EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

A survey: applications of blockchain in the Internet of Vehicles

Chao Wang, Xiaoman Cheng, Jitong Li, Yunhua He* and Ke Xiao

*Correspondence: heyunhua@ncut.edu.cn
School of Information Science and Technology, North China University of Technology, Beijing 100144, People's Republic of China

Abstract

Blockchain technology has completely changed the area of cryptocurrency with a Peer-to-Peer system named Bitcoin. It can provide a distributed, transparent and highly confidential database by recording immutable transactions. Currently, the technique has obtained great research interest on other areas, including the Internet of vehicles (IoVs). In order to solve some centralized problems and improve the architecture of the IoVs, the blockchain technology is utilized to build a decentralized and secure vehicular environment. In this survey, we aim to construct a comprehensive analysis on the applications of blockchain in the IoV. This paper starts with the introduction of the IoVs and the blockchain. Additionally, some existing surveys on the blockchain enabled IoVs are reviewed. Besides, the combination of the blockchain technology and the IoVs is analyzed from seven aspects to describe how the blockchain is implemented in the IoVs. Finally, the future research directions related to the integration are highlighted.

Keywords: Survey, Internet of Vehicles, Blockchain, Security

1 Introduction

In order to improve the performance of vehicular networks and overcome the limitations of intelligent transport systems (ITS), vehicular networks are coming into a new era, namely the Internet of vehicles (IoVs). The communication modes [1] in IoVs can be divided into two types, namely vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication, to provide convenient network service. In both communication modes, vehicles collect information with on-board units (OBUs) and follow the dedicated short-range communication (DSRC) or LTE-V protocols [2]. Relying on these communication modes, real-time data (such as traffic information and weather status) may help vehicles or traffic managers take actions in time (such as intelligent route planning and emergency message notification). V2V and V2I communications in traditional IoV architecture are depicted in Fig. 1. Unfortunately, there are still some challenges with applications under the IoV architecture. For example, in the process of information collection, malicious vehicles can easily publish false information, or tamper shared data, which leads to several security problems as shown in paper [3].

The blockchain [4], which acts as a popular distributed ledger, could be considered as a powerful solution to the challenges in the IoVs. It can provide credit support for

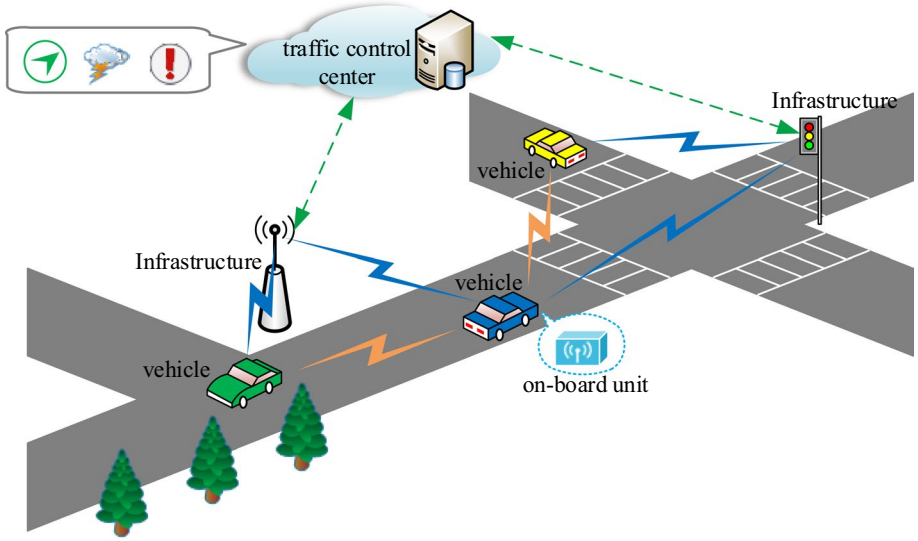

Fig. 1 Traditional structure of a vehicular network

the core information management in the IoVs at a low cost, which improves the IoV environment to a transparent, immutable and privacy preserving environment [5]. For example, the complete lifecycle information of vehicles, such as vehicle certificate, car insurance and other information, can be saved on the blockchain [6]. Moreover, the violation and car failure information, and auxiliary certificates for car dealers can also be stored on the blockchain. Specifically, the incentive mechanisms can be utilized within the blockchain to improve vehicles' cooperation, with the smart contract inside the blockchain to guarantee the executing process secure and efficient.

Some papers have done some researches on how to implement the blockchain technology to the IoTs or some related scenarios, such as [7–9]. However, some of them [7–9] focus on how the blockchain solves the challenges in IoTs. These papers do not point out how the blockchain technology could be used in the IoV scenarios.

On the contrast, some papers such as [10–12] focus much more on IoVs. Paper [10] concerns on managing trust in social IoVs (SIoVs). The main factors to build trust models for SIoVs and the brief overview of trending solutions (e.g., blockchain and fog computing) are also provided. Paper [11] gives an introduction on the IoVs and the blockchain. Comparisons of different blockchain technologies applied to the IoVs are conducted in detail. In paper [12], some application examples of blockchain applied to VANETs are presented. The main application scenarios are prevention of forged data, revocation of network certificate, vehicular authorization and transportation service. Besides the advantages of decentralization, transparency and immutability are also the characteristics that can be used in VANETs.

In conclusion, the integration of blockchain technology and the Internet of things (IoTs) has already been exploited by the previous work. However, these papers do not concern the applications of blockchains in the IoVs. Although some papers recently focus on the applications of blockchain in the IoVs, compared with these surveys, our

investigation focuses on the question that "Applications of Blockchains in the IoVs," and highlights several aspects on how to implement the blockchain in the IoVs. The main contributions of this survey are listed as follows:

- A brief background introduction about the IoVs and blockchain is presented.
- The ways of implementing the blockchain in the IoVs are compared from several aspects, such as security and privacy.
- The future research directions in the field of blockchain-enabled IoVs are pointed.

The organization of the survey is as follows. Section 2 gives a brief background introduction about the IoV and blockchain. Moreover, the features of blockchain and the designing principles of blockchain-based IoV architecture are presented. In Sect. 3, the integration of blockchain and IoVs are presented and discussed from several aspects, including architecture, privacy, security and data management. Some future directions of the blockchain used in the IoVs are analyzed in Sect. 4. Finally, Sect. 5 concludes this survey.

2 Background

2.1 Internet of Vehicles

The IoVs is similar to vehicular ad hoc network (VANET). However, the IoVs brings new technologies into vehicular networks and aims to overcome the limitations of VANETs. Paper [13] compares VANETs and IoVs from different aspects, highlighting the advantages of the IoVs in terms of design and development. To achieve real-time communication among vehicles, roadside units (RSUs) are also deployed. Then, the issues of traffic safety and efficiency can be addressed by VANETs at a lower cost. However, due to the commercialization limitations of VANETs devices, such as low reliability of Internet service, and incompatibility with devices, the IoVs appear and evolve. Compared to the VANET, the communication architecture of the IoVs includes not only RSUs, but also other complex and market-oriented communication devices. The IoVs focuses on many more intelligent communications among vehicles, roadside infrastructures, personal devices and sensors.

Another reason for evolution from the VANET to the IoVs mentioned by paper [14] is that the VANET cannot handle and evaluate the increasing data in the vehicular environment. Compared with the VANET, the IoVs can support traffic management services and vehicular safety services even in the country area. Thus, it is clear that the IoVs is a larger network than the VANET and the VANET can be regarded as a sub-network of the IoVs [15]. In this context, with the development of 5G, the performance of the IoV architecture is also improved through the integration of different technologies [16], such as software defined network (SDN), edge computing (EC) and network function virtualization (NFV).

However, although the evolution from the VANET to the IoV overcomes many limitations, the IoV is still vulnerable to cyberattacks from malicious entities. On the one hand, privacy and security issues of IoVs are still big challenges, such as security of data authentication, the privacy of vehicles, and the availability of resources [14, 17, 18]. On the other hand, the integration of different technologies in the IoV architecture is also of

challenge [17]. For example, in order to encourage vehicles to participate in the process of data sharing and resource scheduling, efficient incentive mechanisms [19] are essential in the vehicular system.

2.2 Blockchain

Blockchain as one of the most popular technologies is built upon a Peer-to-Peer system named Bitcoin [20]. All the network peers have the same copy of the blockchain data and each copy cannot be modified. What's more, the public key is used as the user's identity to provide anonymity and protect the user's privacy. Therefore, the blockchain could provide a decentralized, transparent, immutable, and secure data storage environment.

Block, as the basic data unit of blockchain, is generated with the cryptography technique and responsible for recording valid transaction information confirmed by each peer in the network. Figure 2 describes the structure of blocks. Generally, a block consists of a block header with metadata and a block body with transaction data. The block header contains three sets of metadata:

- Hash of the previous block.
- Timestamp, difficulty of mining, random number (Nonce).
- Merkle root.

In the consensus process, various consensus algorithms have been proposed [21], such as PoW (Proof of work), PoS (Proof of stake), DPOS (Delegated proof of stake), PBFT (Practical byzantine fault tolerance), Ripple, Tendermint, and Paxos. Some typical applications of different consensus mechanisms are listed in Table 1.

Initially, the Bitcoin system was just used to enable the exchange of cryptocurrencies and did not contain smart contracts. Smart contracts as a trusted digital contract are generated by Szabo [22]. The typical feature of smart contracts is that the rules are made in advance and are executed automatically. Recent platforms like Ethereum [23] and Hyperledger [24] have smart contract programmability, and people can deploy many different services, applications, or contracts on these platforms.

According to the network access control mechanism, blockchains can be divided into three types [25]:

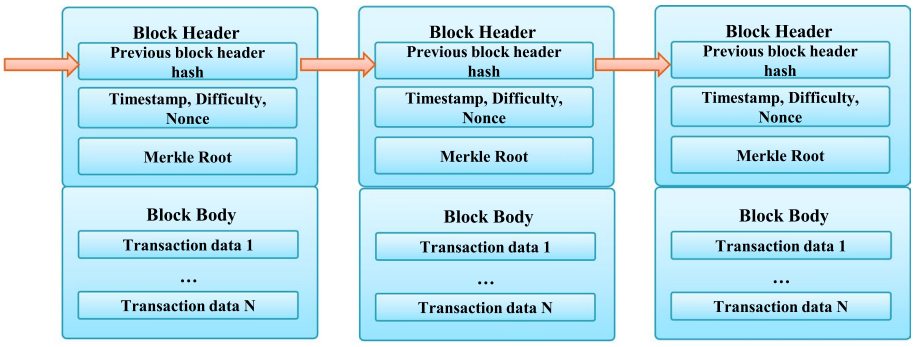

Fig. 2 Data structure of blocks

Table 1 Typical applications of consensus algorithms

Consensus algorithms	Applications
PoW	Bitcoin, Litecoin, Ethereum
PoS	PeerCoin, NXT, Ethereum
DPoS	BitShare
PBFT	Hyperledger Fabric
Ripple	Ripple
Tendermint	Tendermint
Paxos	Google Chubby, ZooKeeper

- *Public blockchain* Everyone can read and access the chain. In addition, everyone can send transactions and participate in the consensus process.
- *Private blockchain* Nodes will be limited and not every node can participate in the blockchain. The chain has strict management on access control.
- *Consortium blockchain* Some nodes that have authority in advance can be chosen to participate in the chain. Consortium blockchains can be seen as "partially decentralized."

Blockchain projects R3 Corda [26] and Hyperledger [24] are both considered as consortium blockchains. In general, the public blockchains are applicable for systems that require public participation and ensure maximum openness and transparency. The nodes are called miners to participate in the consensus process to obtain rewards. The data in a private blockchain is invisible and the speed of transaction is faster. What's more, the storage and exchange of information are safer.

There are several other classifications of the blockchain: permission blockchain [27] and hybrid blockchain [28]. Each node needs permission to join the blockchain system, which is called permission blockchain. The private blockchain and consortium blockchain belong to the permission blockchain. With the development of blockchain technology, the architecture of blockchain is no longer simply divided into public blockchain and private blockchain, so the concept of hybrid blockchain is proposed later.

Through the above analysis of the IoVs, to resolve the issues of security, privacy, cooperation and trust problems, more reliable and scalable mechanisms are needed. The following features of blockchain can make it an attractive technology to address issues in IoVs:

- *Decentralization* In a blockchain-based decentralized system, the rights and obligations of all nodes are equal. The operation of the system will not be affected even though a node stops working.
- *Transparency* There is no requirement to establish a trust relationship among nodes because the operation of the whole system is open and transparent. Within the rules in the system, nodes cannot cheat each other.
- *Collective maintenance* The system is maintained by all nodes with maintenance functions. Everyone in the system participates in the maintenance work.

- *Reliable database* All the network nodes have the same copy of the blockchain ledger. It is invalid to modify the database of a single node because the system will compare the data records on each node automatically.
- *Automation* With the help of smart contracts, the resource and data sharing services could be automatically executed without human intervention.

3 Integration of the blockchain and the IoVs

This section analyzes the combination of the blockchain and the IoVs from seven aspects, as shown in Table 2, which categorizes and illustrates various proposed scenarios in recent researches.

Table 2 Integration of the blockchain and the IoVs

Categories		Proposed	Implemented by
IoV security	Access control	[29]	BlockAPP
		[30]	Intelligent vehicle trust point (IVTP)
	Message validation	[31]	Trust clustering mechanism for VANET (TCMV)
		[32]	Distribute trust clustering mechanism for VANET (DTCMV)
		[33]	Blockchain-based traffic event validation (BTEV) framework
Trust management		[34]	Vehicular announcement protocol echo-announcement
		[35]	Anonymous cloaking region construction scheme
		[36]	Blockchain-based trust management with conditional privacy-preserving scheme (BTCPS)
Certificate management		[37]	Blockchain-based privacy preserving authentication (BPPA) scheme
		[38]	Decentralized key management mechanism (DB-KMM)
		[39]	A blockchain-based anonymous reputation system (BARS)
		[40]	Semicentralized traffic signal control (SCTSC) mode
Data management		[41]	Miner selection and block verification solutions
		[42]	Mobile crowd sensing (MCS) with blockchain
		[19]	A DQDA incentive mechanism
Data monetization		[43]	Blockchain-based data trading and loaning system
		[44]	Consortium blockchain-based data trading framework
		[45]	Consortium blockchain-based resource trading system
Privacy preserving		[46]	A hybrid blockchain-PermiDAG
		[47]	Blockchain-assisted privacy-preserving authentication system (BPAS)
Revised IoV architecture		[48]	Blockchain-based software-defined VANET (block-SDV) framework
		[49]	Blockchain-SDN-enabled architecture in 5G and fog computing systems

3.1 Blockchain-based IoV security

The centralized IoV model and its dependence on the third party trust authority lead to some security problems in the IoV. First, if the centralized authority failed, the overall system may not work properly which is a threat to the system availability. Besides, in order to keep the network secure, the traditional IoV model should have access control mechanisms and operations of message validation. In the following, we describe the combination of the IoV and blockchain from two aspects: access control and message validation.

3.1.1 Access control

Lots of vehicular information systems have appeared with the rapid development of the IoV. The quality of the transportation services is seriously affected by the availability of IoV. Paper [29] considers two main aspects of robustness, namely authentication and privacy preservation. The authentication and privacy preservation of vehicles can be achieved with blockchain, where a robust, decentralized and scalable architecture is proposed. The authenticity of authorized access is realized by uploading a valid transaction to the blockchain. There are four major entities, namely the registration server, service providers, blockchain and vehicles, and they form the proposed three-phase system, namely the registration phase, authentication phase and authorization phase. These steps work together with their own function to maintain the robustness of the proposed system. In the authentication phase, this paper uses the blockchain to ensure the security and privacy preservation of the system with the smart contract implemented in the Remix platform.

The blockchain technology is utilized in paper [30] to solve the authentication problem of communications in VANETs. In this paper, two blockchains are proposed, including a local dynamic blockchain and a main blockchain. Some summary information on vehicle movement and message transmitting is stored in the local blockchain. Once unusual events happened, these events would be stored on the main blockchain. However, based on the architecture, there are several problems. First, in VANETs, the amount of message traffic at the same time is too large so that it is hard to tackle all message authentications in real time. Besides, when message authentication is needed, the waiting time of any authentication cannot be too long. To solve the above problems, the authors split the local dynamic blockchain into multiple parallel blockchains, each of which is responsible for distinct regions or movement directions. To solve the problem of trust, the authors propose the concept of intelligent vehicle trust point (IVTP), which is used to evaluate the degree of trustiness of a vehicle. However, this paper does not detail too much about the IVTP distribution or how to earn the IVTP.

3.1.2 Message validation

Many applications can be implemented in ITSs with the maturity of communication technology, and more and more information is shared in ITSs, which affects road traffic, such as road status information. However, the forged message is a normal attack

that can be embedded in the vehicular environment. Therefore, a message verification mechanism should be proposed for shared messages.

Much literature has mentioned the idea of clustering. Vehicles are organized into different clusters and the cluster headers (CHs) are elected from clusters by clustering mechanism for VANET (CMV). Each CH, on behalf of all the other vehicles in the cluster, communicates with the other CHs. Paper [50] proposes a clustering mechanism with blockchain, which can save network resources by optimizing and selecting new CHs. Based on the reputation of vehicles, paper [31] utilizes trust clustering mechanism for VANET (TCMV) to achieve secure message exchanges by checking the message's credibility of CHs in vehicular networks. However, the message's credibility is not enough to fix whether an exchanged information is malicious. Thus, based on TCMV, the authors in paper [32] propose a blockchain-based distributed TCMV (DTCMV). The proposed DTCMV is composed of three steps, namely message transmission, block creation and block validation. The RSUs act as miners in DTCMV and are responsible for exchanging the data among RSUs, creating the block of messages, and storing messages.

Encouraged by the advantages of blockchains, a blockchain-based traffic event validation (BTEV) framework is proposed in the paper [33]. In BTEV, a two-pass threshold-based event validation mechanism can help validate an event, and the submission of transactions can be accelerated based on a two-phase consecutive transaction. Besides, a proof-of-event (PoE) consensus mechanism is introduced, which is proposed for achieving the reliability of event occurrence. Besides, the Merkle Patricia Trie (MPT) structure is introduced to BTEV to make RSUs submit the confirmed event to the blockchain more efficiently.

3.2 Trust management in IoVs

With the consideration of security, it is assumed that the third party authority can be trusted absolutely. However, the assumption cannot always be satisfied due to network instability or in-network attacks. Thus, a trust-less architecture is proposed to solve the above problems, where the trust value of each vehicle in the network is kept by other vehicles. Then, the behavior of each vehicle can be evaluated with the help of vehicle trust. The details of trust management are described in the following papers.

An effective announcement network—CreditCoin is proposed in the paper [34] to solve two main problems of message forwarding in the IoVs. In details, one is how to forward reliable announcements without exposing users' privacy; the other is how to motivate vehicle nodes to forward announcements. For the first problem, the vehicular announcement protocol Echo-Announcement is proposed, which can achieve efficiency and privacy-preserving while forwarding announcements. Then, a blockchain-based incentive mechanism is proposed for the second problem. Each user can manage its reputation points while earning or spending coins which act as the incentive.

Paper [35] focuses on the issue of location privacy leakage. This paper proposes a distributed management mechanism of location privacy protection based on the blockchain and the distributed k-anonymity [1] mechanism. First, based on the characteristics of different participants, the authors design a trust management method based on Dirichlet distribution. Then, the blockchain acts as a distributed database to record the trust

value in this mechanism, so that the initiating vehicles and the cooperating vehicles only cooperate with the vehicles they trust in the anonymous cloaking region.

Paper [36] targets to solve two issues in the network whether messages are reliable and whether the privacy of vehicles is protected. For the first question, a conditional privacy-preserving announcement protocol (BTCPS) for secure vehicular communication is proposed. In BTCPS, message aggregation can achieve authentication effectively and reduce the network overhead. The reliability of message announcements can be improved by the threshold number of vehicles. For the second issue, a blockchain-based trust management model is implemented which contains two parts—the updating algorithm of reputation and the distributed consensus algorithm. The reputation data are stored in the blocks and its value will be evaluated by the direct trust value and the indirect trust value. Conditional privacy, reliability and timeliness can be guaranteed with the method proposed in this paper.

3.3 Certificate management in IoVs

The certificate issued to each vehicle is the communication identity of each vehicle in the IoV. In the traditional IoVs, the work of certificate management is accomplished by the public key infrastructure (PKI), including certificate issuing and revoking. However, this architecture suffers from the single point failure problem, which will reduce the reliability of the network. The following papers solve this problem from several aspects.

Paper [37] offers blockchain-based privacy preserving authentication (BPPA) scheme for VANETs. Authors in this paper assume that the trusted authority (TA) is semi-trusted and will not maliciously track or reveal the linkage between the public key and the real identity of the target vehicle in case of dispute. In addition, semi-TAs are transparent and verifiable because all the certificates and transactions are recorded permanently and immutably in the blockchain. Finally, BPPA employs the Chronological Merkle Tree (CMT) and the Merkle Patricia Tree (MPT) to extend the conventional blockchain structure, which enhances efficiency and scalability.

To solve the certificate management problem, a decentralized key management mechanism (DB-KMM) is proposed in the paper [38], in which the lightweight authentication and the blockchain-based key agreement are integrated. DB-KMM is implemented with the blockchain and the smart contract. Based on the mechanism, some typical attacks such as resisting internal and external attacks, public key tampering, DoS attack and collusion attack can be defended.

Paper [39] presents a blockchain-based anonymous reputation system to solve three problems in VANETs, which are reputation management, certificate management and the privacy preservation between the certificate and the vehicle identity. In the blockchain-based anonymous reputation system, the authors propose three blockchains, including blockchain for messages, blockchain for certificates and blockchain for revoked public keys, to manage the process of certificate initialization, updating, revocation and authentication. Second, it presents a reputation evaluation algorithm to build the trust model in VANETs. This algorithm utilizes the reward mechanism to motivate honest and active nodes while utilizing the punishment mechanism to suppress misbehaviors such as distributing forged messages. Third, it uses the third party—law enforcement authority—to keep the privacy on vehicle identities. The third-party institute takes

place of some functions of the certificate authority and the certificate authority does not learn the linkage between the vehicle identity and its related certificate, which is controlled only by the law enforcement authority. However, some problems are not solved completely. First, all the messages transmitted in the network are recorded on the blockchain for messages, which will cost too much bandwidth. Especially in VANETs, messages are distributed frequently and not all the messages can be recorded in time on the blockchain. Second, the paper uses the third part—law enforcement authority to protect the certificate authority from exposing the vehicle identity. However, this way does not make too many differences from the original mechanism which uses the certificate authority only.

Authors in paper [40] construct the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) blockchain in Semi-centralized Traffic Signal Control (SCTSC) system to support vehicle access control to traffic data. The structure is described from three aspects. First, before starting communication, authentication centers (AC) and trace managers (TM) authenticate users' identities, and vehicles are divided into groups based on their attributes (such as dynamic position and direction). Second, vehicles reach a temporary signal control agreement by interacting with others without leaking privacy. Finally, after establishing communication, final decisions are verifiable to all users.

3.4 Data management in IoVs

Data management in the IoVs involves the management of on-chain data and off-chain data. On-chain data should notice two aspects namely storage and sharing of data, and off-chain data should be highlighted the query-processing and analysis of data. However, the exciting issues of traditional data management are that they cannot guarantee data integrity and trust when processing heterogeneous vehicle data.

A blockchain-based platform of data sharing records is proposed by paper [41] in the scenario of IoVs. There are two challenges that are proposed in this paper. One is how to add blocks to the blockchain by proper miners. The other is the design of incentive mechanisms. To solve the first problem, a reputation-based policy is proposed to select proper miners. The reputation of a candidate is calculated in two aspects: the historical interactions with other vehicles and recommended opinions from other vehicles. Both active miners and standby miners have a higher reputation value than other nodes. For the second problem, the contract theory is utilized to design an incentive mechanism. To protect from internal collusion, standby miners are motivated by incentive mechanisms to participate in the verification process.

To solve the problem of huge data collecting in scenarios such as IoVs, mobile crowd sensing (MCS) can be seen as a promising way. Many incentive mechanisms are proposed in different work, but most of them fail to consider the situation of an emergent sensing task in a vehicular network. A blockchain-based efficient collaboration and incentive mechanism for IoVs with security information exchange is proposed by paper [42]. For the general sensing task, the authors designed an incentive mechanism to encourage the vehicles to contribute to their targets. What's more, the authors proposed a blockchain-based framework to exchange data securely in the vehicular MCS network. Specifically, blockchain not only acts as an information exchange medium

between devices and the IoT center but also as a database to ensure the security of the framework.

To effectively manage the data of on-chain and off-chain, an auction incentive mechanism is proposed by paper [19]. This incentive mechanism is based on the quality of the consortium blockchain drive to ensure the data trust for both the on-chain and the off-chain data. For off-chain data, an expectation-maximization (EM) algorithm-based data quality estimation is presented by authors to evaluate the actual task data and the quality of data. Besides, the incentive mechanism is based on the data quality-driven auction (DQDA) model with blockchain to maximize welfare at a low cost. A consortium blockchain mechanism is adapted to address the security issue of on-chain data. Finally, the authors design a smart contract to share data and compute costs automatically. The process of filtering messages is described as a reverse auction in which the server acts as an auctioneer that purchases data from users.

3.5 Monetization of IoV data

Vehicle data can be divided into two categories: resource data and non-resource data. As a great important part of IoVs, the collected data from various vehicular devices are explosive increasing in recent years. To meet the requirements of protecting users' privacy and fast data exchange, the original cloud-based centralized system needs to be improved. Although blockchain-based data markets for IoVs could offer a relatively secure vehicular environment, some challenges are still present.

To address the efficiency challenges, the paper [43] proposes an auxiliary debit–credit mechanism for the blockchain-based IoV data trading system. In this system, the multi-interface-based stations as aggregators provide the service of high-speed communication and ledge storage for vehicles. What's more, the authors apply a consortium blockchain to provide secure P2P data trading and loan services. Based on the five-layer heritage structure, the authors establish a two-stage Stackelberg game model to solve the pricing problem in the process.

To solve the problems in the paper [44], a consortium blockchain-based P2P data trading system is proposed. Edge servers as brokers are introduced to manage the process of data trading and exchange in the framework. The transaction verification is performed by the local aggregator as the authorization node to collect the data transaction information instead of relying on the trusted third party. In the process of transaction, the authors propose a budget balanced double auction to achieve the desired economic benefits and protect the privacy of buyers and sellers.

Vehicles can act as transporters of resources in IoVs. As presented in paper [45], the authors propose an on-demand P2P data trading system based on consortium blockchain to achieve flexible computing resource allocation. What's more, to encourage users to participate in the system, this paper constructs a two-stage Stackelberg game for the interaction between the computing resource buyers and sellers. In the first stage, computing resource buyers set the discriminatory pricing for renting resources to do computing tasks within a unit time. In the second stage, the sellers decide the volume of resource transactions and then send it to the resource buyer. In addition, the optimal computing resource pricing and trading strategies with the Stackelberg game are presented.

3.6 Privacy preserving through blockchain in IoVs

With the development of intelligent transport systems (ITS), more and more vehicle information is generated. For example, the camera data [51] can record vehicle accidents and improve the driving experience. However, the availability and privacy preservation of this information are conflicted with each other in vehicular communication. Thus, privacy preservation through blockchain in IoVs needs to be considered.

Authors in this paper [46] propose a novel hybrid blockchain named PermiDAG to relieve the transmission load of entities and improve data security in the vehicular environment. The two main components of PermiDAG are permissioned blockchain and the local directed acyclic graph (DAG). As an efficient consensus protocol, delegated proof of stake (DPoS) is adopted in PermiDAG, with the reputation of vehicles considered. To learn models from edge information, an asynchronous federated learning scheme is proposed by authors. What's more, the authors utilize deep reinforcement learning (DRL) to select the node which can minimize the execution time and maximize the accuracy of the aggregated model. Finally, the reliability of shared data is guaranteed by integrating learned models into blockchain and executing a two-stage verification.

In the context of the traditional centralized IoV, which highly depends on the service center, message transmission will encounter many privacy problems. With the goal of ensuring the accuracy and reliability of the transmitted messages, a new authentication framework is proposed named blockchain-assisted privacy-preserving authentication system (BPAS) [47]. On the one hand, even though there is no centralized third party, BPAS guarantees that the transmission information is reliable with automatic authentication. On the other hand, BPAS integrates blockchain features and cryptogram primitives together, which enable BPAS to effectively deploy privacy preserving authentication even when the trusted party is offline.

The privacy preserving problem is also concerned by papers [34, 37, 39]. In these papers, privacy preserving is not the main purpose, but an important condition for other targets. Although privacy-preserving is not the main point, an important condition for other targets. Different methods are adopted to protect the privacy of network entities. Paper [37] assumes that the TA is semi-trusted (Semi-TA) and will not maliciously track or reveal the real identity of the vehicle in case of dispute. The TA named law enforcement authority (LEA) in paper [39] has to keep the privacy on vehicle identities.

3.7 Blockchain-based revised IoV architecture

As shown in Sect. 2.1, the performance of IoVs could be improved by integrating different technologies, such as SDN, EC, AI and so on. In addition, as a distributed technology, blockchain could improve security effectively due to its transparency and immutability. That is why some applications are classified as "Blockchain-based Revised IoV Architecture" in this subsection.

Paper [48] proposes a permissioned blockchain enabled software-defined framework named block-SDV for VANETs. The consensus mechanism named Redundant Byzantine fault tolerance (RBFT) is proposed by authors to ensure all the consensus nodes perform relevant operations correctly which include executing and writing transactions. A joint optimization problem is modeled as a Markov decision process with three functions which are state space, action space and reward functions.

To manage and control the vehicular network efficiently and effectively, in the case of ensuring the security of the standardized vehicular communication architecture, paper [49] proposes a blockchain-SDN-enabled system for IoVs in fog computing and fifth-generation (5G) communication networks. As sharing management, blockchain and SDN are incorporated into IoVs. On the one hand, the need for trust among the connected peers is satisfied by blockchain. On the other hand, effective network management and the control process are guaranteed by SDN. What's more, the handover problems of SDN when lots of vehicles are connected to the RSUs are addressed by fog computing. To enhance network performance, low-latency communication services are applied by 5G. Finally, the authors introduce the network trust model that can curb malicious activities to determine whether the information provided by peers in-network is trustworthy enough.

4 Future direction

As shown in the previous section, different applications of blockchain in the IoV have been designed and discussed. The major benefit of these integrations is that they could contribute to improve the vehicular network environment. Nevertheless, future research directions in this field should be highlighted.

4.1 Trust of off-chain data

Although blockchain technology has been applied to IoVs to address trust challenges and security issues, ensuring trust in off-chain data for the blockchain-based approaches is still an open issue. What's more, with the increasing demand for privacy and security of IoVs, the quality of off-chain data has attracted more attention. For example, in the paper [19], the authors proposed a DQDA-based incentive mechanism that guarantees trust in both on-chain data and off-chain data. Thus, to guarantee the security and privacy of the data on the chain, the security of the data quality under the chain needs more attention.

4.2 Resource management

In the blockchain-based IoV, the number of transactions on each node is very high, which has a big impact on energy resource consumption and the transmission or storage of data. In addition, the current consensus mechanisms also have the issue of resource waste. For example, PoW relies on physical machines to perform lots of mathematical operations to obtain the right number. Although PoS and DPoS can reduce the resource consumption caused by mathematical operations, they have the problem of weak supervision and poor security. Finally, considerable overheads may be caused because of the operations of the public key. Therefore, the design of blockchain-based lightweight frameworks and lightweight cryptography algorithms like [52, 53] is necessary.

4.3 Evaluation criteria

As shown in the previous section, most of the proposed architectures and algorithms are based on independent simulation and evaluation, and there is no comparative experiment as a benchmark to better illustrate the advantage of these solutions. From another perspective, the availability of these solutions has not been evaluated. Thus, the criteria of different evaluations could be interesting research directions in IoVs.

4.4 Integration of future architectures

Inspired by paper [16], the integration in the vehicular architecture of different technologies (SDN, 5G and NFV) has many challenges. One of the major challenges related to this integration is the design of the security and privacy plane. As a distributed ledger, blockchain could be used to improve security as its transparency and immutability. What's more, many papers are in the proposal stage and many issues have to be solved. For example, the architecture of paper [49] is a hybrid framework that applies many different technologies (SDN, 5G and Fog Computing). Authors in this paper apply blockchain technology to manage framework securely. Therefore, it is a worthy research direction to apply blockchain technology into a hybrid vehicular framework.

5 Conclusion

In the future vision of the IoVs, every vehicle will be connected to the Internet, and blockchain is expected to provide credit support for the core information of vehicles at a low cost. Blockchain technology is an effective distributed ledger to overcome the problem that the centralized IoV architecture is suffering. Although different surveys have already explored the integration of blockchain technology with IoVs, there are still many aspects of these applications that have not been considered. Thus, based on the introduction of the fundamental principles of the IoV and blockchain, we provide an extensive discussion and comparison of the existing surveys about applications of blockchain, with a specific focus on the integration of the blockchain technology with the IoV. Then, various proposed scenarios in recent researches from seven aspects, including blockchain-based IoV security, trust management, certificate management, privacy-preserving in IoV, are categorized and illustrated. Based on this survey, several open issues and future research directions are proposed to yield major problems in the IoV in the near future.

Abbreviations

IoVs: Internet of vehicles; ITS: Intelligent transport systems; OBUs: On-board units; VANET: Vehicular ad hoc network; V2V: Vehicle-to-vehicle; V2I: Vehicle-to-infrastructure; V2P: Vehicle-to-personal devices; V2S: Vehicle-to-sensors; SDN: Software defined networking; PoW: Proof of work; PoS: Proof of stake; DPOS: Delegated proof of stake; PBFT: Practical byzantine fault tolerance.

Acknowledgements

This work is supported in part by the National Natural Science Foundation of China under Grant 61802004 and Grant 61802005, and the Scientific Research Project of Beijing Educational Committee under Grant KM202010009008.

Author's contributions

All authors were involved in the discussion of the work described in this paper. All authors read and approved the final manuscript.

Funding

This work is supported in part by the National Natural Science Foundation of China under Grant 61802004 and Grant 61802005, and the Scientific Research Project of Beijing Educational Committee under Grant KM202010009008.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 4 October 2020 Accepted: 24 March 2021
Published online: 07 April 2021

References

1. J. Wang, Z. Cai, J. Yu, Achieving personalized *k*-anonymity-based content privacy for autonomous vehicles in cps. IEEE Trans. Ind. Inf. **16**(6), 4242–4251 (2020)
2. C. Wang, J. Li, Y. He, K. Xiao, H. Zhang, Destination prediction-based scheduling algorithms for message delivery in IoVs. IEEE Access **8**, 14965–14976 (2020)
3. Z. Cai, X. Zheng, J. Yu, A differential-private framework for urban traffic flows estimation via taxi companies. IEEE Trans. Ind. Inf. **15**(12), 6492–6499 (2019)
4. S. Zhu, Z. Cai, H. Hu, Y. Li, W. Li, zkCrowd: a hybrid blockchain-based crowdsourcing platform. IEEE Trans. Ind. Inf. **16**(6), 4196–4205 (2020)
5. Y. Pu, T. Xiang, C. Hu, A. Alrawais, H. Yan, An efficient blockchain-based privacy preserving scheme for vehicular social networks. Inf. Sci. **540**, 308–324 (2020). https://doi.org/10.1016/j.ins.2020.05.087
6. A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: a distributed solution to automotive security and privacy. IEEE Commun. Mag. **55**(12), 119–125 (2017)
7. A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and Solutions (2016). arXiv:1608.05187
8. M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet Things J. **6**(2), 2188–2204 (2019)
9. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1676–1717 (2019)
10. R. Iqbal, T.A. Butt, M. Afzaal, K. Salah, Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. Int. J. Distrib. Sens. Netw. **15**(1), 1550147719825820 (2019). https://doi.org/10.1177/1550147719825820
11. L. Mendiboure, M.A. Chalouf, F. Krief, Survey on blockchain-based applications in internet of vehicles. Comput. Electr. Eng. **84**, 106646 (2020). https://doi.org/10.1016/j.compeleceng.2020.106646
12. S. Majumder, A. Mathur, A. Javaid, A study on recent applications of blockchain technology in vehicular adhoc network (VANET) (2020), pp. 293–308
13. O. Kaiwartya, A.H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, X. Liu, Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects. IEEE Access **4**, 5356–5373 (2016)
14. J. Contreras-Castillo, S. Zeadally, J.A. Guerrero-Ibañez, Internet of vehicles: architecture, protocols, and security. IEEE Internet Things J. **5**(5), 3701–3709 (2017)
15. F. Yang, S. Wang, J. Li, Z. Liu, Q. Sun, An overview of internet of vehicles. China Commun. **11**(10), 1–15 (2014)
16. L. Mendiboure, M.A. Chalouf, F. Krief, Towards a 5g vehicular architecture, in *Communication Technologies for Vehicles*. ed. by B. Hilt, M. Berbineau, A. Vinel, M. Jonsson, A. Pirovano (Springer, Cham, 2019), pp. 3–15
17. S. Tanwar, J. Vora, S. Tyagi, N. Kumar, M.S. Obaidat, A systematic review on security issues in vehicular ad hoc network. Secur. Privacy **1**(5), 39 (2018). https://doi.org/10.1002/spy2.39
18. Y. Pu, C. Hu, S. Deng, A. Alrawais, Rpeds: a recoverable and revocable privacy-preserving edge data sharing scheme. IEEE Internet Things J. **1**, 8077–8079 (2020)
19. W. Chen, Y. Chen, X. Chen, Z. Zheng, 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 (2019)
20. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. Technical report, Manubot (2019)
21. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in *2017 IEEE International Congress on Big Data (BigData Congress)* (IEEE, 2017), pp. 557–564
22. N. Szabo, Formalizing and securing relationships on public networks. First Monday (1997)
23. G. Wood et al., Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. **151**(2014), 1–32 (2014)
24. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in *Proceedings of the Thirteenth EuroSys Conference* (2018), pp. 1–15
25. I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges. IJ Netw. Secur. **19**(5), 653–659 (2017)
26. M. Valenta, P. Sandner, Comparison of ethereum, hyperledger fabric and corda, no. June (2017), pp. 1–8
27. H. Sukhwani, J.M. Martínez, X. Chang, K.S. Trivedi, A. Rindos, Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric), in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)* (2017), pp. 253–255
28. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: securing a blockchain applied to smart contracts, in *2016 IEEE International Conference on Consumer Electronics (ICCE)* (2016), pp. 467–468
29. R. Sharma, S. Chakraborty, Blockapp: using blockchain for authentication and privacy preservation in IoV (2018), pp. 1–6
30. M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle. Comput. Netw. **145**, 219–231 (2018). https://doi.org/10.1016/j.comnet.2018.08.016
31. A. Kchaou, R. Abassi, S.G. El Fatmi, Towards a secured clustering mechanism for messages exchange in VANET, in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (2018), pp. 88–93
32. A. Kchaou, R. Abassi, S. Guemara, Toward a distributed trust management scheme for VANET, in *Proceedings of the 13th International Conference on Availability, Reliability and Security* (2018), pp. 1–6

33. Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, C.-C. Liu, Blockchain-based traffic event validation and trust verification for vanets. IEEE Access **7**, 30868–30877 (2019)
34. L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transp. Syst. **19**(7), 2204–2220 (2018)
35. B. Luo, X. Li, J. Weng, J. Guo, J. Ma, Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Trans. Veh. Technol. **69**(2), 2034–2048 (2020)
36. X. Liu, H. Huang, F. Xiao, Z. Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. IEEE Internet Things J. **7**(5), 4101–4112 (2020)
37. Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy-preserving authentication scheme for VANETs. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **27**(12), 2792–2801 (2019)
38. Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, W. He, An efficient decentralized key management mechanism for VANET with blockchain. IEEE Trans. Veh. Technol. (2020). https://doi.org/10.1109/TVT.2020.2972923
39. Z. Lu, W. Liu, Q. Wang, G. Qu, L. Zhenglin, A privacy-preserving trust model based on blockchain for vanets. IEEE Access **PP**, 1–1 (2018). https://doi.org/10.1109/ACCESS.2018.2864189
40. L. Cheng, J. Liu, G. Xu, Z. Zhang, W. Wang, Sctsc: a semicentralized traffic signal control mode with attribute-based blockchain in IoVs. IEEE Trans. Comput. Soc. Syst. **6**(6), 1373–1385 (2019)
41. J. Kang, Z. Xiong, D. Niyato, D. Ye, D.I. Kim, J. Zhao, Toward secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory. IEEE Trans. Veh. Technol. **68**(3), 2906–2920 (2019). https://doi.org/10.1109/TVT.2019.2894944
42. B. Yin, Y. Wu, T. Hu, J. Dong, Z. Jiang, An efficient collaboration and incentive mechanism for internet of vehicles (IoV) with secured information exchange based on blockchains. IEEE Internet Things J. **7**(3), 1582–1593 (2020)
43. K. Liu, W. Chen, Z. Zheng, Z. Li, W. Liang, A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles. IEEE Internet Things J. **6**(5), 9098–9111 (2019)
44. C. Chen, J. Wu, H. Lin, W. Chen, Z. Zheng, A secure and efficient blockchain-based data trading approach for internet of vehicles. IEEE Trans. Veh. Technol. **PP**, 1 (2019). https://doi.org/10.1109/TVT.2019.2927533
45. X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, M. Guizani, Blockchain-based on-demand computing resource trading in IoV-assisted smart city. IEEE Trans. Emerg. Top. Comput. **1**, 1–1 (2020)
46. Y. Lu, X. Huang, K. Zhang, S. Maharjan, Y. Zhang, Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans. Veh. Technol. **69**(4), 4298–4311 (2020)
47. Q. Feng, D. He, S. Zeadally, K. Liang, Bpas: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Trans. Ind. Inf. **16**(6), 4146–4155 (2020)
48. D. Zhang, F.R. Yu, R. Yang, Blockchain-based distributed software-defined vehicular networks: a dueling deep *Q*-learning approach. IEEE Trans. Cogn. Commun. Netw. **5**(4), 1086–1100 (2019)
49. J. Gao, K.O. Obour Agyekum, E.B. Sifah, K.N. Acheampong, Q. Xia, X. Du, M. Guizani, H. Xia, A blockchain-SDN-enabled internet of vehicles environment for fog computing and 5g networks. IEEE Internet Things J. **7**(5), 4278–4291 (2020)
50. V. Sharma, An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). IEEE Commun. Lett. **23**(2), 246–249 (2019)
51. Z. Xiong, W. Li, Q. Han, Z. Cai, Privacy-preserving auto-driving: a GAN-based approach to protect vehicular camera data, in *2019 IEEE International Conference on Data Mining (ICDM)* (2019), pp. 668–677
52. Y. Liu, K. Wang, Y. Lin, W. Xu, LightChain: a lightweight blockchain system for industrial internet of things. IEEE Trans. Ind. Inf. **15**(6), 3571–3581 (2019)
53. W. Yang, X. Dai, J. Xiao, H. Jin, Ldv: a lightweight DAG-based blockchain for vehicular social networks. IEEE Trans. Veh. Technol. **69**(6), 5749–5759 (2020)

Publisher's Note