and roadside equipment can be used reasonably.

The edge computing model can process massive temporary data at the network's edge. Only data with high computational complexity can be uploaded to the cloud, significantly reducing the pressure on network bandwidth and data center [34]. At the same time, it can provide data processing services near the data production terminal, eliminating the step of requesting a response from the cloud computing center and achieving the goal of reducing system delay and enhancing service response. Edge computing can prevent users from uploading private data, mainly by storing private data in network edge devices to mitigate the risk of data leakage [35]. In addition, edge computing can provide more personalized services based on user privacy data and improve user experience.

In the edge computing system, vehicle data needs frequent interaction, which leads to end-to-end data transmission. Big data can play a key role and quickly provide basis for decision-making [36]. In the wireless communication process of computing nodes, data is vulnerable to various malicious attacks such as man in the middle attack, eavesdropping attack, etc. The central control node may also suffer from a single point of failure, which may cause data leakage [37] or malicious tampering, leading to task execution failure or economic losses. Therefore, it is very important to ensure the privacy, correctness and integrity of data during task execution. To

Table 1 Differences of three types of blockchains

Blockchain type	user	Bookkeeper	Degree of centralization	propagation velocity	visibility	Consensus mechanism
Public Chain	Anybody	All Members	Decentralization	slower	all	Pow,Pos
Federation Chain	Federation Members	Federation Selected Members	Incomplete Decentralization	Quick	Partially visible	DPos, PBFT
Private Chain	Internal Company	Administrators	Weak Centralization	Fastest	Internal visibility	PAXOS

achieve this goal, edge computing oriented data security sharing and storage, access control and other schemes are feasible technical routes.

Consensus mechanism

In recent years, blockchain application has been involved in many fields such as medical care, finance and transportation. In a decentralized system with highly decentralized decision-making power, realizing the effectiveness and consistency of block data is key to blockchain technology research. Different consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS) [38], and Delegated Proof of Stake (DPoS) have been proposed successively. It solves the problems of who accounts, the long-standing Byzantium, and how to reach consensus in a completely free and open blockchain and ensure the system's consistency.

The core idea of the PoW consensus mechanism is that each node performs the hash operation of the node through computing power competition to obtain the generation permission of blocks and ensure the consistency of network distributed accounting. But it also exposes the disadvantage that the PoW consensus mechanism requires computers to have powerful computing power. For example risk and revenue game will inevitably lead to joint mining problems [39, 40], so under the PoW consensus mechanism, although can guarantee the reliability of the consensus process, a block takes too long, too much computing and power resources are wasted in competition, and over-concentrated computing power also makes the blockchain network more concentrated, so more vulnerable to attack. Therefore, it does not adapt to the high-speed changing application scenarios of the IoV.

For the problems of PoW, the PoS consensus mechanism was born, which proved to be very feasible and scalable. The essence of PoS is to use the certificate of rights and interests instead of the computing power-based workload proof in PoW, and the node in the system with the highest equity rather than the highest computing power obtains the block accounting right [41]. PoS somewhat reduces the time to reach a consensus and reduces the waste of resources in the PoW mechanism. However, the PoS consensus mechanism also has some disadvantages: the higher the rights and interests of the nodes can occupy more accounting rights in the subsequent consensus process. So that the accounting rights are more and more concentrated in the nodes with higher rights and interests, thus destroying the fairness of the network consensus. At the same time, it is more likely to cause the blockchain fork [42] than the PoW algorithm, so many nodes need to be run to ensure a normal consensus network. So the PoW cannot support large-scale data sharing in the IoV.

DPoS is an evolutionary version of POS. Its accounting rights are generated by node voting. Ordinary nodes can vote for the relatively credible representative as the block producer, and the partial nodes with the most votes will get the right to generate the block [43]. In the DPoS consensus mechanism, each node can decide the authorization nodes it trusts, and these authorization nodes take accounts to generate new blocks. Therefore, the number of nodes involved in validation and bookkeeping is significantly reduced, resulting in fast consensus validation. However, DPoS also has the following risks: ordinary nodes do not actively participate in voting because the election of representatives consumes a lot of time and computing power. The weight of each node is proportional to the amount of money, so there is a potential risk of malicious nodes and bribery nodes with a significant weight voting for themselves, resulting in corruption. If malicious nodes fail to generate blocks, the whole blockchain's production capacity will decline, damaging all nodes' interests.

Zhang et al. [44] proposed a blockchain-based trust management system of IoV that combines the consensus mechanism of PoW and PoS. Larger vehicles that can change their reputation can be updated to the blockchain first. The scheme has obvious limitations for malicious vehicles. However, the enthusiasm for node voting is not high, and the delay of the IoV trust management system still needs to be reduced. Tan et al. [45] designed an alliance blockchain based on the digital twin, proposing that the BFT-POS consensus algorithm achieves an effective consensus on transaction recording. At the same time, a contract-based incentive mechanism is developed to ensure the enthusiasm of data owners to share data. But the privacy protection of data is not perfect. Chai et al. [46] proposed a diffusion and practical Diffusion and practical Byzantine fault-tolerant mechanism which reduces the consensus latency, improves the operational efficiency of the blockchain and can reach consensus efficiently and safely in the blockchain network. Still, it does not consider the data-sharing incentive mechanism between vehicles. A consensus protocol based on a voting mechanism and alliance blockchain was proposed by Li et al. [47]. However, the protocol does not match the participants of the Internet of Vehicles in terms of roles. And it lacks a sound reward and punishment mechanism to deal with possible malicious attackers. Zhang et al. [48] proposed a blockchain-based IoV system, but the consensus protocol used is the original PoW protocol. The protocol consumes a lot of time and resources to generate blocks, thus burdening the IoV.

Although experts have done a lot of research on consensus mechanisms, and the innovations have their advantages and disadvantages, the efficiency of data sharing in the consensus mechanism is not well solved. So further research on the consensus mechanism applicable to IoV systems is still needed.

IoV data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing

Hybrid architecture IoV data sharing scheme

Vehicle data assets are non-physical assets and play a vital role in providing high quality services for IoV. Blockchain can well solve the security problem of the network layer of vehicle data asset transaction. However, the IoV's original data volume is huge, the system complexity is high, the number of users is large, the data is relatively scattered, and if all the data is notified to the whole network, it will make the cost huge. Therefore, the distributed storage achieved by simply using blockchain technology does not meet the needs of IoV data sharing platform. If the blockchain is separated from the database and only the blockchain is used for transactions, this architecture deviates from the original intention of the blockchain and cannot guarantee the security of data storage. Due to the complexity of the Internet of vehicles terminal equipment, the system can process a large amount of data in a short time. Under the traditional blockchain architecture, the huge data set in edge computing is difficult to be quickly confirmed by the whole network, resulting in the edge network system cannot process a large amount of data in a short time.

In order to solve the above problems, data blocks and transaction blocks can be separated to construct a dual chain blockchain. The vehicle condition analysis result can be isolated from the vehicle privacy data, and the data can be double encrypted to enhance the protection of vehicle data security and privacy. The combination of edge computing and blockchain, the deployment of blockchain nodes in the Internet of Things devices with edge computing capabilities, to achieve the safe storage of edge data. As the "local brain" of Internet of Vehicles devices, edge computing can store and process data of different devices, optimize and modify the working state and path of various devices, so as to achieve the overall application efficiency of real-time scenes.

As shown in Fig. 2. The platform is top-down into three levels: user layer, operation layer, and data layer: (1) The data layer is composed of vehicle information collection chain *VC* (vehicle chain) and real-time vehicle condition analysis chain *AC* (analysis chain). A summary of vehicle information data stored by *VC* is actively generated and uploaded by vehicle sensors and intelligent

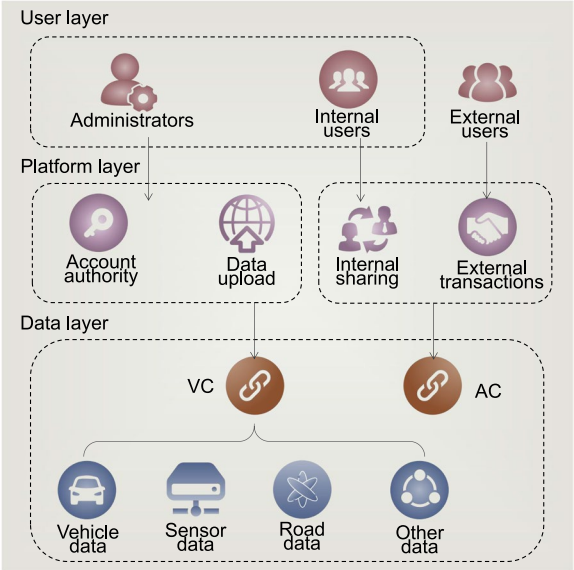

Fig. 2 Functional model

electronic devices; a data report is generated after analyzing vehicle information data stored in *AC*. (2) The operation layer consists of permission management, data transmission, and intelligent contract. Account authority can manage the rights of account and data, only for the user level; The data upload interacts with the VC of the data layer; the smart contract is divided into internal access contract and external access contract, where users access the analysis report in the *AC*. (3) The user layer includes administrators, internal users, and external users. Administrators have access to internal and external users' data and administrative access to data upload. Internal and external users further analyze and apply the obtained data to various scenarios.

In the double-chain structure, *VC* chain and *AC* chain are connected in a hash-based manner. In order to save system resources and improve storage efficiency, user U_i generates a key through the Elliptic Curve Cryptography (ECC), selects random number k as the user's private key, calculates elliptic curve point KG as the public key, and obtains a public-private key pair (pk_i,sk_i) for requesting and decrypting the data. The data owner UN_j uploads the hash value and data digest stored in the edge device to the VC chain, and at the same time generates a symmetric key $SyKey_j$ in addition to the public-private key pair (pk_j,sk_j) to encrypt the original data and store it in the idle in edge devices.

In addition, the data owner designates a set of users who have access to all of its files, and generates and maintains an access control matrix M_j to record user access rights. The file data is uploaded to the cloud after being

divided into blocks and symmetrically encrypted. The user's public key and the data owner's access control matrix are stored in the blockchain for sharing. The data owner can obtain the authorized user's public key from the blockchain. Users can also obtain the access control matrix of multiple data owners through the blockchain to check their own access rights to different data.

After receiving the data request sent by the user U_i, the data owner U_i, the data owner UN_j verifies the access authority of the user in the access control matrix M_j. If the corresponding position of the matrix is 1, the public key pk_i of U_i is used to encrypt the symmetric key $SyKey_j$, and is used as the elliptic curve. on a specific point, and encode the data to the corresponding position of the curve, generate a random number r, calculate $C_1 = M + rKG$, $C_2 = rG$, and obtain the encrypted symmetric key $CSKey_j$. The signed data package is stored in the cloud platform, which includes encrypted data, encrypted symmetric key and access control matrix. The authorized user downloads the data package in the cloud, obtains the relevant ciphertext, then uses his own private key sk_i to decrypt $CSKey_j$, calculates $C_1 - kC_2$ to obtain the symmetric key $SyKey_j$, and finally uses $SyKey_j$ to decrypt to obtain the requested data. Data demanders with internal authority upload the report generated after analyzing the vehicle information data in edge devices to the AC chain, and provide the results to external users through smart contracts, so that the results of vehicle condition analysis are isolated from private data and enhance the understanding of vehicle data. The protection of security and privacy, to solve the security problem of system data sharing.

According to the computing power and storage capacity of Internet of things devices, the devices are divided into ordinary nodes and butler nodes. Ordinary nodes only participate in the broadcast of transactions. The butler node packages the blocks and is responsible for broadcasting and verifying transactions. A complete distributed ledger is saved on both the common node and the butler node. The system framework mainly includes smart contracts, blockchain networks, distributed ledger, and Internet of things equipment.

As shown in Fig. 3, When the data demand issues the data request transaction on the blockchain through the smart contract, the data owner listens to the transaction of the data demand on the blockchain network. If

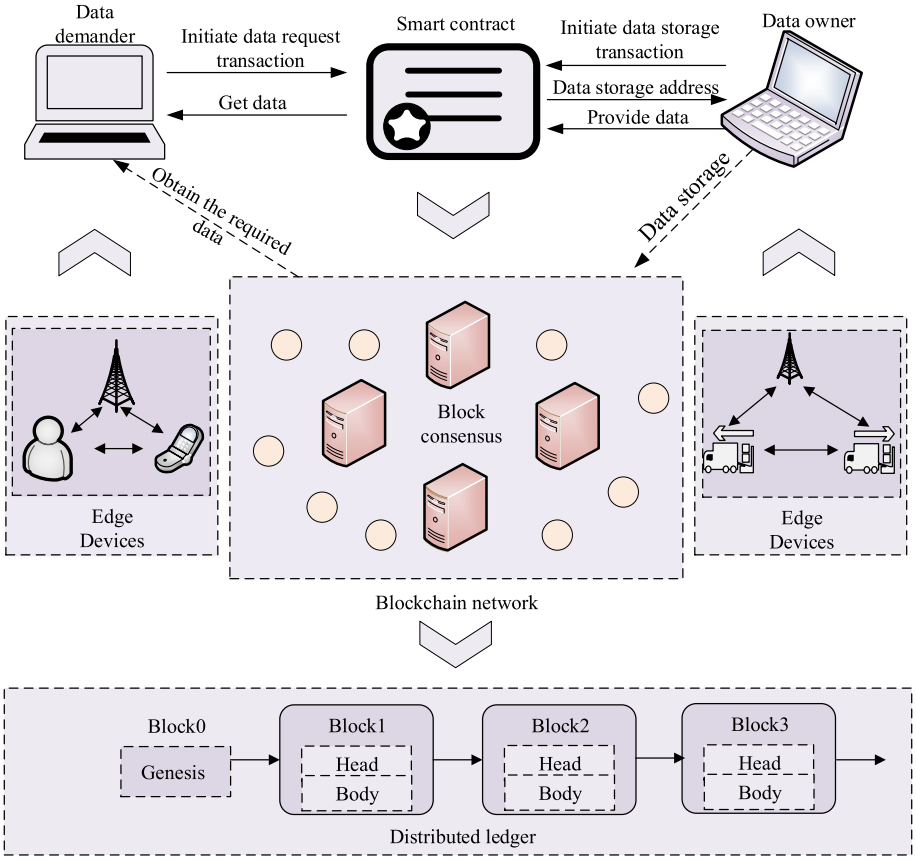

Fig. 3 Data sharing framework

there is the required data, the following operation: send the storage request to the consensus node through the smart contract. After obtaining the response of the consensus node, the raw data is sent to the consensus node, and the consensus node encrypts the data. The encrypted data, data description and storage time are uploaded to the edge devices for storage, and then the hash value and data summary of the shared data in the edge devices are sent to the blockchain. Realize shared data storage, address chain storage and data chain storage. After the data demand person obtains the data key from the data owner, he can obtain the required data from the corresponding data address. After the data demanders obtain the data, they use the data to better tap the potential value of the data.

Consensus mechanism for edge resource allocation

There is no same central database in the blockchain network as in traditional database systems. Each node is peer to peer, so a consensus mechanism must ensure that all peers can cooperate effectively. However, consensus mechanism and block publishing require multiple rounds of broadcasting throughout the network. In a dynamic environment, intermittent communication links of vehicles will increase the block chain operation delay. In addition, the traditional consensus mechanism relies on mining algorithms to ensure the fairness of blocks, which will lead to excessive computational overhead of the system as a whole. At the same time, due to the strong mobility of the vehicle itself, there is often a problem of data migration and synchronization across regions. If the traditional blockchain ledger transmission method is used, the operation efficiency will be significantly reduced. Therefore, we need to improve the traditional consensus mechanism for the above issues.

In the data sharing scenario of the IoV, there are a large number of decentralized and heterogeneous edge devices, which usually have considerable computing resources and are often idle. Therefore, each edge node can participate in the running process of the common knowledge mechanism by delegating its own idle resources to other nodes, while the elected nodes will actually participate in the block generation and blockchain maintenance process, To complete resource allocation and data sharing.

Therefore, in the design of this scheme, consensus mechanism based on virtual resource voting type is more appropriate, such as PoS and DPoS. Comparing the two consensus mechanisms represented by PoS and DPoS, we can find the direct voting method employed by PoS. In principle, PoS allows all nodes to compete. This process usually involves many nodes voting simultaneously. And the more nodes are participating, the less efficiently the consensus mechanism runs and the greater the network traffic pressure, which cannot meet the low latency requirements for real-time data processing.

The DPoS, based on inheriting that POS does not need to consume computing resources, greatly improves the operation efficiency. The voting method of its commission system is similar to the operation mode of the board of directors. Ordinary nodes are only responsible for electing "witness nodes", while the immediate consensus process is only carried out among the selected "witness nodes". Therefore, the block output speed is very fast. In this way, we can combine DPoS technology to solve the problem of nodes consuming a lot of arithmetic power to reach consensus and improve the efficiency of the consensus mechanism. However, due to the application characteristics of this scheme, we still need to make some adjustments to the existing DPoS, which is adapted to the use of this scheme. Aiming at the problems of malicious nodes and voting enthusiasm in the consensus process, this paper proposes an edge resource oriented DPoS mechanism (ERDPoS) based on the DPoS consensus mechanism. It improves the voting model, optimizes the reward and punishment mechanism, and solves the problems of untimely processing of malicious nodes and low voting enthusiasm of nodes in the DPoS algorithm. The participants in the Internet of vehicles can reach consensus efficiently and reduce the impact of malicious nodes on the consensus process.

Voting model calculation scheme

The generation of blocks is used to record specific transaction information and store it in the blockchain. The nodes in the system need to select qualified nodes to generate the blocks. Therefore, in order to ensure the security of the information, the node hopes to give the power to generate the blocks to those reliable and trusted nodes. Nodes are divided into normal nodes and butler nodes.

A) Ordinary nodes are composed of vehicles connected to the IoV and basic equipment on the side of the road, which is responsible for block distribution and transaction transmission and reception. They collect data on the surrounding vehicles and environment in real-time and send the messages after being signed. Normal nodes can see the entire consensus process and use the system's services. At the same time, ordinary nodes have voting rights, and they elect the butler node according to the success rate of the task within the specified time and refer to the integral of the node.
B) The butler node is responsible for generating and packaging the blocks while reviewing the content of the blocks. The butler node collects all kinds of

information sent by ordinary nodes from the Internet of vehicles and packages them into blocks. Subsequently, the butler node will sign it on its block by signing it. At the same time, each block generated on the IoV needs to be sent to the butler node. The butler node will make a corresponding judgment according to the authenticity of the information in the block. Blocks are only considered valid by more than half of the butler nodes, and effective blocks will be uploaded to the blockchain and be widely spread among producers. In addition, the butler node will also deal with the possible malicious attackers like double spend attack and sybil attack, and faulty nodes on the IoV in time.

This paper presents the concept of dedication point (DP). *DP* as a node evaluation index, which is used to evaluate the node credibility. The higher the contribution integral, the higher the work efficiency of the node, the more trustworthy; conversely, it means that the node cannot complete the task of generating blocks or auditing to some extent, and may be a malicious node. For highly efficient nodes, different *DP* will be rewarded according to their contribution to the Internet of Vehicles. For the fault node or the malicious node, if the packaging and audit operation cannot be completed within the specified time, the *DP* of the node will be deducted. Excluding *DP* would mean that it is more difficult for nodes to become packaged nodes in the next round, with less weight when voting for other nodes and no more rewards.

Voting mechanism

In the DPoS consensus algorithm, the node voting lacks fairness, and the node appears political apathy. In this scheme, the voting mechanism of the traditional DPoS consensus algorithm is improved, and certain rewards can be obtained for each vote. Specifically, after the end of each consensus process, a representative node of the successful production block has to distribute the reward to all the nodes in the corresponding proportion voting for it. When voting, the node votes support vote *SV*, and votes against negative vote *NV*, and chooses the top 15% of the nodes in the voting list to become the butler node. The scheme effectively reduces the probability of malicious nodes becoming representative nodes while increasing the voting enthusiasm of ordinary nodes.

The formula for the total votes of the nodes based on the contribution integral is as follows:

$$V_i = \left(\frac{\sum_1^m SV_{\mathrm{i}}}{m} - \frac{\sum_1^n NV_{\mathrm{i}}}{n} \right) + DP \tag{1}$$

In the Eq. 1, SV_i is the *DP* value that the *i*th node that voted *SV* has by itself; NV_i is the *DP* value that the *i*th node that voted *NV* has by itself; *m* is the number of *PV* votes obtained by the node; *n* is the number of *DP* votes obtained toward the node. When the V_i value is less than 0, the *score* value is counted as 0. In a round of voting, the V_i values obtained by the nodes are ranked from high to low, and the nodes located at the last 10% are defined as malicious nodes. This new calculation of voting results improves the fairness of elections and thus the system's security.

When an ordinary node is engaged in an election vote, it needs to collect feature information between the nodes through the block transmission process to judge whether a node can be trusted. This propagation is divided into two situations: 1) Direct propagation between nodes calculates its direct trust value by directly propagated information; 2) Other nodes obtain information from the node to calculate its indirect trust value. Direct propagation information is available based on historical records, but indirect propagation information needs to be obtained according to the recommendations of other nodes.

Direct trust

In this scheme, direct trust is a trust relationship established by the two parties to the transaction. Since trust is not caused by a single aspect but by multiple factors, there are different ways to assign weights when combining trust. In this model, the main factors affecting node trust are Node attributes, Network factors, and Safety factors. In this paper, the above factors are subdivided. Select the Computing Power of the factors affecting the node attribute in the blockchain, select the Delay of the factors affecting the network, and select the Bugged Probability. Some thresholds were selected according to the survey to rank these evaluation factors.

$$computing\ power = \begin{cases} 1,\ 0 < v \le 400k/s \\ 2,\ 400 < v \le 800k/s \\ 3,\ 800 < v \le 1000k/s, \end{cases}$$

$$Postpone = \begin{cases} 1,\ 65 < t \le 100 \\ 2,\ 25 < t \le 65 \\ 3,\ 1 < t \le 25, \end{cases}$$

$$Bugged\ Probability = \begin{cases} 1,\ 0.20 < p \le 0.35 \\ 2,\ 0 < p \le 0.20 \end{cases}$$

In the block generation cycle, there is *N*th propagation between nodes, so *C*, *D*, and *Bp* of the butler nodes are rated during each propagation process. Rating is a way to

quantify each attribute after the nodes complete the task. According to the selection index, the calculation formula of direct trust is: $T_D = C/(P \times BP)$. The trust value of the butler nodes depends not only on the nodes that directly propagate but also on the recommendations from other nodes, by which more information can be collected.

Indirect trust

It is a reliable way to calculate the trust values based on the history of the nodes. Still, it is not reliable to rely solely on the direct propagation between the nodes to estimate the trust values of the target butler nodes. When the number of direct propagation between ordinary and butler nodes is small, it is not reliable to calculate the trust value of the butler nodes by only relying on the natural interaction history. Therefore, when the number of propagation between the nodes is very few, we should consider the recommendation situation of the other nodes to calculate the indirect trust value, which is obtained by the interaction between the other nodes and the validation nodes. For example, if node A wants to know the indirect trust of node D, Then TC and TB are obtained through the feedback of direct interaction between nodes B and C and node D. That is, the formula can be extended if multiple nodes interact with it: $T_S = \frac{1}{n}\sum_{i=1}^{n} T_i$

Comprehensive trust value calculation

The trust value calculation of verification nodes combines direct trust and indirect trust. Generally, nodes believe that direct trust is more reliable because it is safer and more reliable through themselves and butler nodes. This avoids the case of the wrong node gang making the malicious node high, so the direct trust weight is set to 0.7, the indirect trust weight is 0.3, and the expression of the comprehensive trust value is: $T_i = 0.7 \times T_D + 0.3 \times T_S$. After obtaining the comprehensive trust value of the nodes, the comprehensive trust values of all the nodes are updated and uploaded through the blockchain system. The voting nodes vote on the nodes according to the score of the credit value, which improves the security of the whole system.

Reward and punishment mechanism

The DPoS algorithm gives a certain reward (Ra) to nodes that successfully packaged blocks and ordinary nodes who elect these packaged nodes. These rewards can increase voting enthusiasm at ordinary nodes and avoid low turnout and unmanned voting problems. When an ordinary node successfully elects a node that can generate a block or reports a malicious node, the node will receive a corresponding reward based on the number of contribution points.

As the node DP increases, the higher the weight of the nodes occupied. In order to avoid the voting results due to the excessive accumulation of some nodes, the function of resetting the reputation value is added to the reward mechanism. Let α be the DP threshold, β be the DP maximum, and Ra_i be the reward received by the ith node that participates in voting or performs packing. Equation 2 takes the packaging node of a successfully packaged block as an example.

$$Ra_i = \begin{cases} SV_i/(\sum_1^m SV_i + DP)Ra, & (DP \le \alpha) \\ SV_i/(\sum_1^m SV_i + DP) \cdot (DP - \alpha)Ra/DP, & (\alpha < DP < \beta) \end{cases} \tag{2}$$

SV_i is the DP value that the ith node that voted SV has by itself; NV_i is the DP value that the ith node that voted NV has by itself; α is the DP threshold and β is the DP maximum, When the node DP reaches the maximum value β, the node DP value will be reset to the threshold value α. Even if the obtained node keeps priority in the election of the steward node, it also maintains the fairness of the elected nodes in the network.

In a round of voting, a node can only cast a negative vote and a positive vote once. If the ordinary node votes in favor of the failed node or malicious node, or votes against the normal node, the node is considered as a malicious vote, and the node will be deducted some DP. When the steward node fails to pack the block successfully, the node will be deducted the credit score and removed from the steward node. Set η as penalty coefficient, DU is the DP value deducted when the node is punished. θ Is the minimum value of DP. When DP is deducted to θ When below, DP value will not change. Take throwing SV to malicious nodes as an example, as shown in Eq. 3.

$$DU = \begin{cases} SV_i/\sum_1^m SV_i \times \eta \times Ra, & DP > \theta \\ 0, & DP \le \theta \end{cases} \tag{3}$$

Compared with DPOS consensus mechanism, this paper mainly improves the selection of node production blocks with high recognition in the stage of selecting block producers to ensure that the selected producers are more reliable; According to the behavior of nodes, malicious nodes are handled in a timely manner to further ensure that the selected nodes have a high degree of trust. Taking VC chain as an example, the working process of improving DPOS is shown below.

Input: Vehicle data
Output: vb
The score sequence is calculated from Equation (1)
Sort score values in descending order
Top 15% of nodes make up the butler queue
while $i < butlerqueue.length()$ **do**
if Node i failed to pack **then**
$Ra_i, DU\ calculated\ from\ Equation(2)(3)$
$DP = DP - DU$
$SV_i = SV_i - DU$
$NV_i = NV_i + Ra_i$
Remove malicious nodes from the butler queue
$i \leftarrow i + 1$
else {Node i packaged successfully}
$Ra_i, DUcalculatedfromEquation(2)(3)$
$DP = DP + Ra$
$SV_i = SV_i + Ra$
$NV_i = NV_i - DU$
$Return\ vb$
end if
end while

Algorithm 1 Improve dpos working mechanism of VBExperimental analysis

In order to verify whether the proposed scheme can improve the enthusiasm of node voting and effectively handle malicious nodes to reduce the weight proportion of malicious nodes, the improved consensus algorithm is simulated and analyzed through simulation experiments. The experiment simulated 100 independent nodes, where the malicious node ratio was set to 15%, α is 100, β is 120, and θ is 10. A total of 150 rounds of experiments were carried out.

Comparison of the participating voting nodes before and after the mechanism improvement

The proportion of the number of nodes participating in the voting is taken as the active degree of the nodes participating in the voting to judge the enthusiasm of the nodes in the scheme. The initial probability of the experimental setting nodes participating in the voting is 50%. Compare ERDPoS with the original DPoS mechanism, At the same time, it is compared with the reputation based improvement DPoS (RDPoS) in the literature cite 9513042. And the results of 10 rounds of voting are randomly taken to get the change map of the number of the nodes participating in the voting, as shown in Fig. 4.

As can be seen from Fig. 4, under the original DPoS mechanism, The total number of people voting accounted for 50% - 60%. In the ERDPoS mechanism scheme, because the incentive mechanism stipulates that the nodes participating in the voting can get the corresponding reward, the more the votes, the more revenue, so more and more nodes participate in the voting mechanism, accounting for 60%-85% of the total nodes. At the same time, compared with the scheme in literature [43], our scheme performs better in terms of node participation. Therefore, the improved DPoS mechanism plays a good effect in improving the low voting enthusiasm of nodes and reducing malicious node attacks. It attracts more and more nodes to participate in the voting, improves the overall resistance of the model, and makes efficient use of the system resources.

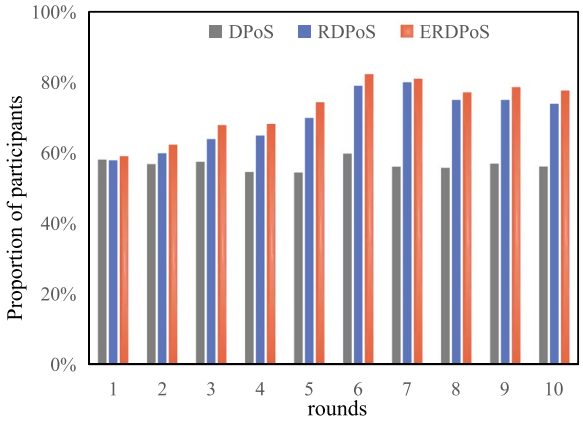

Fig. 4 Proportion of nodes participating in voting

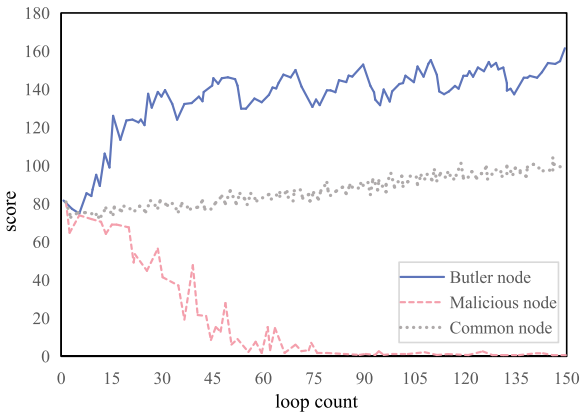

Fig. 5 150 rounds of voting results

Comparison of different types of nodes in multiple rounds of voting

To verify whether this scheme can effectively eliminate malicious nodes and reduce the proportion of malicious nodes. At the same time, verify whether the contribution points obtained by ordinary nodes increase gradually when they actively participate in the voting process. We judge the efficiency of the scheme to eliminate malicious nodes based on the decline rate of votes obtained by malicious nodes. This paper compares the trend of votes received by butler, ordinary and malicious nodes in 150 rounds of voting, as shown in Fig. 5.

According to the analysis of the broken line comparison chart, the number of votes obtained will increase significantly after the butler node successfully packs the blocks and gradually accumulates contribution points. This means that the steward node's performance is in a good and stable state, which makes other nodes more inclined to vote for it to obtain rewards. The general nodes show a butler upward trend. With the gradual increase of contribution points, the general nodes also have the opportunity to join the butler queue. The number of votes obtained by malicious nodes is similar to that of ordinary nodes at the beginning, but errors or no blocks are generated in the process of block generation. Therefore, under the mediation of the punishment mechanism, with the increase of the number of rounds, the contribution points quickly decreased around the 15th round. Other nodes vote against malicious nodes to obtain rewards, effectively preventing malicious nodes from entering the butler queue. The experimental results show that the improved DPoS mechanism can rapidly reduce the probability of malicious nodes becoming butler nodes. Thus, the safety and stability of the system are improved.

Comparison of time consumption of consensus algorithm before and after improvement

Time consumption is one of the more important reference indicators in the blockchain system based on the Internet of Vehicles. Low time consumption means that the waiting time for the vehicle to complete a data service is short, but the security cannot be guaranteed. High time consumption means that the trust relationship between nodes needs to be confirmed in each round, so the scheme has high reliability. In the consensus delay experiment, the experimental control group is the traditional consensus algorithm. In order to verify that the ERDPoS consensus algorithm has higher security than the traditional DPoS, the running time of the two consensus algorithms is simulated when the number of network nodes is 10, and repeated experiments are carried out for many times, taking 10 of them as the simulation results, as shown in Fig. 6.

It can be seen from Fig. 6 that the improved dpos consensus algorithm consumes more time than the dpos consensus mechanism because it needs to confirm the trust relationship between nodes and calculate the node DP in each round. The purpose of the computing node DP is to obtain a trusted node with a high degree of trust and avoid a malicious node becoming a steward node. Therefore, the improved consensus algorithm is more secure than the traditional DPoS.

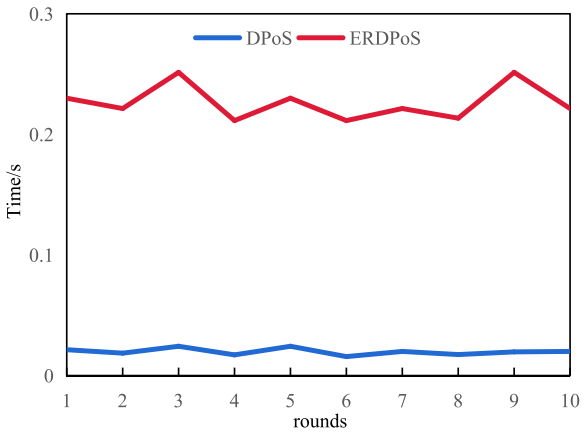

Fig. 6 Time consumption comparison

This paper scheme compared with other existing DPOS scheme

This paper compares with other models regarding consensus mechanism, security, and efficiency, as shown in Table 2. The data sharing model adopts the dual chain structure based on the alliance chain to reduce the pressure of the main chain. At the same time, the dual encryption is used to protect the privacy of the original data, which realizes the efficient and safe data security sharing. In addition, this paper analyzes the problems faced by IoV regarding privacy security, data storage, work efficiency, and the advantages of this Table 3. When faced with the problem of large-scale storage, the data sharing model of IoV based on the hybrid architecture of blockchain and cloud edge computing realizes the storage and convenient access of large-scale data, improves the utilization of edge devices, and solves the problem of small block capacity in blockchain based models. Double chain improves the packaging efficiency of blocks, and the improved consensus algorithm effectively reduces resource waste in the process of data transmission and block packaging. The scheme in this paper still needs to be improved. In future work, the model will be further improved to improve work efficiency and improve consensus algorithm.

Conclusions

As the IoV advanced, the combination of blockchain and cloud edge computing has increased significantly. There are many data interaction scenarios in IoV. These data weigh important value in scientific research, business, and traffic governance, hence how to share data efficiently and securely in IoV has caught increasing amout of attention. In this paper, we anaylze the problems in existing IoV, and propose a decentralized, efficient, and

Table 2 Comparison of improved DPoS with other schemes

	Consensus mechanism	Security	Efficiency
This paper	ERDPoS	Improved on DPoS to increase node activity, eliminate malicious nodes, and ensure system security	efficient
Zhang et al.	PoW, PoS	It plays a good role in limiting malicious vehicles and has high security	Time extension, Low efficiency
Tan et al.	BFT-PoS	The privacy protection of data is not perfect	While ensuring low delay and high efficiency, expand the scope of vehicle remote resource sharing

Table 3 Current problems and solutions for improved scheme

Type	Problems	Solutions for Improved Scheme
Privacy Security	Tamperable, Data Leakage, Hacker Attack	The underlying architecture based on blockchain is adopted to ensure data security by taking advantage of the decentralized and non tampering characteristics of blockchain; The malicious nodes are effectively filtered
Data Storage	Accessibility, Large scale data storage, Small block capacity	The data is stored in edge devices, which realizes the storage and convenient access of large-scale data
Efficiency	Delay, Waste computing resources	Adopt double chain structure to improve work efficiency; Reduced resource waste compared to pow

storage space-rich IoV hybrid architecture data sharing model. It enhances the protection of vehicle data security and privacy, and solves the problem of safe storage and sharing of system data. In addition, we have made some improvements to the existing DPoS consensus protocol to solve the problems in the DPoS algorithm, such as untimely processing of malicious nodes and low enthusiasm of nodes to vote. It enables participants in the Internet of Vehicles to reach consensus efficiently and reduces the impact of malicious nodes on the consensus process. It can better meet various practical needs of IoV. Later, we will add identity authentication and access control management to the model to further improve the security of the model. At the same time, the consensus algorithm is further optimized. In this paper, we hope to provide new research ideas for the coming integraton of blockchain and IoV, and seek a broader application area of consensus mechanism.

Acknowledgements
The authors would like to thank the anonymous reviewers for their insightful comments and suggestions on improving this paper.

Authors' contributions
Conceptualization, Experimental analysis, Data collation, Writing-original draft, Writing-review & editing, Software. Junhua Wu Conceptualization, Experimental analysis, Data collation, Writing-original draft, Resources, Supervision, Writing-review & editing, Software. Guangshun Li Writing-original draft, Writing-review & editing, Software, Validation. All authors reviewed the manuscript.

Funding
This work is supported by the National Natural Science Foundation of China Grants 61832012, and 61771289; Major Basic Research of Natural Science Foundation of Shandong Province with Grants ZR2019ZD10; Key Research and Development Program of Shandong Province with Grants 2019GGX101050; National Natural Science Foundation of Shandong Province Grants ZR2022MF304.

Availability of data and materials
Due to the nature of this research, participants of this study did not agree for their data to be shared publicly, so supporting data is not available.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Received: 19 September 2022 Accepted: 25 June 2023
Published online: 05 July 2023

References

1. Chen Y, Zhao J, Wu Y, Huang J, Shen XS (2022) QoE-Aware Decentralized Task Offloading and Resource Allocation for End-Edge-Cloud Systems: A Game-Theoretical Approach. IEEE Transactions on Mobile Computing
2. Mao Y, Zhang J, Letaief KB (2016) Dynamic computation offloading for mobile-edge computing with energy harvesting devices. IEEE J Sel Areas Commun 34(12):3590–3605. https://doi.org/10.1109/JSAC.2016.2611964
3. Sandhu AK (2022) Big data with cloud computing: Discussions and challenges. Big Data Min Analytics 5(1):32–40. https://doi.org/10.26599/BDMA.2021.9020016
4. Huang J, Wan J, Lv B, Ye Q, Chen Y (2023) Joint Computation Offloading and Resource Allocation for Edge-Cloud Collaboration in Internet

of Vehicles via Deep Reinforcement Learning. IEEE Systems Journal 17(2):2500–11. https://doi.org/10.1109/JSYST.2023.3249217
5. Chen Y, Hu J, Zhao J, Min G (2023) QoS-Aware Computation Offloading in LEO Satellite Edge Computing for IoT: A Game-Theoretical Approach. Chin J Electron
6. Tan X, Zhang J, Zhang Y, Qin Z, Ding Y, Wang X (2021) A puf-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Sci Technol 26(1):36–47. https://doi.org/10.26599/TST.2019.9010048
7. Cheng J, Yuan G, Zhou M, Gao S, Liu C, Duan H, Zeng Q (2020) Accessibility analysis and modeling for iov in an urban scene. IEEE Trans Veh Technol 69(4):4246–4256. https://doi.org/10.1109/TVT.2020.2970553
8. Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y (2020) Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans Veh Technol 69(4):4298–4311. https://doi.org/10.1109/TVT.2020.2973651
9. Wang J, Huang J, Kong L, Chen G, Zhou D, Rodrigues JJC (2021) A privacy-preserving vehicular data sharing framework atop multi-sharding blockchain. In: 2021 IEEE Global Communications Conference (GLOBECOM). pp 1–6. https://doi.org/10.1109/GLOBECOM46510.2021.9685366
10. Qi L, Hu C, Zhang X, Khosravi MR, Wang T (2020) Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment. IEEE Trans Ind Inf 17(6):1–1
11. Chen W, Chen Y, Chen X, Zheng Z (2020) Toward secure data sharing for the iov: A quality-driven incentive mechanism with on-chain and off-chain guarantees. IEEE Internet Things J 7(3):1625–1640. https://doi.org/10.1109/JIOT.2019.2946611
12. Rehman M, Javaid N, Awais M, Imran M, Naseer N (2019) Cloud based secure service providing for iots using blockchain. In: 2019 IEEE GLOBECOM. pp 1–7. https://doi.org/10.1109/GLOBECOM38437.2019.9013413
13. Xu S, Chen X, He Y (2021) Evchain: An anonymous blockchain-based system for charging-connected electric vehicles. Tsinghua Sci Technol 26(6):845–856. https://doi.org/10.26599/TST.2020.9010043
14. Kang J, Yu R, Huang X, Wu M, Maharjan S, Xie S, Zhang Y (2019) Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J 6(3):4660–4670. https://doi.org/10.1109/JIOT.2018.2875542
15. Ma Z, Wang L, Zhao W (2021) Blockchain-driven trusted data sharing with privacy protection in iot sensor network. IEEE Sensors J 21(22):25472–25479. https://doi.org/10.1109/JSEN.2020.3046752
16. Wang H, Fan K, Zhang K, Wang Z, Li H, Yang Y (2022) Encrypted data retrieval and sharing scheme in space-air-ground integrated vehicular networks. IEEE Internet Things J 9(8):5957–5970. https://doi.org/10.1109/JIOT.2021.3062626
17. Sharma S, Ghanshala KK, Mohan S (2019) Blockchain-based internet of vehicles (iov): An efficient secure ad hoc vehicular networking architecture. In: 2019 IEEE 5GWF. pp 452–457. https://doi.org/10.1109/5GWF.2019.8911664
18. Wang Z, Zhang F, Yu Q, Qin T (2021) Blockchain-envisioned unmanned aerial vehicle communications in space-air-ground integrated network: A review. Intell Converged Netw 2(4):277–294. https://doi.org/10.23919/ICN.2021.0018
19. Li F, Yu X, Ge R, Wang Y, Cui Y, Zhou H (2022) Bcse: Blockchain-based trusted service evaluation model over big data. Big Data Min Analytics 5(1):1–14. https://doi.org/10.26599/BDMA.2020.9020028
20. Ren J, Li J, Liu H, Qin T (2022) Task offloading strategy with emergency handling and blockchain security in sdn-empowered and fog-assisted healthcare iot. Tsinghua Sci Technol 27(4):760–776. https://doi.org/10.26599/TST.2021.9010046
21. Arun M, Balamurali S, Rawal BS, Duan Q, Kumar R, Balamurugan B (2020) Mutual authentication and authorized data access between fog and user based on blockchain technology. In: IEEE INFOCOM. pp 37–42. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162915
22. Wang Y, Wang Z, Zhao M, Han X, Zhou H, Wang X, Voundi Koe AS (2022) Bsm-ether: Bribery selfish mining in blockchain-based healthcare systems. Inf Sci 601. https://doi.org/10.1016/j.ins.2022.04.008
23. Guo J, Wang Y, An H, Liu M, Zhang Y, Li C (2022) Iidqn: An incentive improved dqn algorithm in ebsn recommender system. Secur Commun Netw 2022:1–12. https://doi.org/10.1155/2022/7502248
24. Liu G, Wu J, Wang T (2021) Blockchain-enabled fog resource access and granting. Intell Converged Netw 2(2):108–114. https://doi.org/10.23919/ICN.2021.0009
25. Lee S, Kim M, Lee J, Hsu RH, Quek TQS (2021) Is blockchain suitable for data freshness? An age-of-information perspective. IEEE Netw 35(2):96–103. https://doi.org/10.1109/MNET.011.2000044
26. Yang Q, Wang H (2021) Blockchain-empowered socially optimal transactive energy system: Framework and implementation. IEEE Trans Ind Inform 17(5):3122–3132. https://doi.org/10.1109/TII.2020.3027577
27. Yin Y, Li Y, Ye B, Liang T, Li Y (2021) A blockchain-based incremental update supported data storage system for intelligent vehicles. IEEE Trans Veh Technol 70(5):4880–4893. https://doi.org/10.1109/TVT.2021.3068990
28. Gao Y, Chen Y, Lin H, Rodrigues JJPC (2020) Blockchain based secure iot data sharing framework for sdn-enabled smart communities. In: IEEE INFOCOM. pp 514–519. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162725
29. Zhang W, Chen X, Jiang J (2021) A multi-objective optimization method of initial virtual machine fault-tolerant placement for star topological data centers of cloud systems. Tsinghua Sci Technol 26(1):95–111
30. Xu X, Shen B, Ding S, Srivastava G, Bilal M, Khosravi MR, Menon VG, Jan MA, Wang M (2022) Service offloading with deep q-network for digital twinning-empowered internet of vehicles in edge computing. IEEE Trans Ind Inform 18(2):1414–1423. https://doi.org/10.1109/TII.2020.3040180
31. Chen Y, Zhao J, Hu J, Wan S, Huang J (2023) Distributed Task Offloading and Resource Purchasing in NOMA-enabled Mobile Edge Computing: Hierarchical Game Theoretical Approaches. ACM Trans Embed Comput Syst. https://doi.org/10.1145/3597023
32. Ying C, Zhao J, Zhou X, Lianyong Q, Xiaolong X, Huang J (2023) A Distributed Game Theoretical Approach for Credibility-guaranteed Multimedia Data Offloading in MEC. Information Sciences 644:119306. https://doi.org/10.1016/j.ins.2023.119306
33. Xu X, Shen B, Yin X, Khosravi MR, Wu H, Qi L, Wan S (2021) Edge server quantification and placement for offloading social media services in industrial cognitive iov. IEEE Trans Ind Inform 17(4):2910–2918. https://doi.org/10.1109/TII.2020.2987994
34. Wang K, Yin H, Quan W, Min G (2018) Enabling collaborative edge computing for software defined vehicular networks. IEEE Netw 32(5):112–117. https://doi.org/10.1109/MNET.2018.1700364
35. Javaid U, Sikdar B (2021) A secure and scalable framework for blockchain based edge computation offloading in social internet of vehicles. IEEE Trans Veh Technol 70(5):4022–4036. https://doi.org/10.1109/TVT.2021.3060002
36. Wang Y, Zhang Y, Zhang X, Liang H, Li G, Wang X (2022) An intelligent forecast for covid-19 based on single and multiple features. Int J Intell Syst 37. https://doi.org/10.1002/int.22995
37. Lu Z, Liang H, Zhao M, Lv Q, Liang T, Wang Y (2022) Label-only membership inference attacks on machine unlearning without dependence of posteriors. Int J Intell Syst 37. https://doi.org/10.1002/int.23000
38. Li T, Chen Y, Wang Y, Wang Y, Zhao M, Zhu H, Tian Y, Yu X, Yang Y (2020) Rational protocols and attacks in blockchain system. Secur Commun Netw 2020:1–11. https://doi.org/10.1155/2020/8839047
39. Li T, Wang Z, Yang G, Cui Y, Chen Y, Yu X (2021) Semi-selfish mining based on hidden markov decision process. Int J Intell Syst 36(7):3596–3612. https://doi.org/10.1002/int.22428
40. Li T, Wang Z, Chen Y, Li C, Jia Y, Yang Y (2021) Is semi-selfish mining available without being detected? Int J Intell Syst https://doi.org/10.1002/int.22656
41. Zhu J, Deng H, Li X, Yuan Y, Wang F (2021) Blockchain-based consensus study on distributed control systems. In: 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI). pp 164–167. https://doi.org/10.1109/DTPI52967.2021.9540197
42. Huang D, Tang ZY, Hu WY, Wu QZ (2021) Blockchain-based electric vehicle charging reputation management mechanism. In: CAIBDA. pp 58–61. https://doi.org/10.1109/CAIBDA53561.2021.00020
43. Chen Y, Liu F (2021) Improvement of dpos consensus mechanism in collaborative governance of network public opinion. In: 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). pp 483–488. https://doi.org/10.1109/AEMCSE51986.2021.00105

44. Zhang H, Liu J, Zhao H, Wang P, Kato N (2021) Blockchain-based trust management for internet of vehicles. IEEE Trans Emerg Top Comput 9(3):1397–1409. https://doi.org/10.1109/TETC.2020.3033532
45. Tan C, Li X, Luan TH, Gu B, Qu Y, Gao L (2021) Digital twin based remote resource sharing in internet of vehicles using consortium blockchain. In: IEEE VTC. pp 1–6. https://doi.org/10.1109/VTC2021-Fall52928.2021.9625367
46. Chai H, Leng S, He J, Zhang K, Cheng B (2022) Cyberchain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles. IEEE Trans Veh Technol 71(5):4620–4631. https://doi.org/10.1109/TVT.2021.3132961
47. Li K, Hui L, Hou H, Li K, Chen Y (2017) Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In: IEEE HPCC/SmartCity/DSS. pp 466–473. https://doi.org/10.1109/HPCC-SmartCity-DSS.2017.61
48. Zhang L, Luo M, Li J, Au MH, Choo K, Chen T, Tian S (2019) Blockchain based secure data sharing system for internet of vehicles: A position paper. Veh Commun 16:85–93

Publisher's Note