Complex & Intelligent Systems
https://doi.org/10.1007/s40747-021-00603-7

SURVEY AND STATE OF THE ART

Distributed ledger technologies in vehicular mobile edge computing: a survey

Ming Jiang[1] · Xingsheng Qin[1]

Received: 4 June 2021 / Accepted: 26 November 2021

Abstract
Blockchain-based systems, coined by distributed ledger technologies (DLTs), have rapidly received tremendous interest from academia, industries, and governments. Recent literature has revealed many research and developments on applying DLTs to the Internet of things (IoT), cloud-edge computing. In this survey, we conduct a comprehensive survey of the newly appeared concepts, theories, platforms, and DLTs-facilitated applications of vehicular networks and mobile edge computing (MEC). We also review the selections of the available DLTs related platforms and tools. Future research directions and issues are discussed, including security, privacy, scalability issues, and multiple applications in various domains.

Keywords Survey · Distributed ledger technologies · Blockchain · Vehicle · Mobile edge computing

الكلمات الرئيسيه (بلوكتشين) · (تقنية الحافة الموزعة) · (فانيت) · (حوسبة الحافة المتنقلة)

Introduction

The advance of intelligent and connected vehicles (ICVs), enabled by the development of big data, artificial intelligence (AI), cloud-edge computing, and Internet of vehicles (IoV) technologies, will radically reshape the intelligent transportation systems (ITS), economy [1] and environment forum [2], and drivers' experience.

Meanwhile, IoV is becoming a vital technology to improve the efficiency and safety of the ITS [3]. And edge computing is another innovative extension of cloud computing, and it significantly reduces the transmission latency through the deployment of edge nodes that are geographically close to the end-users [4]. Technologies like fog computing, virtual cloudlet, and mobile cloud are all based on the same concept to enable a large scale of heterogeneous devices to run complex applications by leveraging the computational capability of the edge servers [5]. Real-time services and applications are not sufficiently handled due to the high latency of the cloud computing structure. On the contrary, MEC clouds are placed at the edge of the network and they can effectively exploit the computing and storage resources of the edge servers and subsequently reduce the delay of network transmission [6, 7]. Hence, the MEC will certainly become a vital enabler of various next-generation technologies like 5G, IoT, cyber-physical systems (CPS), vehicle-to-vehicle (V2V), and vehicle-to-everything (V2X) communications [8].

The research goal of ICVs in MEC is to improve road safety and boost the efficiency of the ITS [9]. Over 1.25 million people die in car accidents globally each year, some researchers believe that the adoption of ICVs will significantly reduce the figure of casualties [10]. Despite the benefits, it is also clear that the ICVs are also exposed to malicious cyber-attacks when ICVs are connected to the IoV [11]. There are various communication modules and interfaces inside an ICV, and these are potential vulnerabilities that could be exploited by malicious attackers. Without appropriate countermeasures, ICVs can be easily controlled by cyber-attackers and threaten the lives of drivers [12, 13].

Meanwhile, the digitalization of the transportation system will produce a large amount of data, particularly in large countries [14]. Through various embedded sensors and communication modules, an ICV can collect users' information, such as the position and speed, the driver's degree of atten-

✉ Xingsheng Qin
qinxingsheng@foxmail.com

Ming Jiang
franknsw2011@gmail.com

[1] Faculty of Electronic Engineering, Guangxi Normal University, Guilin, China

Published online: 05 April 2022

tion, acceleration, and brake interventions, and send to the central server [15]. And these enormous quantities of data can also threaten the safety of ICVs and potentially compromise the privacy of users. The development of privacy-preserving and cyber-security techniques of ICVs are critical to a sustainable ITS [16, 20].

The emerge of DLTs and Blockchain (BC) instantly received enormous interest from researchers, industries, and governments [17, 18]. Due to their security characteristics, the implementation of these technologies could have the potential for anti-cyber attacks and privacy-preserving in the IoV [19, 20]. The integration of DLTs and MEC into the IoV systems can empower reliable access, data storage, and computation capacity which are distributed at the edge servers [21]. And security challenges of edge-based ICVs such as confidentiality and authenticity attacks, which can also be mitigated by leveraging the advance of DLT-based techniques. DLTs and MEC techniques have the potential ability to ensure the safety and security of V2X communication while improving the efficiency of data transmission [22]. Therefore, it is very important to do an in-depth investigation and analyze these technologies' security requirements before implementation.

Our work aims to reveal how a range of emerged DLTs and edge computing techniques in recent years have been applied to tackle security and privacy issues within the Intelligent Transportation System and to survey potential applications of DLTs to ICVs. And we focus on the following questions: What are DLTs and MEC? How have DLTs and MEC techniques been used in the ITS? And what potential challenges DLTs can resolve?

Hence, an IoV network built on a DLT-based architecture has the potential to empower a secure and privacy-preserving ITS in an effective way. Other challenges in the IoV network concern the authentication mechanism, access control, and data management issues. Existing solutions to these challenges cannot be used in the IoV domain due to the limitation of computational capability and the scale of IoV. New designs and DLT-based technologies are needed to tackle these challenges. Table 1 enlists all the abbreviations used in this paper.

Contributions

There are several survey papers related to the integration of DLTs with ITS [23–30]. In the work of [21–24], they focus on the implementations of BC technologies in the IoV and IoT domains. However, the use of mobile edge computing in vehicular networks is not fully investigated in these papers. Likewise, in [25–28], the authors focus on the security and privacy solutions and challenges related to BC and vehicular edge computing (VEC) integration. Thus, DLTs and MEC integrated solutions in the ITS are only analyzed partially, and the existing DLT-based platforms and useful tools in vehicular MEC research are not discussed in detail. A comparison table of the different aspects of relevant surveys and the main issues in this article is given in Table 2. In comparison with the aforementioned survey papers, the contributions of this survey are four-fold:

Table 1 Abbreviations in the paper

Abbreviation	Full name
AI	Artificial intelligence
BC	Blockchain
BLA	BC-assisted lightweight anonymous authentication
BSM	Basic safety message
CA	Certificate authority
CPS	Cyber-physical systems
DAG	Directed acyclic graph
DLT	Distributed ledger technology
DRL	Deep reinforcement learning
dPoW	dynamic proof of work
EVM	Ethereum virtual machine
ICV	Intelligent and connected vehicle
IoT	Internet of things
IoV	Internet of vehicles
ITS	Intelligent transportation systems
LBS	Location-based service
MEC	Mobile edge computing
NDN	Named data networking
OBU	Onboard unit
P2P	Peer-to-peer
PH	Platoon head
PKI	Public key infrastructure
PM	Platoon member
PoW	Proof of work
PoS	Proof of stake
PUF	Physical unclonable functions
PVFC	Parked vehicle assisted fog computing
QoS	Quality of services
RSU	Roadside unit
SDN	Software define network
TA	Trusted authority
V2G	Vehicle-to-grid
V2I	Vehicle-to-infrastructure
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
VANET	Vehicular Ad hoc NETwork
VEC	Vehicular edge computing
VFC	Vehicular fog computing
VFCS	Vehicular fog computing service
VSN	Vehicular social network

Table 2 Comparison with related existing surveys

Refs.	Security and privacy	Network framework	Data management	Consensus mechanism	Energy sharing and trading	Platforms and tools for MEC
[21]	√	×	×	×	×	×
[22]	√	×	×	√	×	√
[23]	√	×	×	×	×	×
[24]	√	×	×	√	×	×
[25]	√	×	√	×	×	×
[26]	×	×	√	×	×	×
[27]	√	√	×	√	×	×
[28]	√	×	√	×	×	×
Ours	√	√	√	√	√	√

(1) Firstly, we focus on vehicular issues of DLTs in the IoV domains. We will also expand the coverage of security and privacy issues in MEC.
(2) Secondly, we will survey the recently updated DLT-based applications in vehicular MEC.
(3) Thirdly, a comparative analysis among various DLT-based applications in MEC is also provided in detail.
(4) Furthermore, several DLTs related platforms and tools in IoV environments are described.

Organization

This paper's remainder is organized as follows: "DLTS and IOV network architecture" presents basic concepts relevant to the DLTs techniques and IoV network architecture. "DLTs for vehicular MEC security and privacy" summarizes the main features of DLTs in MEC, and "Applications of DLTs in vehicular MEC environment" presents the application scenarios of DLTs in vehicular MEC. "DLT related platforms and tools for vehicles in MEC" analyzes DLT related platforms and tools that are market available for Vehicles in MEC. "Open issues and challenges" analyzes the open issues and challenges of using DLTs in the IoV. "Conclusions" concludes the article. Figure 1 illustrates the overall organization of the paper.

DLTS and IOV network architecture

After the invention of computers, traditional ledgers were replaced by digital ledgers to record money and property in a centralized manner. Digital distributed ledgers technology is a combination of cryptographic puzzles, security protocols, and incentive mechanisms [17, 31], and it is based on decentralized architecture and requires trust and transparency.

We describe the basic concept of a DLT-based system and its main features, and an overview of IoV architecture is also presented that provides the background information of IoV and its essential components.

Distributed ledger techniques

DLTs system structure

Bitcoin has already become a popular and expensive digital currency, which was introduced by Satoshi Nakamoto [32]. It is built on a decentralized structure based on BC technology, and transactions can be digitally made among Bitcoin owners without disclosure of user privacy.

A typical distributed ledger system has five layers [24], as shown in Fig. 2, including Data Layer, Network Layer, Consensus Layer, Contract Layer, and Application layer.

The transaction is the basic unit of a DLT-based ledger, which is collected into blocks by leveraging hash functions. And these blocks are linked together in a BC in which blocks of data are chronologically connected. Each block contains a pre-hash which is used to link the previous block.

Each block contains a blockhead and a block body, as shown in Fig. 3. The block header has three parts: (1) the data used to connect the previous block and index of hash value from the parent block; (2) the mining difficulty, nonce (random number), the timestamp; (3) the Merkle root data of all the transactions which are stored in the block body [33]. The block body contains the transaction data, including the private keys, the figure of transactions, and the digital signature. It can be seen that most of the functions of BC can be realized through the blockhead. Meanwhile, directed acyclic graph (DAG) was developed to improve the scalability and efficiency problem of BC [34].

DLTs systems are built on the peer-to-peer (P2P) network structure in a decentralized manner, where all users share resources without central servers [35]. For instance, every node in the Bitcoin system is involved in the process of transmission and validation of transactions in the P2P network [32, 36]. A whole copy of the ledger is kept in each Full node,

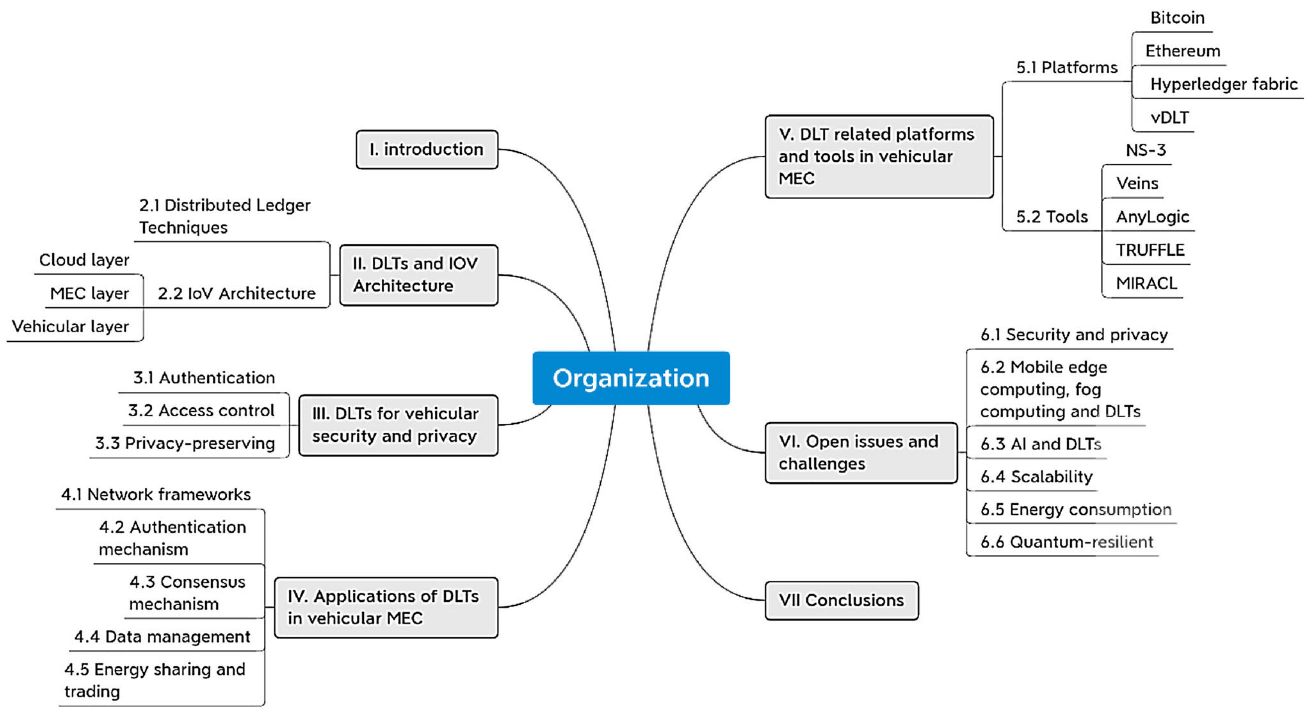
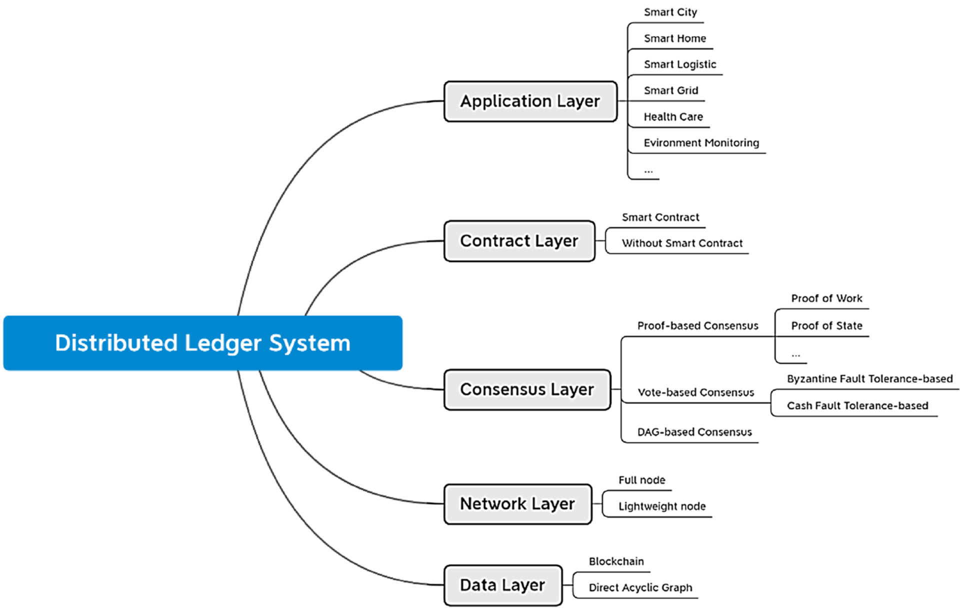


Fig. 1 Organization of the survey on DLTs in vehicular MEC

Fig. 2 The structure of a typical distributed ledger system



which makes it possible for them to verify the content of the transactions. Lightweight nodes have limited computational capability and storage space, so they only store the block headers for consistency verification.

The consensus algorithm is introduced to guarantee that each node can have the correct record of the ledger. Researchers have presented various consensus algorithms and used DLTs systems, and most of them fall into three categories: proof-based, vote-based, and DAG-based consensus algorithms [37].

Proof-based consensus: like proof of work (PoW) and proof of stake (PoS), requires the nodes to provide evidence that they should be included in the system [38].

Vote-based consensus requires nodes to share their results of verifying a new block before reaching an agreement [38].

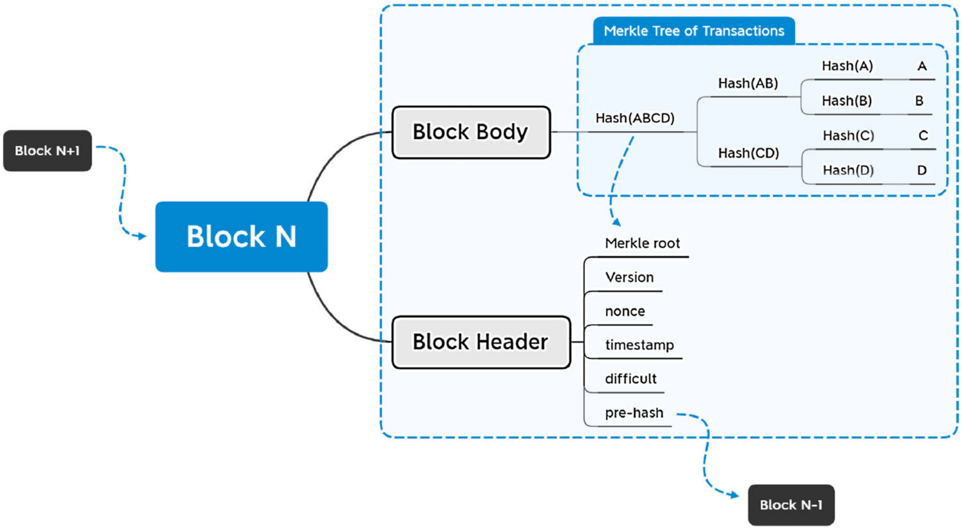


Fig. 3 Detailed structure in the chained block

And a multi-party communication protocol is needed to obtain each node's state to reach a consensus.

DAG-based consensus: users are obligated to order their transactions when a leader vote is unnecessary. A representative's weight is calculated as the sum of all balances for nodes that chose this representative. Based on the voters' weight, the node that gains the most votes will be the winner [34].

A smart contract is a computer protocol that can execute automatically, and it is written into code after the agreement is achieved between seller and buyer. The DLT-based system is the perfect environment for smart contracts to run due to its security intrinsic. Through smart contracts, DLT-based platforms can be used not only for cryptocurrencies but also for various applications in the real world [18, 24, 39].

Features of distributed ledger techniques

There are four features of the DLTs, which can be summarized as follows:

(1) **Distributed and decentralization**: DLT-based system is distributed storage and computing without centralized management, and all nodes have the same rights and obligations. Meanwhile, numerous nodes are competing to obtain accounting rights in the BC, the single node error will not affect the functionality of the whole system. Only when over 51% of the computational power is in control, then malicious users can master the whole system in the BC which is almost impossible.
(2) **Openness:** without a central authority, the nodes in the DLT-based systems do not trust each other but trust the whole system. Because of the conflict of interest between nodes and systems, DLT-based systems have to disclose information on the system. Meanwhile, for privacy-preserving, the information of each node is confidential to other nodes.
(3) **Transparency:** the data recording and updating operation of the DLT-based system is transparent to the whole network, which is the basis of the trustworthiness of the DLT-based system. DLT-based systems use open-source programs, open rules, therefore data records, and operational rules can be reviewed and tracked by each node to guarantee transparency.
(4) **Tamper-proof:** in DLTs systems, the data is permanently stored and cannot be changed after it is verified and added to the BC. Any attempt to modify data on a single node is impossible, and therefore the data stability and reliability of the DLTs system are extremely high.

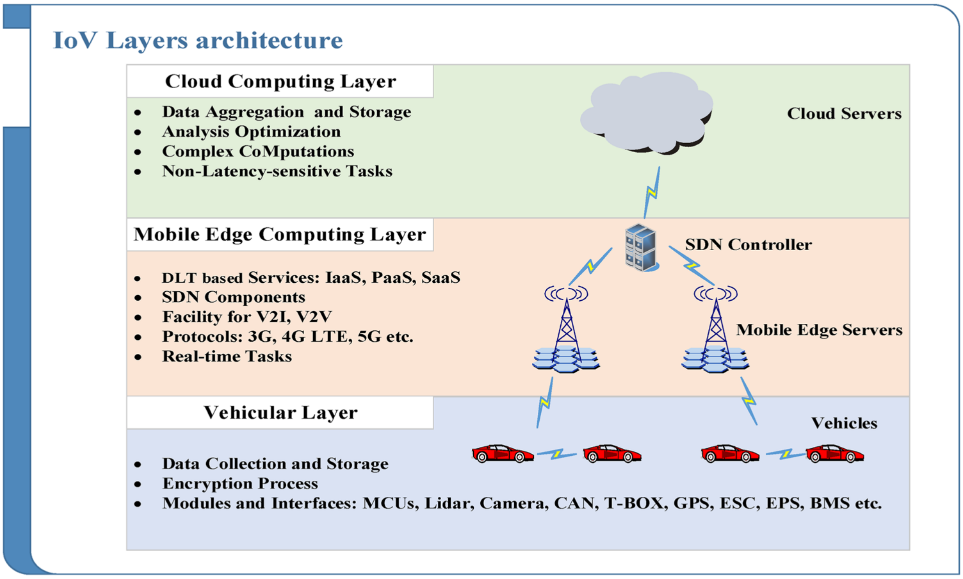
IoV architecture

The advancement of ICVs creates new requirements on the ITS to support the increasing workloads and real-time applications and reshapes the transportation system. The future ITS includes smart vehicles, Roadside units (RSUs), network infrastructure, MEC edge, and the cloud. The MEC techniques enhance the edge cloud for autonomous driving by providing services like real-time Maps, real-time traffic monitoring, etc. Meanwhile, it empowers ICVs to drive cooperatively and roadside awareness, and provide better user experience and trust to drivers [40].

This section illustrates the IoV network architecture and modes of operations. As shown in Fig. 4, the architecture has three layers: cloud layer, mobile edge computing layer, and vehicular layer.

The Cloud layer has two main functions: storage and computation. It deals with data aggregation, data mining, big data storage, batch processing, and the workload of complex

Fig. 4 IoV Layered Architecture


IoV Layers architecture
Cloud Computing Layer
Data Aggregation and Storage
Analysis Optimization
Complex CoMputations
Non-Latency-sensitive Tasks
Cloud Servers
Mobile Edge Computing Layer
DLT based Services: IaaS, PaaS, SaaS
SDN Components
Facility for V2I, V2V
Protocols: 3G, 4G LTE, 5G etc.
Real-time Tasks
SDN Controller
Mobile Edge Servers
Vehicular Layer
Data Collection and Storage
Encryption Process
Modules and Interfaces: MCUs, Lidar, Camera, CAN, T-BOX, GPS, ESC, EPS, BMS etc.
Vehicles

computations, and the storage and computation requirements of these tasks cannot be provided by the edge servers [41]. Moreover, the cloud layer computes enormous amounts of data and complex computations in a short period. And the data storage in the cloud could be exploited for future purposes and non-real-time applications, which are sent to the cloud layer through Software Define Network (SDN) controller.

The MEC layer is the middle of the vehicular and cloud layers to ensure data exchange. This poses challenges to the wireless communication modules in the ICVs [30]. To provide low latency, be aware of the roadside environment, emergency management, data caching, content delivery, computation capability, and improve the quality of services (QoS) since the MEC layer is close to ICVs, which is used to deal with real-time tasks from ICVs, such as traffic signs recognition, video analytics, and human behavior recognition.[42]. Thus, the MEC layer provides the following services to ICVs in the IoV.

Infrastructure as a service: ICVs need extra storage to run their applications and make a backup for a temporary purpose. This requirement is fulfilled by leveraging the resources that are provided by the distributed and decentralized edge servers. Edge servers provide free storage and computation facilities for clients to run their applications and construct the DLT-based vehicular network.

Platform as a service: DLT-based services are offered as a platform, which provides a development environment, programming languages, and toolkits for users. Meanwhile, it also gives useful APIs to the edge servers such as BC-based storage, smart contracts, and consensus mechanism.

Software as a service: multiple services for the vehicles are applications that are running on the edge servers, such as information sharing, encryption, authentication. Apart from offering a communication facility for V2V and vehicle to infrastructure (V2I), data sharing between ICVs happens constantly until data arrive on the RSUs or edge servers [43]. For instance, when an ICV shows abnormal behavior, like direction change, violation of the speed limit, or mechanical failure, nearby vehicles and RSUs will receive emergence messages, which contain information about that ICV [44]. And the data exchange among ICVs also relies on V2I communication facilities like RSUs and micro base stations over wireless connections managed through SDN.

The Vehicular layer is geographically around ICVs, and they share computing and storage resources by leveraging the 5G communication network [44]. The ICVs can collect from sensors, cameras, radar, lidar, GPS, etc. [3], and then the data will be sent to the MEC layer, which could be used to provide certain services like environmental awareness and behavior recognition of drivers. Meanwhile, with the implementation of Artificial Intelligence (AI) technologies, ICVs can anticipate the drivers' intentions.

DLTs for vehicular MEC security and privacy

Regardless of the type of applications, it has become a key challenge to ensure the security of the IoV network, while strengthening privacy. After the advent of DLTs, it has been considered as a potential solution to this challenge. In this section, we discuss the way that DLTs techniques are being used to tackle these issues in vehicular MEC. The related security measures can be categorized as authentication, access control, and privacy-preserving.

Authentication

Identification is used for authentication to check whether the user is authorized [45]. In the IoV network, Basic safety messages (BSMs) are constantly broadcasted among ICVs to empower various applications, which are lightweight messages that contain critical information of ICVs. However, it can also be exploited by malicious attackers to control an ICV remotely by injecting fake BSMs [46]. The key to solving this threat is to guarantee that the ICVs verify the authenticity of the RSUs while authenticating themselves in a fast and effective way. Thus, a completely new design of lightweight and fast authentication between moving ICVs is needed to face this challenge.

According to the mechanisms and algorithms, there are five different authentication techniques: (1) light-weight authentication, (2) hash-based authentication, (3) batch verification-based authentication, (4) dual authentication, and (5) privacy-preserving authentication [47].

Normally, in the IoV environment, a user authentication mechanism involves the following steps [48]:

- System configuration: the trusted authority (TA) is in charge of the system parameters generation.
- Registration: before the deployment of ICVs and RSUs, they must be registered with the TA. Then the essential identifiers are embedded in the Onboard Unit (OBU) of the registered ICVs and RSUs.
- User registration: users need to register with the TA to access the services offered by RSUs, and after analyzing the users' data, the registered user will receive a smart card or mobile device from the TA.
- Login: users provide their credentials, and after validation of the credentials by their smart cards or mobile devices, a "login request message" is sent to the RSU through a public channel.
- Authentication and key agreement: after receiving the login request message, the RSU validates the message and sends the “authentication request message” to the user. The user also checks the validity of the received message and then rapidly replies to the RSU. Once validating the received message from the user, the RSU and user agree on a standard session key for secret communication between them.
- Password and biometric update: users can change their passwords or biometrics locally with the absence of the TA, and this process is important for security enhancement.
- Smart card/mobile device revocation: this phase is essential when a registered smart card or mobile device is missing, and a new smart card or mobile device will be issued with updated credentials.
- Dynamic node addition: this session allows a new vehicle or an RSU to be added after deployment.

To authenticate ICVs and certify their identities, Public Key Infrastructures (PKIs) are introduced, but centralized PKIs have various pitfalls like single point of failure, privacy, trust, expensive, etc. [23]. In this context, various DLT-based PKIs have been proposed in the IoV domain.

Access control

Access control is another critical security measure to guarantee the safety of data generated in the IoV networks, where only authorized nodes can access sensitive data. An access control mechanism contains two tasks [48]:

- Node authentication: new nodes (ICVs and RSUs) must authenticate themselves before they can access the services.
- Key establishment: To enhance secure communication between nodes, a secret key is needed from the new node to its neighbors when the mutual authentication is finished.

RSUs are the basic elements of the Vehicular Fog Computing (VFC) infrastructures which are located at the edge of the IoV network, and it is used to handle generated data within the ICVs. Sharma et al. [49] proposed a DLT-based vehicular data management architecture to access these data securely and efficiently. In this architecture, RSUs are exploited as the key components to manage data and a consensus is introduced to maintain the trustworthiness of the newly added data. Similarly, Kai et al. [50] developed three security measures: key management, cache poisoning detection, and access control, which are used to improve the cyber-security of named data networking (NDN) VEC networks.

Privacy-preservation schemes

ICVs are exposed to various cyber-attacks when the central servers can access the users' data which raises another concern about privacy violation [15]. To address these issues, researchers developed various DLT-based privacy-preserving schemes in the IoV. Ferdous et al. [51] presented a DLT-based scheme that empowers ICVs to generate a tamper-proof record of data. Similarly, Kong et al. [52] developed a scheme for sensory data sharing based on DLTs in the VFC, which can improve the protection of user privacy and data integrity.

Likewise, Li et al. [53] proposed a scheme for carpooling using DLT-based techniques and VFC. To guarantee data auditability, RSUs are chained together to form a private BC and it is used to record carpooling processes in a DLT-based ledger.

A DLT-based parking system was proposed by Amiri et al. [54], to ensure the security, transparency, and availability of the parking offers, in which parking spot owners create a consortium BC. Likewise, Hu et al. [55] developed a BC-based framework for parking management by integrating Block Chain Open Source and smart contract technology to secure the privacy of users. And Zhang et al. [56] proposed a BC-based parking scheme by leveraging group signatures, bloom filters, and vector-based encryption for privacy-preserving.

Applications of DLTs in vehicular MEC environment

The design goal of ITS is to boost the performance of Vehicular Ad hoc NETworks (VANETs), and it provides various services including smart parking, smart routing, traffic monitoring, and smart insurance claiming [24]. But traditional ITS is based on centralized servers which have many security pitfalls [57]. With the emerging of DLTs, researchers begin to develop the integrated applications of DLTs and IoV. This section will discuss many cases of DLTs in VEC scenarios, such as the design of network structures, authentication schemes, consensus algorithms, data sharing, and energy sharing and trading.

Network frameworks

Centralized solutions are not suitable for the smart ITS, on the contrary, decentralized and tamper-proof DLT-based frameworks are developed to improve trustworthiness. For example, RSUs are used to offload tasks to nearby ICVs in the framework designed by Iqbal et al. [58], and reputation scores of ICVs are maintained on a BC.

Gao et al. [59] presented a framework based on BC and SDN, and it is designed for VFC systems by leveraging the 5G communication network. The BC technology is introduced to boost the efficiency of IoV and build trust among ICVs, and SDN is exploited for management in VANET systems. By leveraging the computational capability of the edge servers in the VFC, the handover issues among the ICVs were improved.

A framework was designed by Liu et al. [60] to solve the security issues for both information and energy interactions in electric vehicles cloud and edge computing. The context-aware vehicular applications were presented based on the EVs' different roles, and they also introduced DLT-based data coins and energy coins to achieve distributed consensus. Meanwhile, data contribution frequency and energy contribution quantities are used for proof determination.

Likewise, Zhang et al. [56] proposed a framework to enhance the security of VANET that integrates BC and MEC. This framework is divided into three layers, namely the perception layer, the edge computing layer, and the service layer. By leveraging the BC-based technology, the perception layer guarantees the safety of VANET data in the communication process and the service layer secures the data in the cloud. The edge computing layer offers computing resources and edge cloud services to the perception layer.

TrafficChain is presented by Wang et al. [61], which uses BC technology to build a secure and privacy-preserving distributed system for traffic data collection. In particular, a two-layer blockchain architecture is introduced to boost efficiency, and a privacy-preserving framework is developed to protect the privacy of users. Meanwhile, a derivation of a LSTM-based deep learning algorithm is used against Byzantine attacks and Sybil attacks. Furthermore, to encourage user participation an incentive mechanism is employed in the framework.

Chen et al. [62] proposed a framework for self-driving vehicles to improve efficiency, in which vehicles are grouped in a platoon and led by the Platoon Head (PH). A PH selection algorithm was designed to offer a motivation for vehicles to be PHs, and update the platoon whenever needed. Moreover, to against malicious and false payments between the PH and Platoon Members (PMs), a smart contract is introduced to enable the BC-based payment.

Chen et al. [63] presented a BC-based searchable public-key encryption framework with forward and backward privacy, in which the central search cloud server is replaced by a decentralized searchable public-key encryption framework using a smart contract. Meanwhile, the framework employs forward and backward privacy to enhance privacy-preserving.

Rawat et al. [64] presented a privacy-aware V2X communications framework by exploiting the BC and NDN. In the proposed framework, only non-private information is included while providing verifiable, secure V2X communications for the integrity and accountability of the communications by combing the advantages of BC and NDN.

Authentication schemes

Vehicular fog computing services (VFCSs) are provided through various distributed data centers, which require cross-data center authentication. Traditional authentication schemes are not suitable for the ICVs in the IoV to access VFCSs, because they often lack consideration of user privacy and communication latency. Recent research on DLT-based authentication schemes are characterized by light-weight, key exchange mechanism, traceable driving route data, and the dynamic proxy mechanism as well as the privacy-preserving. Specifically, Yao et al. [65] proposed a BC-assisted lightweight anonymous authentication (BLA) mechanism for distributed VFCSs offering to ICVs. Flexible cross datacenter authentication can be achieved in the BLA scheme, in which an ICV can choose whether or not to be re-authenticated when it goes into a neighbor vehicular edge. Meanwhile, through anonymity and granting drivers' responsibility users' privacy is protected. To achieve the lightweight performance, both the interactivity between ICVs and service managers and the communication between SMs in the authentication process are eliminated, as a result, the communication latency is significantly decreased. By leveraging cryptographical and BC technologies, BLA is tamper-proof to the risk of single point of failure by design.

A lightweight authentication and key exchange scheme for VFC infrastructures have been proposed in [66]. The scheme is based on VEC and BC, in which ICVs can access VFCS with multiple features like cross datacenter authentication, user anonymity, mutual authentication, lightweight, privacy-preserving, and confidentiality. The proposed scheme considerably reduces communicational and computational overheads with effective security countermeasures. Similarly, Huajie et al. [67] proposed a BC-based lightweight Certificate Authority (CA) for efficient privacy-preserving location-based service in IoV networks.

Zhang et al. [68] presented a DLT-based authentication scheme for ICVs in the IoV, and each node contains a decentralized identification that is based on traceable driving route data and the dynamic proxy mechanism. In the dynamic proxy edge computing (DPEC) mode, cooperative authentication based on secret sharing and DLT-based data tracking and trust management is employed to enhance the protection of user privacy while improving system performance.

A lightweight threshold CA for consortium BC and a privacy-preserving location-based service (LBS) protocol enforced vehicular social networks (VSNs) is proposed by Shen et al. [67]. In this scheme, a lightweight threshold CA framework, a threshold proxy signature where the proxy signing key is issued by a coalition of the threshold number of CAs as authorized nodes in the consortium BC. A privacy preserving LBS protocol PPVC is designed against the background analysis attack by updating the ICVs' BC address regularly.

Wang et al. [69] proposed a B-TSCA scheme, which is a BC-assisted trustworthiness scalable computation system-based V2I authentication, to reduce the complexity of continuous identity authentication when the ICVs pass the nearby RSUs. Fast re-authentication among network nodes is achieved in the scheme, through sharing ownership between RSUs securely based on DLT-based techniques.

Consensus mechanism

Vehicular MEC has been considered as an essential application of edge computing in IoV networks. Bonadio et al. [70] proposed an architecture inspired by edge paradigm to achieve a full context awareness for VANET, and deal with anomalous traffic conditions. Classical DTN Flooding based, NC multi-flows, and chord protocols are investigated, while DLTs are introduced to achieve a distributed consensus. The generated data of ICVs have linked to a permissionless blockchain in a correlated traffic pattern joint the consensus-making process. And an alternative PoW is introduced, which implements a lightweight and time-based consensus mechanism, to reduce complexity and boost reactiveness. In this architecture, ICVs send the information they collected and update the content of their block. Once a block is filled, ICVs initiate the validation phase and send the validated block to other nodes through a VM.

To implement offloading services, enhance network security and boost efficiency, Huang et al. [71] proposed a Parked Vehicle Assisted Fog Computing (PVFC) Chain by using DLTs technology. Request posting, workload undertaking, task evaluation, and reward assignment are organized and validated automatically through the execution of a smart contract.

Javaid et al. [72] developed a BC-based protocol using smart contracts, Physical unclonable functions (PUF), certificates, and a dynamic proof of work (dPoW) consensus algorithm in IoV. Combined with contracts and the BC, a secure system is formed to register trusted ICVs and block malicious ones. PUFs are exploited to improve trustworthiness through which a unique identity is given to each ICV. The use of dPoW consensus allows the protocol to scale based on the traffic and certificates are issued by RSUs for privacy-preserving.

To resolve the Byzantine Generals Problem, Zheng et al. [73] introduced lightweight BC consensus protocols on VSN. In this scheme, a hybrid chain is formed by a private chain and a public chain. Communication reliability is considered on the private chain and a scheme is provided for transferring data onto the public chain.

Data management

Vehicular sensing is empowered by the enormous data generated in ICVs, and the RSUs can also be used as edge nodes to collect and share data in MEC. Nevertheless, there are still several issues to be solved to guarantee that the sensory data can be shared securely in MEC.

Chen et al. [74] built a two layers data-sharing system based on DLTs. The demands and supplies of nodes are collected by the nearest RSUs at the bottom layer which can be used for further matching at the upper layer. A matching algorithm is developed to achieve the balance between demand and supply. Meanwhile, to motivate nodes to offer positive services, a reputation management mechanism was introduced.

By leveraging consortium BC and smart contract technologies, Kang et al. [75] presented a P2P data-sharing system, in which a reputation-based mechanism is developed to secure data sharing among ICVs. And a three-weight subjective logic model is used for handling the reputation of the ICVs. In this scheme, accurate reputation management for data sharing is achieved, and during the data sharing process, ICVs have the option to choose high-ranked data providers.

To reduce transmission costs and protect user privacy, Lu et al. [76] presented a framework based on federated learning and developed a hybrid blockchain architecture to secure the model parameters by combining the permissioned BC and the local DAG. Moreover, an asynchronous federated learning scheme is introduced based on Deep Reinforcement Learning (DRL) for fast node selection. To ensure data reliability, they integrated the trained models into BC and employed a double verification.

A BC-based data sharing scheme is presented for vehicular networks in [77]. Edge service providers are introduced to boost the efficiency of data sharing, which are placed close to the ordinary nodes to guarantee the reliability of communication between them. Interplanetary file system, a distributed file storage system, is introduced to store the data generated within the IoV network to tackle the issues related to data storage in centralized architectures, including data tampering, lack of privacy, vulnerability to hackers, etc. And with monetary incentives, edge nodes are motivated for accurate and fast service provisioning.

Dai et al. [78] integrated DRL and permissioned BC into IoV for intelligent and secure content caching. And a BC-based distributed content caching framework is designed where ICVs perform content caching and base stations maintain the permissioned BC. By employing the advanced DRL approach, a content caching scheme is introduced with taking mobility into account. Furthermore, a block verifier selection technique is also developed, Proof-of-utility (PoU), to shorten the block verification process.

Jeong et al. [79] proposed a BC-based platform for vehicle data marketplace, along with a data-sharing scheme, using BC-based data-owner-based attribute-based encryption (DO-ABE). The proposed platform achieves data confidentiality, integrity, and privacy, and handles large-capacity and privacy-sensitive black box video data by storing the metadata on BC and encrypted raw data on off-chain storage. Furthermore, the data owners can control their data by applying the BC-based DO-ABE and owner-defined access control lists.

Javaid et al. [80] presented DrivMan that is a PUF and BC-based solution for driving trust management and data-sharing in VANETs. DrivMan is a trustless system model that uses BC and a CA to register ICVs and withdraw their registration. Certificates issued by RSUs are used to preserve the privacy of the ICVs and PUFs are used to ensure data reliability.

Liu et al. [81] proposed a data-trading and debt-credit system for IoV based on the BC technique to solve the efficiency issues caused by transaction confirmation delays and cold-start problems of new users. In this system, a motivation-based debt-credit mechanism is designed to encourage data exchange among ICVs. Meanwhile, a two-stage Stackelberg game is formulated to maximize the profits of involving ICVs in the data exchange procedure.

Energy sharing and trading

To introduce the opportunities brought by plug-in hybrid electric vehicles (PHEV) to the energy network, Sun et al. [82] proposed a local V2V energy trading architecture based on FC in social hotspots and model the social welfare maximization (SWM) problem to balance the interests of both charging and discharging PHEVs. Consortium BC is employed in this architecture, by leveraging the decentralized nature of the DLTs techniques, which reduces reliance on third parties. Moreover, they improved the practical Byzantine fault tolerance (PBFT) algorithm and developed a consensus algorithm, called delegated proof of stake algorithm, which significantly lowers the cost of resources and boosts consensus efficiency. An energy iterative bidirectional auction mechanism is employed to tackle the SWM problem and obtain optimal charging and discharging decisions and energy pricing, to encourage PHEVs to join V2V energy transactions.

Similarly, Firoozjaei et al. [83] proposed the EVChain, which is a trustworthy and decentralized platform empowered by BC technology. The main BC in EVChain is connected to one or more subnetwork blockchains to share credits. Meanwhile, an interconnection position is introduced for privacy-preserving among users with k-anonymity protection. Likewise, a P2P energy trade network was developed by Thakur et al. [84] that combines V2V or V2X energy trades. In an energy distribution network, energy transfer among microgrids is not permitted so each microgrid operates one local charging station in this system. For the optimum utilization of energy, these microgrids can trade EV charging requests among themselves.

For the sake of energy companies, Fu et al. [85] proposed an EV charging system to improve the user experience with the help of energy companies. Charging information is managed and recorded on a consortium BC and a smart contract is employed to balance the distribution of the charging EVs to ensure that energy companies have equal opportunities to make a profit on this platform. A bio-objective mixed-integer programming model is presented as the logic of smart

Table 3 Application scenarios of DLTs in vehicular MEC

Application scenarios	References	Purposes and approaches
Network structure, edge computing framework	[58–60, 89]	DLT-based architectures and MEC techniques are used in 5G and fog computing to solve the security issues for information and energy interactions and the large computational problem
Traffic information, platooning	[61, 62]	A decentralized traffic information system on the BC and smart contracts is designed to secure the transactions within the platoon
Encryption scheme, communications framework	[63, 64]	Blockchain-based searchable public-key encryption scheme and smart contract design, and V2X communications framework based on BC and NDN
Authentication mechanism	[65, 67–69]	BC-based light-weight anonymous authentication (BLA) mechanism for distributed VFC and privacy-preserving LBS protocol in BC enforced VSNs, rapid re-authentication V2I
Consensus mechanism, Smart contract, and protocol	[70–73]	Light-weight and time-based consensus mechanism for VANET, PVFC Chain based on BC to improve network security and efficiency, and BC-based protocol for IoV using smart contracts, PUF, certificates, and dPoW consensus algorithm
Data sharing, caching, trading and trust management	[74–81]	BC-based reputation management mechanism, data sharing and trading system, data sharing architecture based on federated learning, data caching mechanism, distributed content caching framework, PUF, and BC-based solution for driving trust management and data sharing in VANETs
Energy trading, sharing, and charging system	[82–87]	BC-based energy trading architecture or platform for energy sharing and trading, cooperation system for new energy companies based on DLTs, V2V trading scheme for EVs, V2G energy trading framework

contracts to balance the trade-off between companies' and customers' interests. Furthermore, a new algorithm named limited neighborhood search with memory is designed to boost the deployment which could significantly improve the performance of the smart contract.

To tackle challenge of the driving endurance for the EVs, Xia et al. [86] proposed a V2V electricity trading framework in BC-enabled IoV, and the Bayesian game is employed for pricing with partial information of the users for privacy-preserving which is implemented through the smart contract. The optimal pricing has been achieved, which maximizes the utilities of both sides of the electricity transaction.

One of the successful applications of CPS is the smart grid. Smart EVs empower the implementation of Vehicle-to-Grid (V2G) technology that is a potential solution to improve the demand–supply mismatch issue. Zhou et al. [87] designed a V2G energy trading framework by combining BC, smart contract, and edge computing. A consortium BC-based energy trading mechanism and an incentive mechanism are introduced. To boost the success rate of block creation, edge computing has been incorporated into this scheme.

Summary

The DLTs techniques are considered as the potential solutions to these challenges faced by traditional centralized architectures. Table 3 lists a set of existing DLT-based solutions for different aspects of VEC. And Figs. 5 and 6 show that ICVs connections structure and DLT-based IoV in smart cities, in which DLT-based IoV is considered as the network architecture (for example, a secure fog computing paradigm in [58] or a BC-SDN-enabled architecture for the IoV in 5G and fog computing systems in [59]) for the integration of different elements of ITS. In the DLT-based IoV network, clustering combines ICVs based on map information [88] and DLT-based approaches (for instance, a BLA mechanism for distributed VFS in [65], a data-sharing system that consists of a double-layer blockchain in [74] or a P2P data-sharing system by exploiting consortium BC and smart contract technologies in [75]) are used to guarantee the security and storage of data in network architecture between ICVs. Meanwhile, the energy trading and sharing between V2V or V2G are also considered in this system, such as a local V2V energy trading architecture based on FC in [82, 84] and the work in [87] a V2G energy trading framework is proposed by exploiting BC, contract theory, and edge computing. In this context, ICVs are connected in the DLT-based system, which offers a secure, privacy-preserving, and efficient platform for transactions, data exchange, and energy trading and sharing in ITS without a centralized deficiency.

DLT related platforms and tools for vehicles in MEC

We will describe some existing DLT-based platforms and useful tools in vehicular MEC research and list some typical platforms and tools that are suitable in the IoV domain,

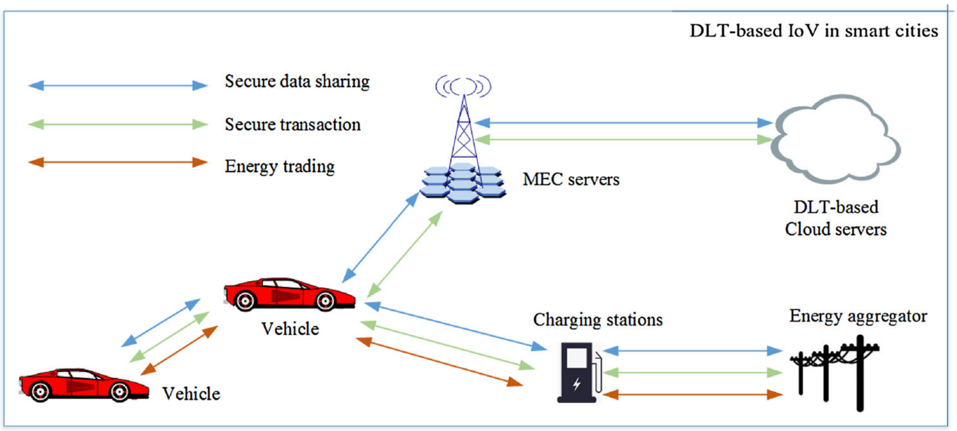


Fig. 5 The structure of ICVs connections

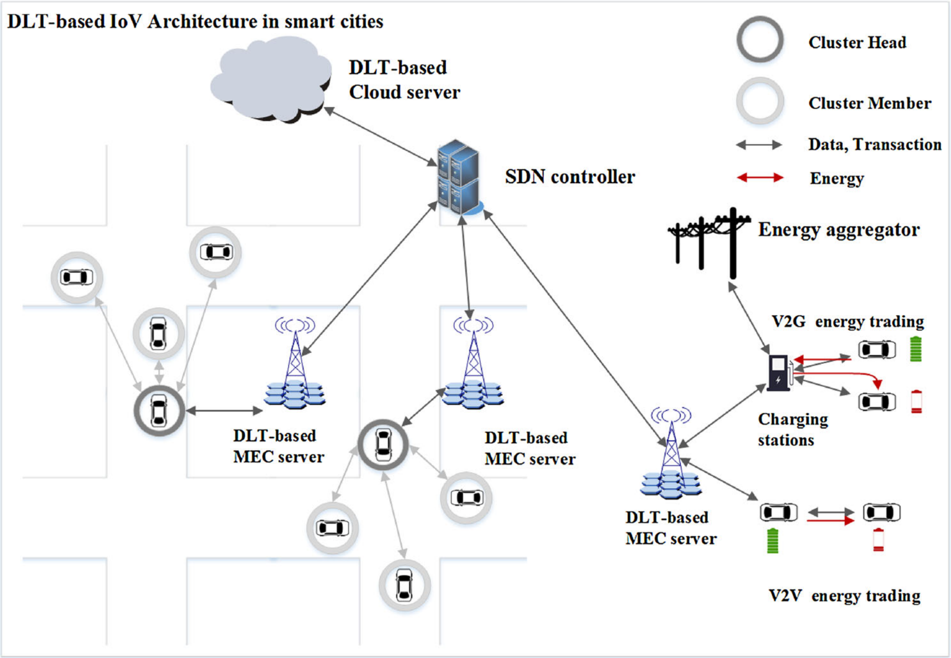


Fig. 6 DLT-based Internet of vehicles in smart cities

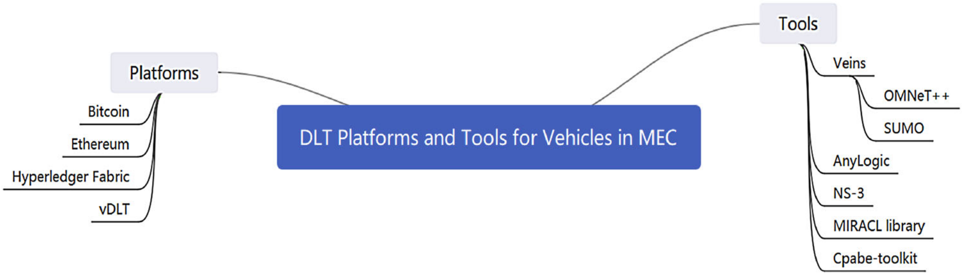


Fig. 7 Typical platforms and tools in the IoV domain

as shown in Fig. 7. And a comparison of distributed ledger platforms for the vehicles in MEC is given in Table 4.

Bitcoin [32] is the very first BC system and the PoW-based cryptocurrency. But the performance of Bitcoin [24] is not suitable for any real-time applications. Even it offers an efficient, cheap, and secure payment system. The innovative data structure and consensus algorithm of Bitcoin inspiring various DLT-based solutions in vehicular MEC, such as in [58, 65, 79].

Table 4 Comparison of distributed ledger platforms for the vehicles in MEC

Platform name	Consensus alg	Open source	Throughput (TPS)	Response time (Secs)
Bitcoin	PoW	Y	3–5	4680
Ethereum	PoW	Y	15–30	360
Hyperledger fabric	PBFT	Y	80,000	< 1
vDLT	Unknown	N	Unknown	Unknown

Ethereum [90] is an open-source platform for decentralized applications created in 2015. And it is a popular programmable BC [91] endorsed by thousands of developers worldwide, and various applications are developed on Ethereum such as cryptocurrency wallets, financial applications, decentralized markets, and so on [86]. Turing complete scripting language, known as Solidity, is used for implementing smart contracts. Ethereum virtual machine (EVM) offers an isolated runtime environment for handling the computation and state of smart contracts in Ethereum [71]. By utilizing the smart contract, lots of IoV applications can be implemented or tested on Ethereum. Sharma et al. [49] implemented vehicular data management as a smart contract on the Ethereum blockchain. Ethereum was also used for performing simulations in the research work of Reference [77], in which a BC-based data storage is presented for decentralized vehicular networks.

Hyperledger fabric [92] is an important member of the open-source BC framework family, Hyperledger [93], supported by the Linux Foundation. Hyperledger Fabric is designed as a platform for developing applications with a modular framework. Consensus and membership services can be plug-and-play on this platform. Its modular and versatile design is suitable for a wide range of industry use scenarios and it provides an extraordinary approach to a consensus that empowers performance while preserving privacy [94]. In [59], Hyperledger Fabric is used as the DLT-based platform, Gao et al. presented a BC-SDN-enabled architecture for the IoV in 5G and FC systems.

vDLT [95, 96] is a service-oriented BC system with virtualization and decoupled management, control, and execution. There are various types of services and applications based on their QoS requirements. Jiang et al. [97] proposed a BC-enabled model sharing approach, and the vehicle BC is based on the vDLT.

TRUFFLE [98] is a friendly development environment for developers, testing framework, and asset pipeline for BC using the EVM. The main features of the TRUFFLE suite include built-in smart contract compilation, linking, deployment and binary management, and automated contract testing for fast development.

NS-3 [99] is a free network simulator for Internet systems, which is widely used in research institutions and universities. To evaluate the performance of their Secure-V2X framework, Rawat et al. [64] used a sharding-based tool built-in NS-3 with different devices and capabilities to join in BC-based communications.

Veins [100] is an open-source framework for running vehicular network simulations. It is based on two well-established simulators: (1) OMNeT + + [101] is an object-oriented, time discrete message passing driven network simulator, and (2) SUMO [102], is a microscopic and continuous multi-modal traffic simulator. OMNeT + + is popular for its modularity, high fidelity, and flexibility, which could also be extended towards the 5G system via VeinsLTE. These features allow the proposal of Bonadio et al. [70] to be allied with the standard for the automotive industry, to model the IoV domain correctly, and to test its performance utilizing network simulations as close as possible to reality. SUMO is an open-source, microscopic, highly portable, and continuous road traffic simulation package designed to handle large road networks. A case study is designed by Javaid et al. [72] for a BC-based protocol using the SUMO simulation package with OSMWebWizard2. Veins' framework extends these to offer a comprehensive suite of Inter-Vehicle Communication (IVC) simulation [103].

AnyLogic [104] is a simulation platform with support for traffic simulation. And it helps to deal with complex challenges like transport network optimization [58]. It allows users to manage transport resource planning, maximize transport load, and minimize costs within the simulation environment.

MIRACL library [105] is a well-known cryptographic library and it is normally used to perform mathematical operations underlying pairing-based cryptography. By utilizing this tool, Ali et al. [106] proposed an efficient certificate-less public-key signature scheme using bilinear pairing to provide conditional privacy-preserving authentication V2I communication in VANETs. Moreover, Chen et al. [63] presented a BC-based searchable public-key encryption scheme with forward and backward privacy for VSN.

Cpabe-toolkit [107] offers a set of programs implementing a ciphertext-policy attribute-based encryption scheme. In a ciphertext policy attribute-based encryption scheme, the private key of each user is associated with a set of attributes representing their capabilities, and ciphertext is encrypted such that only users whose attributes satisfy a certain policy can decrypt. Feng et al. [108] introduced a framework called BC-assisted privacy-preserving authentication system, and it effectively protects user privacy in VANETs, which is based on the cpabe-toolkit.

Open issues and challenges

The adoption of DLTs in the IoV domain is still in its early phase, and its evolution may follow different potential directions. There is a wide range of open issues and challenges with the application of DLTs to VEC.

Security and privacy: even though DLTs are introduced to solve the security and privacy issues in the IoV, it still has various security deficiencies which can be exploited by malicious attackers. For instance, attacked by malicious users, the IOTA users lost over 4 Million dollars [19]. Various vulnerabilities can be used by cyber-attackers, including canceling all transactions, random forks, selfish mining, and double-spending. In the IoV network, ICVs need to share data effectively even the communications between ICVs being unstable. Further and thorough research is still needed to improve data sharing efficiency and enhance network reliability. Meanwhile, drivers are increasingly worried about the security of their data and privacy-preserving that can deter them from positive data-sharing. Consequently, it is still an open issue to secure the data generated in IoV without sacrifice the system performance.

Mobile edge computing, fog computing, and DLTs: edge and fog computing is a potential architecture to reduce the load of the central cloud and boost real-time applications [109]. The rapid development of MEC and FC is due to their abilities to ease some difficult issues like network congestion, latency, and local autonomy. The integration of MEC and BC technologies empowers the upgrade of ITS. For instance, Bonadio et al. [70] proposed a fog communication and computing paradigm to deal with anomalous conditions in the ITS. However, those proposed solutions and applications have not been deployed worldwide due to scalability and communication deficiency [46].

AI and DLTs: researchers have already investigated the integration of BC and AI [110]. In the framework of traditional machine learning (ML), a centralized server is required to collect data. On the contrary, the new emerging federated learning paradigm is a promising approach for distributed circumstances, in which users keep their data with themselves and only the parameters are sent to the server for aggregation [76]. This mechanism enables users to learn a wide model collaboratively while their privacy is well protected [111]. Unfortunately, the ML that directly applies federated learning to ICVs still has pitfalls relying on a central server due to updates of the global ML model are centralized. In the work of Reference [112], Fu et al. designed a BC-based collective learning framework, in which central servers are replaced by the BC system, which can improve the security and performance of the collective learning process. Despite these meaningful research outputs, the implementations of AI and DLTs still have a long way to go, and further research efforts are still needed, such as incentive mechanisms, optimal selection mechanism of model sharing, and so on.

Scalability: a significant challenge within the cybersecurity domain is scalability. The network applications serve thousands of users and the scales grow rapidly. The transaction speed in some BC-assisted systems is relevantly low with a higher charging fee.

Energy consumption: PoW is the most popular consensus mechanism in most BC systems. For instance, by 2020, the energy consumption of Bitcoin reaches 59.26 Terawatt-Hours (TwH), which is even higher than those in some largest countries around the world [113].

Quantum-resilient: another challenge is caused by the emergence of quantum computers, and secure quantum-resilient security architectures are needed against cyberattacks from quantum computers shortly. The authors in [114] proposed a distributed ledger scheme to face this threat. Quantum computing will bring challenges for BC and be used as part of DLTs systems [115].

Conclusions

This survey has provided a review of DLTs techniques and applications in the vehicular MEC. Meanwhile, we have listed the open issues and future research directions like security and privacy, the integration of AI and DLTs, and energy consumption to quantum resilient.

Acknowledgements This work is partially supported by National Natural Science Foundation of China [61762018], the Basic Ability Enhancement Program for Young and Middle-aged Teachers of Guangxi [Grant Numbers 2021KY0060], the Guangxi Key Research and Development Funding [2019AB35004; AB20238030], Natural Science Foundation of Guangxi [2018JJA170109, 2018GXNSFAA281310], the research funding of Guangxi Key Lab of Multisource Information Mining & Security [18-A-02-02], Guangxi Natural Science Foundation [2020GXNSFBA297119], and Guangxi Science and Technology Plan Project [GuiKe-AD20238025].

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Lanctot R (2017) Accelerating the future: the economic impact of the emerging passenger economy. Intel: https://preview.tinyurl.com/ycps9xgh
2. Forum IT (2015) Urban mobility system upgrade. How shared self-driving cars could change city traffic. International Transport Forum. https://www.itf-oecd.org/sites/default/files/docs/15cpb_self-drivingcars.pdf
3. Zhang K et al (2017) Mobile-edge computing for vehicular networks: a promising network paradigm with predictive off-loading. IEEE Veh Technol Mag 12(2):36–44
4. Hassan N et al (2018) The role of edge computing in Internet of things. IEEE Commun Mag 56(11):110–115
5. Khan WZ et al (2019) Edge computing: a survey. Futur Gener Comput Syst 97:219–235
6. Feng J et al (2019) Mobile edge computing for the internet of vehicles: offloading framework and job scheduling. IEEE Veh Technol Mag 14(1):28–36
7. Ji H, Alfarraj O, Tolba A (2020) Artificial intelligence-empowered edge of vehicles: architecture, enabling technologies, and applications. IEEE Access 8:61020–61034
8. Ansari N, Sun X (2017) Mobile edge computing empowers internet of things. IEICE Trans Commun 101:604–619
9. Liu S et al (2019) Edge computing for autonomous driving: opportunities and challenges. Proc IEEE 107(8):1697–1716
10. WHO (2020) Road traffic injuries. Available from: http://www.who.int/news-room/factsheets/detail/road-traffic-injuries
11. Arif M et al (2019) A survey on security attacks in VANETs: communication, applications and challenges. Veh Commun 19:100179
12. Petit J, Shladover SE (2015) Potential cyberattacks on automated vehicles. IEEE Trans Intell Transp Syst 16:546–556
13. Škorput P, Vojvodic H and Mandžuka S (2017) Cyber security in cooperative intelligent transportation systems. In: 59th International Symposium ELMAR-2017. 2017: Zadar, Croatia.
14. Retzer MSS (2018) Defining the future of mobility: intelligent and connected vehicles (ICVs) in China and Germany: opportunities, challenges and the road ahead. Available from: http://www.sustainabletransport.org/wp-content/uploads/2018/09/Defining-the-Future-of-Mobility-ICVs-in-China-and-Germany-1-1.pdf.
15. Joy J and Gerla M (2017) Internet of vehicles and autonomous connected car privacy and security issues. In: 26th International Conference on Computer Communication and Networks (ICCCN). Vancouver, BC, Canada, pp 1–9
16. Lim HSM, Taeihagh A (2018) Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications. Energies 11(5):1062
17. M, W., Distributed Ledger Technology: Beyond Blockchain. 2016, UK Government Office for Science[R]
18. Xiong H et al (2021) On the design of Blockchain-based ECDSA with fault-tolerant batch verication protocol for Blockchain-enabled IoMT. IEEE J Biomed Health Inform. https://doi.org/10.1109/JBHI.2021.3112693
19. Anita N and Vijayalakshmi M (2019) Blockchain security attack: a brief survey. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Kanpur, India, pp 1–6
20. Song J et al (2022) A new secure arrangement for privacy-preserving data collection. Comput Stand Interfaces 80:103582
21. Yang R et al (2019) Integrated blockchain and edge computing systems: a survey, some research issues and challenges. IEEE Commun Surv Tutor 21(2):1508–1532
22. Gupta R, Kumari A, Tanwar S (2020) A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Trans Emerg Telecommun Technol 32(6):e4009
23. Mendiboure L, Chalouf MA, Krief F (2020) Survey on blockchain-based applications in internet of vehicles. Comput Electr Eng 84:106646
24. Zhu Q et al (2020) Applications of distributed ledger technologies to the Internet of things. ACM Comput Surv 52(6):1–34
25. Mohanta BK et al (2019) Blockchain technology: a survey on applications and security privacy Challenges. Internet Things 8:100107
26. Fraga-Lamas P, Fernandez-Carames TM (2019) A review on Blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE Access 7:17578–17598
27. Butt TA et al (2019) Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. IEEE Access 7:79694–79713
28. Zhou H et al (2020) Evolutionary V2X technologies toward the internet of vehicles: challenges and opportunities. Proc IEEE 108(2):308–323
29. Wang Y et al (2020) Challenges and solutions in autonomous driving: a blockchain approach. IEEE Network 34:218–226
30. Raza S et al (2019) A survey on vehicular edge computing: architecture, applications, technical issues, and future directions. Wirel Commun Mob Comput 2019:1–19
31. Lejun Z et al (2020) Secure and efficient medical data storage and sharing scheme based on double blockchain. Comput Mater Continua 66(1):499–515
32. Satoshi Nakamoto (2008) Bitcoin: a peer-to-peer electronic cash system. Available from: https://bitcoin.org/bitcoin.pdf
33. Lao L et al (2020) A survey of IoT applications in Blockchain systems. ACM Comput Surv 53(1):1–32
34. Bencic FM and Podnar Zarko I (2018) Distributed ledger technology: Blockchain compared to directed acyclic graph. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). Vienna, Austria, pp 1569–1570
35. Schollmeier R (2002) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proceedings First International Conference on Peer-to-Peer Computing. Linkoping, Sweden, pp 101–102
36. Wang W et al (2021) Blockchain-based reliable and efficient certificateless signature for IIoT devices. IEEE Trans Indust Inform. https://doi.org/10.1109/TII.2021.3084753
37. Bamakan SMH, Motavali A, Babaei Bondarti A (2020) A survey of blockchain consensus algorithms performance evaluation criteria. Expert Syst Appl 154:113385
38. Kim N, Nguyen G-T (2018) A survey about consensus algorithms used in blockchain. J Inf Process Syst 14(1):101–128
39. Zhang L et al (2021) Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing. Trans Emerg Telecommun Technol. https://doi.org/10.1002/ett.4315
40. 5GAA (2017) White Paper: toward fully connected vehicles: edge computing for advanced automotive communications. Available

from: https://5gaa.org/news/toward-fully-connected-vehicles-edge-computing-for-advanced-automotive-communications/
41. Olariu S (2019) A survey of vehicular cloud research: trends, applications and challenges. IEEE Trans Intell Transp Syst 21:2648–2663
42. Fernando N, Loke SW, Rahayu W (2013) Mobile cloud computing: a survey. Futur Gener Comput Syst 29(1):84–106
43. Lee E-K et al (2016) Internet of Vehicles: from intelligent grid to autonomous cars and vehicular fogs. Int J Distrib Sens Netw 12(9):155014771666550
44. Zhang J, Letaief KB (2020) Mobile edge intelligence and computing for the internet of vehicles. Proc IEEE 108(2):246–261
45. Hu VC et al (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. National Institute Standards and Technology NIST SP, NIST Special Publication, pp 800–162
46. Nkenyereye L et al (2019) Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing. Sensors 20(1):154
47. Bagga P et al (2020) Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges. IEEE Access 8:54314–54344
48. Das AK, Zeadally S, He D (2018) Taxonomy and analysis of security protocols for Internet of Things. Futur Gener Comput Syst 89:110–125
49. Sharma R and Chakraborty S (2018) B2VDM: blockchain based vehicular data management. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI). Bangalore, India, pp 2337–2343
50. Lei K et al (2020) Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks. J Grid Comput. https://doi.org/10.1007/s10723-020-09531-1
51. Ferdous MS et al (2020) Immutable autobiography of smart cars leveraging blockchain technology. Knowl Eng Rev 35:E3
52. Kong Q et al (2020) Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain. IEEE Trans Intell Transport Syst 22(8):4889–4898
53. Li M, Zhu L, Lin X (2019) Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. IEEE Internet Things J 6(3):4573–4584
54. Amiri WA, et al (2019) Privacy-preserving smart parking system using blockchain and private information retrieval. In: International Conference on Smart Applications, Communications and Networking (SmartNets). Sharm El Sheik, Egypt, pp 1–6
55. Hu J et al (2019) Parking management: a blockchain-based privacy-preserving system. IEEE Consum Electron Mag 8(4):45–49
56. Zhang C et al (2020) BSFP: blockchain-enabled smart parking with fairness, reliability and privacy protection. IEEE Trans Veh Technol 69(6):6578–6591
57. Dorri A et al (2017) BlockChain: a distributed solution to automotive security and privacy. IEEE Commun Mag 55(12):119–125
58. Iqbal S et al (2020) Blockchain-based reputation management for task offloading in micro-level vehicular fog network. IEEE Access 8:52968–52980
59. Gao J et al (2019) A Blockchain-SDN enabled internet of vehicles environment for fog computing and 5G networks. IEEE Internet Things J 7(5):4278–4291
60. Liu H, Zhang Y, Yang T (2018) Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Network 32(3):78–83
61. Wang Q et al (2020) TrafficChain: a blockchain-based secure and privacy-preserving traffic map. IEEE Access 8:60598–60612
62. Chen C et al (2020) Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. IEEE Trans Industr Inf 16(6):4122–4133
63. Chen B et al (2020) A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks. IEEE Trans Veh Technol 69(6):5813–5825
64. Rawat DB et al (2020) Blockchain enabled named data networking for secure vehicle-to-everything communications. IEEE Network 34:185–189
65. Yao Y et al (2019) BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet Things J 6(2):3775–3784
66. Kaur K, et al (2019) Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In: 2019 IEEE International Conference on Communications Workshops (ICC Workshops). 2019: Shanghai, China, pp 1–6
67. Shen H et al (2020) Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks. IEEE Internet Things J 7(7):6610–6622
68. Zhang P, Liu H and Zhang Y (2019) Blockchain enabled cooperative authentication with data traceability in vehicular edge computing. In: Computing, communications and IoT applications (ComComAp). Shenzhen, China, pp 299–304
69. Wang C et al (2020) B-TSCA: blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. IEEE Trans Emerg Top Comput. https://doi.org/10.1109/TETC.2020.2978866
70. Bonadio A et al (2019) An integrated framework for blockchain inspired fog communications and computing in internet of vehicles. J Ambient Intell Humaniz Comput 11(2):755–762
71. Huang XM et al (2020) Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. IEEE-CAA Journal of Automatica Sinica 7(2):426–441
72. Javaid U, Aman MN, Sikdar B (2020) A scalable protocol for driving trust management in internet of vehicles with blockchain. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.3002711
73. Zheng Z, Pan J, Cai L (2020) Lightweight blockchain consensus protocols for vehicular social networks. IEEE Trans Veh Technol 69(6):5736–5748
74. Chen C et al (2020) A secure content sharing scheme based on blockchain in vehicular named data networks. IEEE Trans Industr Inf 16(5):3278–3289
75. Kang J et al (2019) Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J 6(3):4660–4670
76. Lu Y et al (2020) Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans Veh Technol 69(4):4298–4311
77. Javed MU et al (2020) Blockchain-based secure data storage for distributed vehicular networks. Appl Sci 10(6):2011
78. Dai Y et al (2020) Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. IEEE Trans Veh Technol 69(4):4312–4324
79. Jeong BG et al (2020) Blockchain-based data sharing and trading model for the connected car. Sensors 20(11):3141
80. Javaid U, Aman MN and Sikdar B (2019) DrivMan: driving trust management and data sharing in VANETs with blockchain and smart contracts. In: IEEE 89th Vehicular Technology Conference (VTC2019-Spring). Kuala Lumpur, Malaysia, pp 1–5
81. Liu K et al (2019) A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles. IEEE Internet Things J 6(5):9098–9111

82. Sun G et al (2020) Blockchain enhanced high-confidence energy sharing in internet of electric vehicles. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.2992994
83. Firoozjaei MD, et al (2019) EVChain: a blockchain-based credit sharing in electric vehicles charging. In: 2019 17th International Conference on Privacy, Security and Trust (PST). Fredericton, NB, Canada, pp 1–5
84. Thakur S, Hayes B and Breslin JG (2018) A unified model of peer to peer energy trade and electric vehicle charging using blockchains. In: Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MEDPOWER 2018). Dubrovnik, Croatia, pp 1–6
85. Fu Z, Dong P, Ju Y (2020) An intelligent electric vehicle charging system for new energy companies based on consortium blockchain. J Clean Prod 261:121219
86. Xia S et al (2020) A Bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles. IEEE Trans Veh Technol 69(7):6856–6868
87. Zhou Z et al (2020) Secure and efficient vehicle-to-grid energy trading in cyber physical systems: integration of blockchain and edge computing. IEEE Trans Syst Man Cybernet 50(1):43–57
88. Hagenauer F, et al (2017) Vehicular micro clouds as virtual edge servers for efficient data collection. In: Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services - CarSys '17. New York, USA, pp 31–35
89. Zhang X, Li R and Cui B (2018) A security architecture of VANET based on blockchain and mobile edge computing. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). Shenzhen, China, pp 258–259
90. Buterin V (2014) A next-generation smart contract and decentralized application platform. White paper 3(37)
91. Wood G (2014) Ethereum: A secure decentralised generalised transactionledger. Ethereum Project Yellow Paper 151:1–32
92. Androulaki, E et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference, pp 1-15
93. Aggarwal, S et al (2021) Hyperledger. In Advances in Computers, Elsevier, 121:323–343
94. Androulaki E, et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference. pp 1–15
95. Yu FR (2018) vDLT: A service-oriented blockchain system with virtualization and decoupled management/control and execution. arXiv preprint arXiv:1809.00290
96. Yu FR et al (2018) Virtualization for distributed ledger technology (vDLT). IEEE Access 6:25019–25028
97. Jiang X et al (2020) Blockchain-enabled cross-domain object detection for autonomous driving: a model sharing approach. IEEE Internet Things J 7(5):3681–3692
98. TRUFFLE (2020) Sweet tools for smart contracts. Retrieved July 3, 2021, Available from: https://www.trufflesuite.com/truffle
99. Carneiro G (2010) NS-3: Network simulator 3. In: UTM Lab Meeting April, Vol 20, pp 4–5
100. Sommer C et al (2019) Veins: The open source vehicular network simulation framework. Recent advances in network simulation. Springer, Cham, pp 215–252
101. Dressler F et al (2011) Toward realistic simulation of intervehicle communication. IEEE Veh Technol Mag 6(3):43–51
102. Krajzewicz D et al (2012) Recent development and applications of SUMO-Simulation of Urban MObility. Int J Adv Syst Measur 5(3&4)
103. Sommer C, German R, Dressler F (2011) Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IEEE Trans Mob Comput 10(1):3–15
104. Borshchev A et al (2014) Multi-method modelling: AnyLogic. Discrete-event simulation and system dynamics for management decision making, pp 248–279
105. Konstantinou E (2002) A software library for elliptic curve cryptography. European Symposiumon Algorithms. Springer, Berlin, Heidelberg, pp 625–637
106. Ali I et al (2019) A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. J Syst Architect 99:101636
107. Bethencourt J et al (2011) Advanced crypto software collection: the cpabe toolkit. Available from: http://acsc.cs.utexas.edu/cpabe. Retrieved 3 July 2021
108. Feng Q et al (2020) BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Trans Industr Inf 16(6):4146–4155
109. Mendki P (2019) Blockchain Enabled IoT Edge Computing. In: ICBCT 2019: 2019 International Conference on Blockchain Technology 2019, Association for Computing Machinery: Honolulu, HI, USA, pp 66–69
110. Hammoud A et al (2020) AI, Blockchain, and vehicular edge computing for smart and secure IoV: challenges and directions. IEEE Internet Things Mag 3(2):68–73
111. Qu Y et al (2020) Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.2977383
112. Fu Y et al (2020) Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE Wirel Commun 27(2):197–203
113. Digiconomist. Bitcoin energy consumption index. 2020 [cited 2020 June 15]; Available from: https://digiconomist.net/bitcoin-energyconsumption#validation.
114. Shahid F, Khan A, Jeon G (2020) Post-quantum distributed ledger for internet of things. Comput Electr Eng 83:106581
115. Edwards M, Mashatan A, Ghose S (2020) A review of quantum and hybrid quantum/classical blockchain protocols. Quantum Inf Process 19(6):184

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.