Ad Hoc Networks 137 (2022) 102980

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Survey paper

Blockchain-based vehicular ad-hoc networks: A comprehensive survey

Sanjeev Kumar Dwivedi [a], Ruhul Amin [a], Ashok Kumar Das [b], Mark T. Leung [c], Kim-Kwang Raymond Choo [d,*], Satyanarayana Vollala [a]

[a] Department of Computer Science & Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, Chattisgarh 892002, India
[b] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[c] Department of Management Science and Statistics, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA
[d] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ARTICLE INFO

Keywords:
Blockchain
Security
Trust
VANETs

ABSTRACT

Vehicular ad-hoc networks (VANETs) are increasingly commonplace, partly due to the popularity of electric vehicles and the digitalization of cities. Data collected and shared in VANETs include traffic-related information, such as those relating to real-time traffic situations and road works. In recent times, there has been a trend of moving away from a centralized approach to a decentralized approach, for example, using Blockchain to facilitate secure data sharing and traceability of critical information. Hence, in this paper, we comprehensively survey the existing literature on blockchain-based VANET systems, focusing on the application of different blockchain technologies in different contexts, as well as the associated challenges and research opportunities.

1. Introduction

Advances in consumer technologies such as Internet-of-Things (IoT) and cloud computing have partly contributed to the reality of smart cities, which comprise systems such as intelligent transportation systems (ITS) and vehicular-ad-hoc networks (VANETs). VANETs, for example, support the communications of intelligent and connected vehicles (ICVs) with other infrastructures (e.g., roadside units (RSUs)) within the smart city and facilitates critical and safety-related applications. In other words, (near) real-time dissemination, mining, and analysis of information within the system are crucial. According to the IEEE 802.11p standard, the frequency of cooperative awareness messages should be in milliseconds [1]. However, various factors such as vehicular node cooperation, message security, service provider authenticity, and so on can have an adverse impact on the performance of message dissemination. For example, security requirements such as ensuring message and source authenticity can introduce additional delays. Hence, privacy and security are two key requirements in VANET-based applications, and example properties are as follow:

- Authentication: All the active entities (for instance, vehicles) must be verified before accessing the VANET system's services. Authentication provides the way by which malicious entities (or) adversaries cannot enter into the system.
- Non-repudiation: The vehicular nodes that participate in the data-sharing process cannot deny the data's operation. By using this, if any entity forwards the false message to other entities, at the later stage, they do not deny that it does not forward the particular message.
- Integrity: The event messages sent by one vehicular node to another are not modified by the participating entities or by the malicious entity. The received event message must be in the original form, as transmitted.
- Privacy: The identity of the vehicular nodes keeps private while transmitting the critical event messages to other vehicles and RSUs.
- Availability: Regardless of false events or poor conditions, the ICVs communicate essential event facts to others and roadside infrastructure at any time. They are also capable of dealing with the attacks while continuing to give their services.
- Confidentiality: Cryptographic primitives (for instance, encryption schemes and hash functions) are used by active entities for secret data transmission to others. As a result, the adversary does not retrieve the actual message.

[*] Corresponding author.
E-mail addresses: sanjeevdwivedi131988@gmail.com (S.K. Dwivedi), amin_ruhul@live.com (R. Amin), ashok.das@iiit.ac.in (A.K. Das), Mark.Leung@utsa.edu (M.T. Leung), raymond.choo@fulbrightmail.org (K.-K.R. Choo), satya4nitt@gmail.com (S. Vollala).

https://doi.org/10.1016/j.adhoc.2022.102980
Received 21 October 2021; Received in revised form 25 March 2022; Accepted 15 August 2022
Available online 27 August 2022

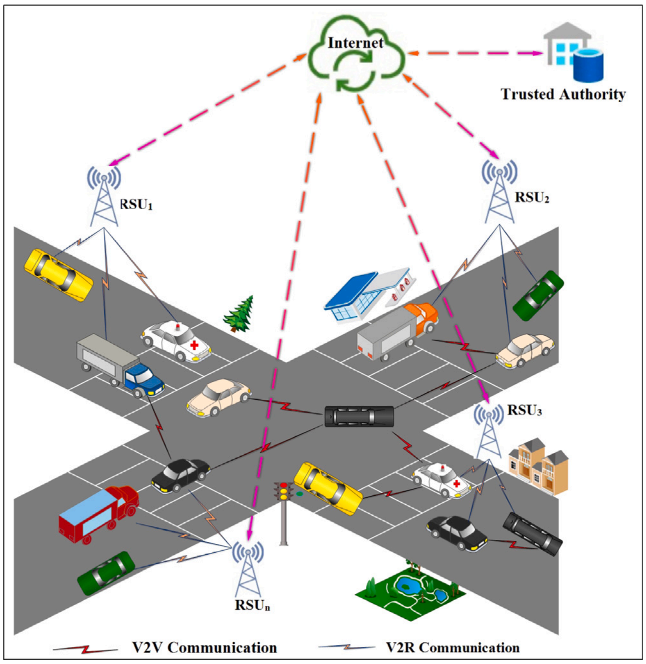

Fig. 1. Systematic architecture of VANET without blockchain.

- Traceability: This is the ability to trace the real identity of the vehicular node when it sends false information to others. Simultaneously, when the adversary captures the vehicular node, it changes the information and sends it to others.
- Efficiency: The critical event messages must be reached to the vehicles and RSUs in real-time so that they can analyze the event messages and take action accordingly.

In VANET, various security aspects such as authentication, confidentiality, integrity, trust, misbehavior detection, and attack detection have been investigated. However, different mechanisms are required to mitigate potential VANET attacks, and these security aspects are directly and indirectly related to each other. The amount of assurance with which a vehicular node accepts information from an arbitrary sender is determined by trust. The main objective of the vehicular network is vehicles can communicate with others and roadside infrastructures in such a way that safety-related information such as environmental hazards and weather reports are available in (near) real-time. In this regard, before disseminating and storing the information, the trust and reputation level of vehicular nodes must be computed. The trust models in the VANET system are broadly classified into three main categories, namely entity-centric trust model (EM), data-centric trust model (DM), and hybrid trust model (HM). The EM evaluates the trust level of vehicles (also known as vehicle trustworthiness) while considering the trust level of nearby vehicles. Similarly, the DM evaluates the trustworthiness of the received event messages from nearby vehicles. On the other hand, the HM mixes EM and DM. It uses both trust levels when determining the trustworthiness of event messages [2,3].

With the emergence of new technology, the vehicular network plays an essential role in saving the life of drivers by spreading critical messages [4]. According to the current scenario, three types of communication exist in the VANET system. The first type considers only vehicles, commonly known as vehicle-to-vehicle (V2V) communication [5]. V2V communication is performed by using the onboard unit (OBU). The second type of communication exists between the vehicles and RSUs, known as vehicle-to-infrastructure (V2I) communication. The RSUs have more computing and storage power than vehicles, which exist along the side of the road. The third type of communication exists between vehicles and pedestrians or cyclists, known as vehicle-to-everything (V2X) communication [6]. Here, everything represents as pedestrians, cyclists, etc. In principle, the VANET system does not follow any fixed topology or architecture. The general architecture of VANET without the blockchain mechanism is shown in Fig. 1. Moreover, the traditional VANET system mainly consists of three types of entities: vehicles, RSUs, and trusted authority (TA). The TA (or key generation center) registers the vehicles and RSUs before deploying them to the network. In the vehicle and RSU registration phase, the TA can store the sensitive parameters in its memory, generated at the registration time. The vehicle collects the crucial information from its surrounding area and delivers it to the nearby RSU. The RSU processes the information according to its requirement and then stores it to the centralized cloud server using various cryptographic primitives such as hashing, encryption, etc. Here, it is assumed that TA and centralized cloud servers are the trusted entities of the VANET network, and they never leak the information to the outsider (or) adversary [7]. These assumptions may not be suited for those real-life applications where the system wants to operate in a decentralized manner without the involvement of a single TA and single cloud server. Furthermore, the inherent assumption of single TA and single cloud servers uplifts the single-point-of-failure (SPoF) problem. As a result, a fully trusted system cannot be achieved. The blockchain is a better option to mitigate these issues, which the centralized VANET system faces. The typical architecture of the blockchain-based VANET system is shown in Fig. 2. In this architecture, the entire VANET system is divided into multiple vehicular domains that maintain the blockchain based on the access-control mechanism. In each vehicular domain, one TA is present to register the vehicles and RSUs. The TA creates a registration block for each deployed RSU and vehicle and stores it to the blockchain network by using the consensus mechanism (suited according to the VANET application). Whenever the vehicles send the crucial information to nearby RSU, the RSU can take advantage of blockchain for the authentication of vehicles (based on the merkle root) and then store this information to the blockchain. The advantages of using blockchain are as follows:

- Whenever vehicles move from one vehicular domain to next, the RSU of the next domain can consider the blockchain mechanism for vehicle authentication [8].
- The crucial information is stored via the blockchain mechanism. Therefore with the assistance of cryptographic features, inherent trust is achieved by the VANET system.
- The blockchain prevents the system from SPoF problem because each vehicular domain maintains its separate but the exact copy of the blockchain.

The advancement of the VANET system necessitates large-scale data exchange and storage capacity. Vehicles in the ITS often have restricted devices with limited computing and storage capacity. The usage of roadside infrastructure in conjunction with the cloud paradigm provides an alternate method of maintaining the exchange of information. Furthermore, because of vehicle's high mobility and volatility, it is also vulnerable to both internal and external attacks. Recently, blockchain technology has promised to overcome the constraints of the VANET system as well as the related threats. Blockchain is an immutable record of linked blocks that are implemented without the central authority or server [9]. The blockchain is an emerging area in the domain of data sharing and trust among the different nodes in the network. It appeals to both industry and academics in a variety of ways. Without a third party, it enables an immutable ledger, trust, decentralization, anonymity, and transparency. In blockchain applications, a cryptographic chained structure of blocks with consensus and smart contracts mechanism is utilized, which can give better security than the existing system. All nodes achieve a shared consensus using Smart contracts, where its execution is immutable. As a result, it prohibits data tampering in the system [10]. To offer readers a full assessment

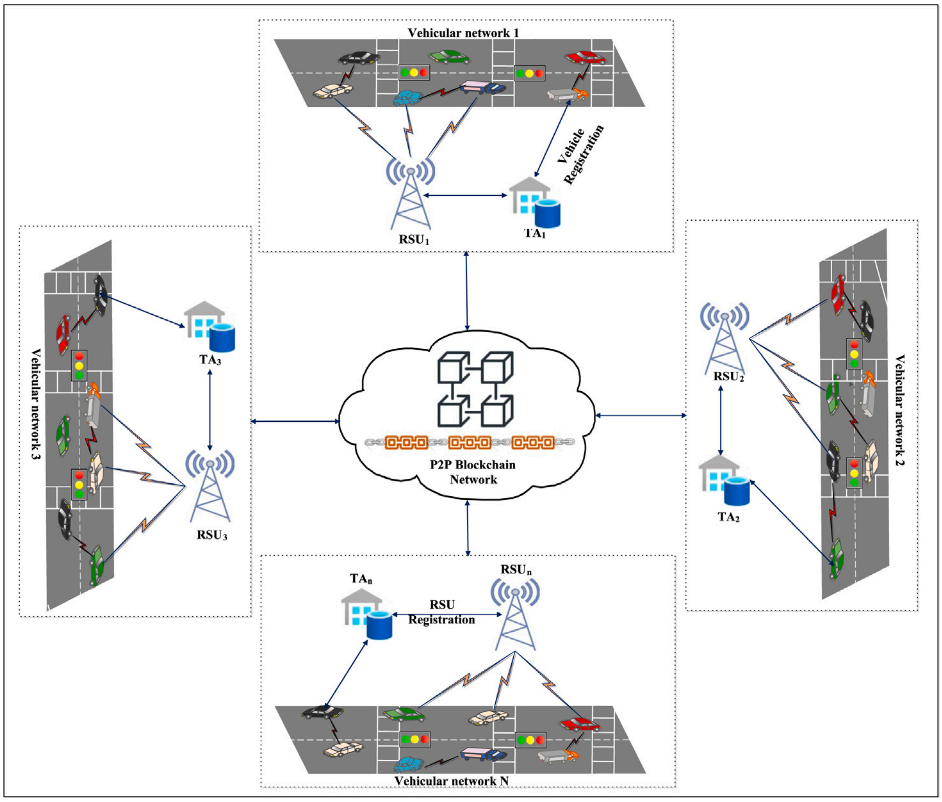

Fig. 2. Systematic architecture of VANET with blockchain mechanism.

of the most recent research on security and trust solutions based on blockchain for the VANET system, it is necessary to systematically investigate and analyze them in a holistic fashion. To fill this gap, this article presents a comprehensive survey of blockchain and VANET integration. This paper aims to investigate the current research trends on the usage of blockchain technology in the VANET system. The paper presents the following novelties: (1) it covers the integration of blockchain technology in different domains, including the various characteristics of blockchain, smart contract and consensus algorithm (2) provide an in-depth study of various articles that used blockchain technology to overcome the problems of traditional VANET system (3) the cutting-edge research, and the insightful discussion according to the various categories of solutions are presented. (4) Moreover, based on the discussion on state-of-the-art research, this paper also presents the learned lessons and highlights open research challenges that can be useful for the researchers to put their efforts.

In our research, we located a number of related literature survey/review articles with different focuses (e.g., see [11,12]). For example, a brief survey on the bitcoin cryptocurrency was presented in [11], whereas in [13–15] the authors focused on the various consensus protocols utilized in existing blockchains. The fundamental structure of the bitcoin protocol was investigated in [16]. The security, privacy, and anonymity implications associated with the use of blockchain technology were investigated in [17–23].

Some authors have focused on specific application domains of blockchain, and examples include the works mentioned in [24–27]. Example applications include the integration and/or application of blockchain products (e.g., smart contracts) with/for IoT systems in [12, 28–39], healthcare applications of blockchain [40–43], the potential of blockchain in supporting edge computing systems [44,45], blockchain in 5G applications [46,47], the application of blockchain in industry 4.0 contexts [48–52], aerospace and defense blockchain-based applications [53], the application of blockchain to protect multimedia contents [54], etc [55,56]. Security of blockchain-based applications has also been the subject of a number of studies, such as those presented in [57–69]. A comprehensive review of sidechains and their platforms was presented in [70], and Xu et al. [71] studied the performance of hyper-ledger fabric blockchain networks. Not surprisingly, given the recent interest in AI, there have also been reviews/surveys focusing on the adoption of AI in blockchain-based systems [72–74]. Closer to the theme of this paper, Gupta et al. [75] studied various blockchain-assisted unmanned aerial vehicles (UAV) communications in a 6 G environment. However, we observe that there is no existing review/survey on blockchain-based VANET systems — see Tables 1 and 2; thus, the focus of this paper.

The main contributions of the paper are:

✓ To the best of our knowledge, this is the first study summarizing various trust models adopted in the VANET system based on the blockchain mechanism.

✓ This paper briefly discusses the blockchain, its features, blockchain types, smart contracts, consensus algorithm, why blockchain is suitable for the VANET, and how this mechanism solves the problem of traditional centralized VANET system.

✓ This paper highlights the related surveys in the blockchain field and provides an overview of the integration of blockchain technology in different application domains, e.g., healthcare, supply chain, etc. To fill the aforementioned gap in the world of literature, this comprehensive survey puts a special focus on blockchain technology in vehicular system.

✓ We develop a taxonomic framework and classify existing solutions, which incorporate blockchain in the vehicular network, into the six main categories: incentive mechanism, data-sharing models, trust establishment, authentication mechanism, privacy-preserving models, and smart contracts based system.

✓ We provide a state-of-the-art comparison of different categories of the presented solutions in a tabular form, concerning the specific goals, blockchain model, technology adopted, performance, strengths, weaknesses and attack counteracted.

Table 1
Related blockchain reviews/surveys: A snapshot.

S.No.	Year	Author	Major objectives
1.	2016	Tschorsch et al. [16]	Fundamental structure of the bitcoin protocol and its application.
2.	2016	Christidis et al. [30]	In-depth study of blockchain and smart contracts for IoT.
3.	2017	Kaushik et al. [11]	Brief survey on the bitcoin cryptocurrency.
4.	2017	Atzei et al. [12]	Focused on security vulnerabilities on smart contracts.
5.	2017	Sankar et al. [13]	Brief overview of consensus protocol.
6.	2017	Lin et al. [19]	A survey of blockchain security and challenges.
7.	2017	Li et al. [21]	Security threats and possible solutions in blockchain.
8.	2017	Yeow et al. [38]	Decentralized consensus and research issue for IoT.
9.	2018	Khalilov et al. [17]	A detailed investigation on security and anonymity in bitcoin digital cash system.
10.	2018	Conti et al. [18]	Security and privacy aspect of bitcoin cryptocurrency.
11.	2018	Zheng et al. [22]	Survey on blockchain challenges and its possible opportunities.
12.	2018	Fernández et al. [24]	Survey on blockchain-based IoT system.
13.	2018	Panarello et al. [25]	Survey on blockchain with the integration of IoT and its application.
14.	2019	Ali et al. [26]	Comprehensive survey on blockchain technology in IoT.
15.	2018	Ferrag et al. [33]	Comprehensive study of the blockchain protocol for IoT and research challenges.
16.	2018	Reyna et al. [36]	Challenges and opportunities while integrating blockchain with IoT.
17.	2019	Feng et al. [20]	A survey on privacy protection in blockchain system.
18.	2019	Lu et al. [23]	State-of-the-art and research challenges of blockchain.
19.	2019	Dai et al. [31]	Review on blockchain of thing and research issue for the next-generation networks.
20.	2019	Nguyen et al. [35]	Review on the integration of blockchain in the cloud of things.
21.	2018	Esposito et al. [32]	A study on blockchain for cloud-based healthcare data security and privacy.
22.	2019	Zou et al. [39]	Challenges and opportunities for development of smart contracts.
23.	2019	Aggarwal et al. [28]	Study on blockchain for smart communities.
24.	2019	Tanwar et al. [72]	A comprehensive study on machine learning adoption in blockchain-based smart applications.
25.	2019	Salah et al. [74]	Open research challenges for blockchain and artificial intelligence (AI).
26.	2019	McGhin et al. [40]	Research challenges and opportunities for Blockchain in healthcare applications.
27.	2019	Yang et al. [44]	A survey on integration of blockchain and edge computing systems.
28.	2019	Liu et al. [63]	A survey on security verification of blockchain smart contracts.
29.	2019	Chaer et al. [46]	Opportunities and challenges for blockchain for $5G$.
30.	2019	Xie et al. [67]	In-depth study of survey of blockchain technology for smart cities applications.
31.	2019	Yang et al. [68]	A comprehensive survey on blockchain-enabled internet service architecture.
32.	2019	Hassan et al. [61]	Challenges and solutions for blockchain technologies for smart energy systems.
33.	2019	Alladi et al. [48]	A review on blockchain applications for industry 4.0 and industrial IoT (IIoT).

Table 2
Related surveys on blockchain: A snapshot (Cont...)

S.No.	Year	Author	Major objectives
34.	2020	Xie et al. [27]	Review on integration of blockchain with cloud exchange with future research directions.
35.	2020	Kumar et al. [73]	Study on blockchain, big data, and machine learning technologies.
36.	2020	Kumari et al. [76]	Study on integration of blockchain and artificial intelligence for energy cloud management.
37.	2020	Ray et al. [41]	A detailed investigation on blockchain for IoT-based healthcare.
38.	2020	Shi et al. [42]	A survey of blockchain technology in electronic health record system.
39.	2020	Bhattacharya et al. [45]	A survey on mobile edge computing-enabled blockchain framework.
40.	2020	Bao et al. [57]	A survey of blockchain technology in the energy sector.
41.	2020	Miglani et al. [65]	In-depth study on blockchain for internet-of-energy (IoE) management.
42.	2020	Thakker et al. [66]	Study of blockchain for diamond industry.
43.	2020	Bodkhe et al. [49]	A comprehensive review on blockchain for industry 4.0.
44.	2020	Gupta et al. [51]	A systematic review on integration of blockchain and autonomous vehicles for industry 4.0.
45.	2020	Mistry et al. [47]	A systematic review on blockchain for $5G$-enabled IoT for industrial automation.
46.	2020	Ghosh et al. [60]	Study on Security and challenges of Cryptocurrencies in blockchain technology.
47.	2020	Bodkhe et al. [50]	A survey on decentralized consensus schemes for cyber–physical systems.
48.	2020	Taylor et al. [52]	A review of blockchain for cyber security applications.
49.	2020	Choo et al. [29]	Review on integration of blockchain with industrial IoT (IIoT) with research challenges.
50.	2020	Singh et al. [70]	A comprehensive review of the state-of-the-art sidechains and its platforms.
51.	2020	Liu et al. [77]	Study on blockchain-based identity management systems.
52.	2021	Bouraga et al. [14]	A surveying on classification of blockchain consensus protocol.
53.	2021	Ferdous et al. [15]	Study on consensus algorithm for crypto-currencies in public blockchain.
54.	2021	Wang et al. [37]	In-depth study on security of ethereum smart contract.
55.	2021	Hu et al. [34]	A comprehensive survey on smart contracts construction and its execution.
56.	2021	Yaqoob et al. [43]	In-depth study of adoption of blockchain technology in healthcare data management.
57.	2021	Chen et al. [59]	A comprehensive survey on integration of blockchain into the mobile crowd-sensing application.
58.	2021	Khoshavi et al. [62]	A survey on blockchain applications in transportation systems.
59.	2021	Berdik et al. [58]	Comprehensive survey on blockchain for information systems management and its security.
60.	2021	Ahmad et al. [53]	In-depth study on blockchain for aerospace and defense.
61.	2021	Xu et al. [71]	Performance analysis of hyper-ledger fabric blockchain network.
62.	2021	Qureshi et al. [54]	Study on blockchain based multimedia content protection with open challenges.
63.	2021	Gupta et al. [75]	Study of blockchain assisted UAV communications in $6G$ environment.
64.	2021	Majeed et al. [64]	Recent advancement and future challenges on blockchain for IoT-based smart cities.
65.	2021	Yu et al. [69]	A review on the security challenges of blockchain in IoT-based smart cities application.
66.	2021	Li et al. [55]	A survey on blockchain-empowered Data-driven Networks.
67.	2021	Huang et al. [56]	A comprehensive survey on theories, modelings, and tools of blockchain.
68.	2021	Dabbagh et al. [78]	A surveying on performance evaluation with the challenges of permissioned blockchain platforms.
69.	2021	Ante et al. [79]	Analysis of adoption of blockchain technology in energy sector.

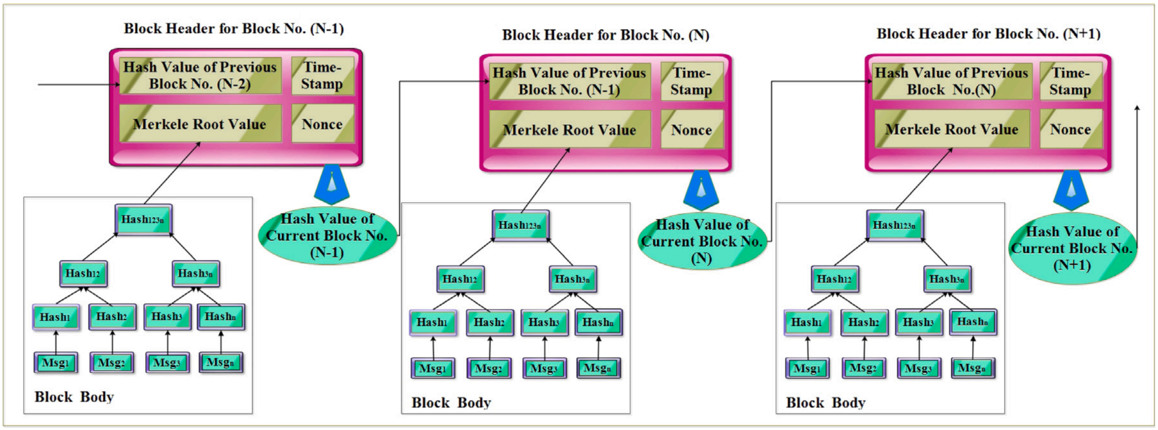
Block Header for Block No. (N-1)
Hash Value of Previous Block No. (N-2)
Time-Stamp
Merkele Root Value
Nonce
Hash Value of Current Block No. (N-1)
Hash$_{123n}$
Hash$_{12}$
Hash$_{3n}$
Hash$_1$
Hash$_2$
Hash$_3$
Hash$_n$
Msg$_1$
Msg$_2$
Msg$_3$
Msg$_n$
Block Body
Block Header for Block No. (N)
Hash Value of Previous Block No. (N-1)
Time-Stamp
Merkele Root Value
Nonce
Hash Value of Current Block No. (N)
Block Body
Block Header for Block No. (N+1)
Hash Value of Previous Block No.(N)
Time-Stamp
Merkele Root Value
Nonce
Hash Value of Current Block No. (N+1)
Block Body

Fig. 3. The structure of a block in blockchain.

✓ Based on our comprehensive survey, this paper provides the open research issues and highlighted issues that can be useful for the development of a blockchain-based VANET system.

The rest of the paper is organized as follows. Section 2 gives a brief overview of blockchain, blockchain features, different types of blockchain, smart contract mechanism, and consensus algorithm used in various types of blockchains. Section 3 describes the related works based on the blockchain mechanism in the VANET system along with the blockchain-related challenges, benefits, and shortcomings. The literature of the paper is classified into six major categories: data sharing mechanism, incentive mechanism, etc. The discussion on the relevant security attacks exist in the VANET system is presented in Section 4. Section 5 presents the highlighted issues from the state-of-the-art research. The open research issues for the VANET infrastructure, including the internet-of-vehicle (IoV), are presented in Section 6. Finally, Section 7 concludes this paper and outlines potential future research opportunities.

2. Background: Blockchain

2.1. Basics

Unlike traditional mechanisms, blockchain technology enables the peer-to-peer exchange of digital assets without the intervention of the third user [80]. Blockchain technology was initially created to support one of the famous cryptocurrencies known as bitcoin [81]. Bitcoin enables an innovative platform to exchange transactions without the involvement of the central authority [19]. The participating nodes in the blockchain are distributed across the network, and there is no central authority that can control it. The elimination of central authority provides trust among all the peers in the blockchain-based network [82].

2.2. Blockchain features

Blockchain mechanism provides the following features: [83,84]

- **Immutability:** Immutability is the core feature of the blockchain mechanism. In the blockchain mechanism, a block is connected with the previous block by utilizing the hash value of the previous block, as shown in Fig. 3. From an adversary perspective, it is impossible to change the hash of all subsequent blocks that are stored in the distributed nodes. Therefore, blocks have become immutable in the blockchain-based system.
- **Distributed-Nature:** Blockchain technology works in a distributed nature. In the blockchain-based system, all the nodes have the same and an updated copy of the blockchain. Therefore, if a few nodes deny that they do not have a consistent copy of the blockchain, the entire process still works [85].
- **Anonymity:** In the blockchain, each network node is linked with the anonymous address (hash of the public key with random value). Therefore, nodes can be anonymous when they exchange resources with the other nodes of the network. As a result, the privacy of each node can be preserved to some extent [86].
- **Trust-less Environment:** Due to the distributed nature, the blockchain mechanism eliminates the central authority and prevents the system from the SPoF problem. It provides trust among all the peer nodes globally distributed across the network and creates a trustless environment across the blockchain network.
- **Transparency:** The blocks (or data) in the blockchain mechanism are utterly transparent [87], as every individual node stores the identical and updated copy of the blockchain, and it is entirely transparent to each peer node in the network.
- **Privacy:** In a blockchain mechanism, any user joins the network, and the personal information of the user is completely anonymous [88]. It means that the users in the network cannot predict the personal information of other users, as it involves cryptographic primitives to preserve the user's identity.
- **Smart Contracts:** Instead of using the legal language, it uses the computer language (known as program or script) for writing the contracts. When the predefined conditions are met, the computer automatically executes digital contracts. As a result, it reduces the cost of contract signing, and its supervision [89].
- **Autonomy:** The blockchain uses consensual protocols to add and store any block in its decentralized network. These protocols are open and transparent that allows the nodes to securely exchange information.
- **Chronological & Time-stamped:** The data blocks are time-stamped, and the current block is linked with the previous one. The cryptographically secured hash functions are used for this. As a result, if an attacker succeeds in tempering to any block, all the successor blocks followed by the tempered block becomes invalidated [90].
- **Exchanges Automation:** By writing the smart contracts, the exchange of resources among the blockchain network nodes can be automated. Therefore, various services are automatically deployed into the network without human intervention.

2.3. Types of blockchain

The blockchain is broadly classified into three types: (1) permissionless blockchain, (2) permissioned blockchain, and (3) consortium blockchains [91]. Any node can join the network and perform the transaction with any other network nodes in a permissionless blockchain. Due to this reason, permissionless blockchains are also called open blockchains (or public blockchain). For joining the open blockchain,

Table 3
Comparisons among permissionless blockchain, consortium blockchain and permissioned blockchain.

S.No.	Property	Permissionless blockchain	Consortium blockchain	Permissioned blockchain
1.	Decentralization/Centralized	Decentralized	Partially decentralized	Centralized
2.	Permissionless/Permissioned	Permissionless	Permissioned	Permissioned
3.	Immutable/Alterable	Immutable	Partially immutable	Alterable
4.	Refusable/Nonrefusable	Nonrefusable	Partially refusable	Refusable
5.	Transparent/Opaque	Transparent	Partially transparent	Opaque
6.	Traceable/nontraceable	Traceable	Partially traceable	Traceable
7.	Consensus determination	All the miner nodes	Selected set of nodes	One organization
8.	Consensus process	PoW, PoS	PBFT, PoA, PoET	Ripple
9.	Efficiency	Low	High	High
10.	Flexibility	Low	Medium	High
11.	Scalability	Low	Medium	High
12.	Examples	Bitcoin, Ethereum	Hyperledger, Ethereum	GemOS, Multichain

approval from any central authority is not required [92]. On the other hand, permissioned blockchains are managed by administrators, and they handle the entire network. Generally, it is based on the access control mechanism, and this mechanism defines whether the participating nodes have the full rights to view or write or perform the transactions with other nodes [22]. Due to this, the permissioned blockchains are also called closed blockchains (or private blockchain). Since administrators manage the permissioned blockchain, it converges in the centralization system and may be vulnerable to the SPoF problem [67]. The permissionless blockchains are based on distributed and decentralized blockchains, so the SPoF problem never exists. The famous bitcoin-cryptocurrency is the application of permissionless blockchain. In contrast, consortium blockchains sit in limbo between permissionless and permissioned blockchains. It is faster than the other two types of blockchains and more efficient in terms of scalability and flexibility. Table 3 summarizes the comparison of three types of blockchains [31].

2.4. Smart contracts and consensus algorithms used in blockchain

Smart contracts are a piece of code (program or scripts) that are written in a high-level programming language such as Java, C++, NodeJS, Python, Go, solidity, etc. [93,94]. Various blockchain platforms use different high-level languages for the execution of smart contracts. Hyperledger fabric platform uses NodeJS, python, Go programming language; whereas, ethereum uses solidity programming language for its smart contracts [12]. On the other hand, the consensus algorithm decides the block-validation process for a new block. Generally, a consensus algorithm is the set of rules to reach into a common viewpoint or agreement [95]. The consensus algorithm is designed in such a way that after the execution of the block, the majority of nodes in the network agree that the block is valid. Once consensus has been achieved, then the block is included in the blockchain [96]. After this agreement, no node denies that block is not valid and hence rejects from the blockchain. There are many consensus algorithms are available proof-of-work (PoW), proof-of-stake (PoS), Raft, byzantine fault tolerance (BFT), practical byzantine fault tolerance (PBFT), etc. [80,97]. The Bitcoin cryptocurrency uses the PoW algorithm.

3. Blockchain-based security solutions for VANETs

In blockchain-based systems, blocks are connected with the previous block, using the hash value of previous blocks. Due to this, blockchain provides immutable blocks. Table 4 specifies the consensus algorithms that are adopted in each of the presented solutions. In Table 5, we try to summarize the implementation-level of the existing solutions. The meaning of hyphens [-] is the non-adoption of a certain level of implementation. As shown in Fig. 4, the survey on blockchain-based VANET system is classified into the six major categories: incentive (reward, cryptocurrency, credit-based), data-sharing mechanism (announcement message, traffic events), trust-establishment (entity, hybrid), authentication (ECSDA, MAC), privacy-preserving (anonymity), and smart-contracts based system.

3.1. Incentive mechanisms

The effectiveness of the blockchain-based VANET system depends on the cooperation of vehicular nodes. When vehicles detect any abnormal situation (for instance, an accident on the road), they must send this crucial information to the other vehicles and RSU. The recipient vehicle and RSU can take the appropriate action, such as divert the route. But unfortunately, the data collection and forwarding in such a system is done in an uncooperative manner which leads to disturbing the whole V2V communication process.

To make the V2V communication more robust, the unselfish nodes are incentivized, which are continuously engaged in the communication process and ready with their computational and storage resources. Incentive mechanisms encourage the vehicular nodes to take part in the data collection and are ready to share their computational and storage resources. The incentive mechanism is broadly classified into two types: credit-based incentive and reputation-based incentive. Generally, in the credit-based system, a central authority assigns virtual currency to each user that can be useful for future transactions. In a reputation-based system, each user's reputation score is assigned according to its honesty and gets rewarded.

To achieve efficient vehicle cooperation and data forwarding in V2V communication, various authors adopted the incentive mechanism in their model. To solve the announcement message problem in internet-of-vehicle (IoV), the authors in [98] suggested the punish–reward mechanism. In their mechanism, if any vehicle broadcasts the true announcement message, the vehicle is rewarded with some cryptocurrency. They termed this cryptocurrency as Vcoin. On the contrary, if the message is found to be fake, the vehicle (announcement message generator) should be punished. The authors divided the whole region of IoV into multiple sub-regions. There are two blockchains present in their system: the parent blockchain and the auxiliary blockchain. The parent blockchain is only one, and all the entities in the system maintain it. There is a single auxiliary blockchain for each region, and all the entities within the region maintain this blockchain. Entities generate four types of messages: announcement messages, reward message generation, punishment message generation, and transaction message generation. Smart contracts, which are deployed into the parent blockchain, will help to maintain the consistency of data between parent and auxiliary blockchain.

Authors in [101] proposed the CreditCoin system based on vehicular announcement aggregation protocol to motivate the vehicles and to forward the announcement messages across the network. The CreditCoin protocol is divided into the two-phase: the first phase is called an announcement protocol, where a group of vehicles sends the traffic information to other vehicles and RSUs. The second phase is called an incentive mechanism where reliable vehicles get the reward (they referred to as coins) based on the authenticity of the announcement message. Vehicles send the information to the RSUs, and then RSUs are voted for the validity of the information.

The credibility of the vehicles and vehicle messages are the crucial factors in the vehicular network when vehicles communicate with

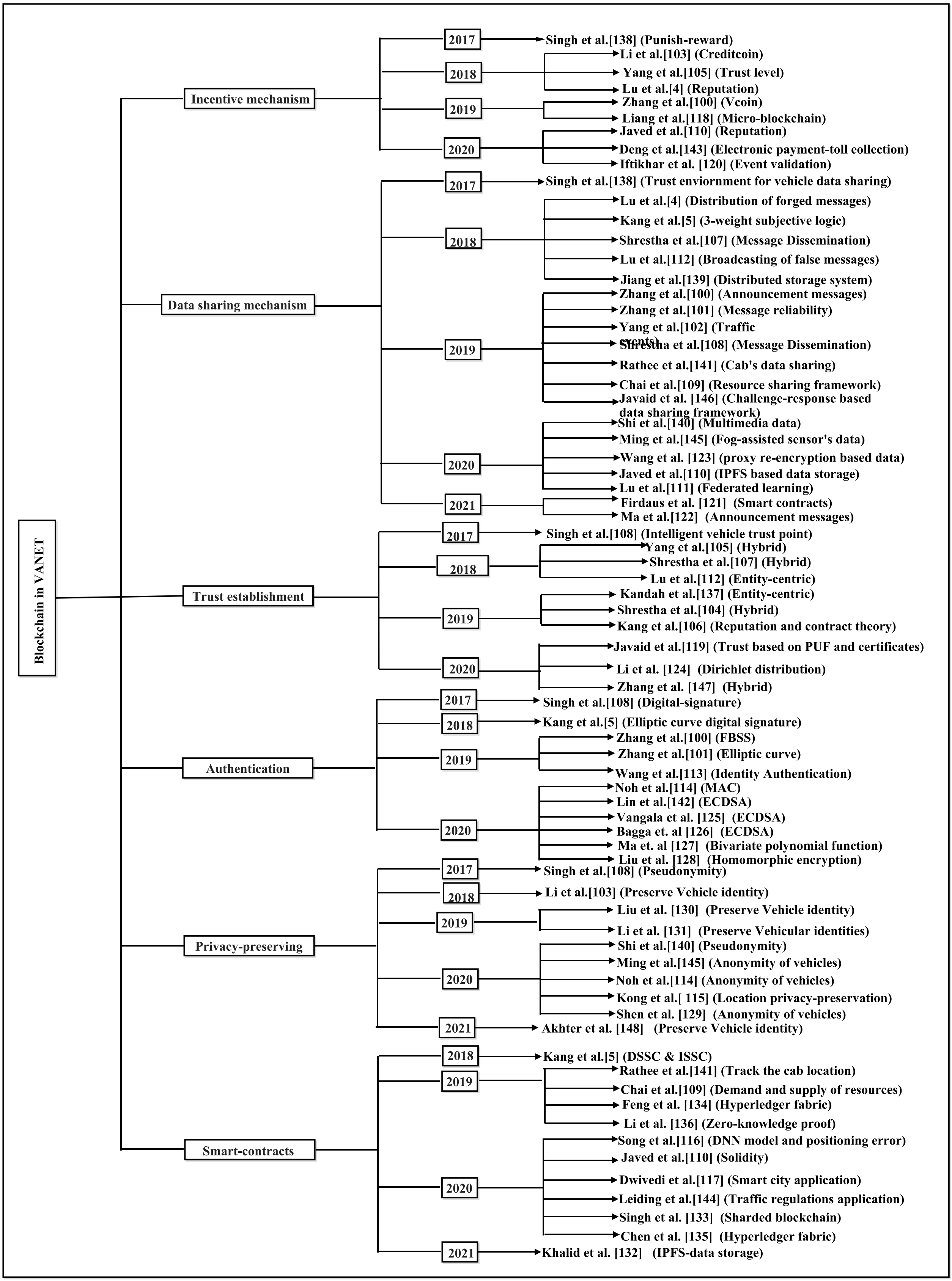
Blockchain in VANET
Incentive mechanism
2017
Singh et al.[138] (Punish-reward)
2018
Li et al.[103] (Creditcoin)
Yang et al.[105] (Trust level)
Lu et al.[4] (Reputation)
2019
Zhang et al.[100] (Vcoin)
Liang et al.[118] (Micro-blockchain)
2020
Javed et al.[110] (Reputation)
Deng et al.[143] (Electronic payment-toll eollection)
Iftikhar et al. [120] (Event validation)
Data sharing mechanism
2017
Singh et al.[138] (Trust enviornment for vehicle data sharing)
2018
Lu et al.[4] (Distribution of forged messages)
Kang et al.[5] (3-weight subjective logic)
Shrestha et al.[107] (Message Dissemination)
Lu et al.[112] (Broadcasting of false messages)
Jiang et al.[139] (Distributed storage system)
2019
Zhang et al.[100] (Announcement messages)
Zhang et al.[101] (Message reliability)
Yang et al.[102] (Traffic events)
Shrestha et al.[108] (Message Dissemination)
Rathee et al.[141] (Cab's data sharing)
Chai et al.[109] (Resource sharing framework)
Javaid et al. [146] (Challenge-response based data sharing framework)
2020
Shi et al.[140] (Multimedia data)
Ming et al.[145] (Fog-assisted sensor's data)
Wang et al. [123] (proxy re-encryption based data)
Javed et al.[110] (IPFS based data storage)
Lu et al.[111] (Federated learning)
2021
Firdaus et al. [121] (Smart contracts)
Ma et al.[122] (Announcement messages)
Trust establishment
2017
Singh et al.[108] (Intelligent vehicle trust point)
2018
Yang et al.[105] (Hybrid)
Shrestha et al.[107] (Hybrid)
Lu et al.[112] (Entity-centric)
2019
Kandah et al.[137] (Entity-centric)
Shrestha et al.[104] (Hybrid)
Kang et al.[106] (Reputation and contract theory)
2020
Javaid et al.[119] (Trust based on PUF and certificates)
Li et al. [124] (Dirichlet distribution)
Zhang et al. [147] (Hybrid)
Authentication
2017
Singh et al.[108] (Digital-signature)
2018
Kang et al.[5] (Elliptic curve digital signature)
2019
Zhang et al.[100] (FBSS)
Zhang et al.[101] (Elliptic curve)
Wang et al.[113] (Identity Authentication)
2020
Noh et al.[114] (MAC)
Lin et al.[142] (ECDSA)
Vangala et al. [125] (ECDSA)
Bagga et. al [126] (ECDSA)
Ma et. al [127] (Bivariate polynomial function)
Liu et al. [128] (Homomorphic encryption)
Privacy-preserving
2017
Singh et al.[108] (Pseudonymity)
2018
Li et al.[103] (Preserve Vehicle identity)
2019
Liu et al. [130] (Preserve Vehicle identity)
Li et al. [131] (Preserve Vehicular identities)
2020
Shi et al.[140] (Pseudonymity)
Ming et al.[145] (Anonymity of vehicles)
Noh et al.[114] (Anonymity of vehicles)
Kong et al.[115] (Location privacy-preservation)
Shen et al. [129] (Anonymity of vehicles)
2021
Akhter et al. [148] (Preserve Vehicle identity)
Smart-contracts
2018
Kang et al.[5] (DSSC & ISSC)
2019
Rathee et al.[141] (Track the cab location)
Chai et al.[109] (Demand and supply of resources)
Feng et al. [134] (Hyperledger fabric)
Li et al. [136] (Zero-knowledge proof)
2020
Song et al.[116] (DNN model and positioning error)
Javed et al.[110] (Solidity)
Dwivedi et al.[117] (Smart city application)
Leiding et al.[144] (Traffic regulations application)
Singh et al. [133] (Sharded blockchain)
Chen et al. [135] (Hyperledger fabric)
2021
Khalid et al. [132] (IPFS-data storage)

Fig. 4. Blockchain-based applications in VANET system.

Table 4
Consensus algorithms adopted in the literature.

S.No.	Papers	Consensus algorithm
1.	Zhang et al. 2019 [98]	Proof-of-work algorithm
2.	Zhang et al. 2019 [99]	Practical byzantine fault tolerance algorithm
3.	Yang et al. 2019 [100]	Proof-of-event algorithm
4.	Li et al.2018 [101]	Byzantine fault tolerance algorithm
5.	Shrestha et al. 2019 [102]	Proof-of-work algorithm
6.	Yang et al. 2018 [103]	Proof-of-work algorithm
7.	Lu et al. 2018 [2]	Proof-of-work algorithm
8.	Kang et al. 2018 [3]	Variant of byzantine fault tolerance algorithm
9.	Kang et al. 2019 [104]	Delegated proof-of-stake algorithm
10.	Shrestha et al. 2018 [105]	Proof-of-work algorithm
11.	Singh et al. 2017 [106]	Proof-of-driving algorithm
12.	Chai et al. 2019 [107]	Proof-of-reputation algorithm
13.	Javed et al. 2020 [108]	Proof-of-authority algorithm
14.	Lu et al. 2020 [109]	Delegated proof-of-stake algorithm
15.	Lu et al. 2018 [110]	Proof-of-presence, proof-of-absence algorithm
16.	Wang et al. 2019 [111]	Variant of byzantine fault tolerance algorithm
17.	Noh et al.2020 [112]	PoW and PBFT algorithm
18.	Kong et al. 2020 [113]	Byzantine fault tolerance algorithm
19.	Song et al. 2020 [114]	Delegated proof-of-stake algorithm
20.	Dwivedi et al. 2020 [115]	Proof-of-work algorithm
21.	Liang et al. 2019 [116]	Practical byzantine fault tolerance algorithm
22.	Javaid et al. 2020 [117]	Dynamic proof-of-work algorithm
23.	Iftikhar et al. 2020 [118]	Proof-of-authority algorithm
24.	Firdaus et al. 2021 [119]	Practical byzantine fault tolerance algorithm
25.	Ma et al. 2021 [120]	Proof-of-storage algorithm
26.	Wang et al. 2020 [121]	Ripple consensus
27.	Li et al. 2020 [122]	Improvement of Practical byzantine fault tolerance algorithm
28.	Vangala et al. 2020 [123]	Practical byzantine fault tolerance algorithm
29.	Bagga et al. 2020 [124]	Practical byzantine fault tolerance algorithm
30.	Ma, et. al 2020 [125]	Proof-of-work algorithm
31.	Liu et al. 2020 [126]	Practical byzantine fault tolerance algorithm
32.	Shen et al. 2020 [127]	Proof-of-stake algorithm
33.	Liu et al. 2019 [128]	Combination of proof-of-work algorithm and practical byzantine fault tolerance algorithm
34.	Li et al. 2019 [129]	Proof-of-work algorithm
35.	Khalid et al. 2021 [130]	Proof-of-work algorithm
36.	Singh et al. 2020 [131]	Authoritative consensus algorithm
37.	Feng et al. 2019 [132]	Practical byzantine fault tolerance algorithm
38.	Chen et al. 2020 [133]	Proof-of-work algorithm (or) practical byzantine fault tolerance algorithm, depends on environment
39.	Li et al. 2019 [134]	Proof-of-authority algorithm

road segments and RSU. The intelligent vehicles collected the information and forwarded it to other segments of the VANET system. In this context, authors in [103] proposed the blockchain technology enabled decentralized trust management system. They utilized the Bayesian Inference Mathematical Model to validate the received messages which vehicles get from the neighboring vehicles. The working of the proposed method is divided into the four significant steps: Rating generation by vehicles and uploaded into the neighboring RSUs, calculation of the trust value offset by RSUs, miner selection, new block generation process, and distributed consensus (synchronize with other RSUs) procedure. The advantage of the proposed scheme is that along with the vehicle's message, they also consider the vehicle's trust level. Due to this, malicious vehicles cannot participate in the block generation process.

The malicious vehicles send the forged message to road segments and RSU to mislead the communication process. As a result, inappropriate actions are taken place. To prevent the distribution of forged messages from vehicles in the VANET system, Zhaojun Lu et al. [2] proposed the blockchain-based anonymous reputation system (BARS) based on the reputation evaluation algorithm. The reputation evaluation algorithm considers both the historical interaction among vehicles and indirect opinions about the particular vehicle. The law enforcement authority (LEA) evaluates the reputation score of each vehicle, and based on this score; vehicles are also rewarded. The reputation evaluation algorithm considers the three aspects of the broadcast message: first, if authentication is true to the transmitted message, the reputation score of the concerned vehicle increase, otherwise decrease. Also, the vehicles who expose malicious vehicles, their reputation score is increased. The authors also propose the privacy-preserved authentication algorithm for the validation of the identity of the vehicle.

In [136], authors proposed the reward (incentive) based vehicles communication, and it is a combination of communication network-enabled devices such as vehicles, smartphones, etc., cloud computing, blockchain technology. They present a seven-layer model named the physical layer, data layer, network layer, handshake layer, reward layer, presentation layer, and service layer. The reward layer deals with the incentive mechanism among all those seven layers. To achieve transparency in the system, authors in [108] proposed the incentive and reputation mechanism-based blockchain for the vehicular network. The edge service providers are also used for the smooth functioning of the system. Interplanetary file system (IPFS) (distributed file storage system) is used to store the huge amount of data which are generated by the smart vehicles. The IPFS easily solves the issues related to the centralized architecture, such as data tampering, etc.

ITS provides various services to the passengers and drivers, and according to the vehicle services, it can be charged. In this context, authors in [141] proposed blockchain-based two electronic payment schemes (V-R transaction protocol and V-Rs transaction protocol) for the toll management and toll collection system. Before avail its services, the platform converts real currency into the virtual currency. Only RSU has participated in the consensus process, and transactions are automatically executed via the smart contracts. The elliptic curve digital signature algorithm (ECDSA256) algorithm is used as a signature algorithm. 460 ms and 444.5 ms are the smart contracts execution time for transaction initiation and transaction confirmation, respectively.

Authors in [116] proposed the dynamic intrusion detection model for V2X based on the micro-blockchain structure. The scheme consists of four planes; named micro-blockchain plane, the control plane, the virtualization plane, and the application and management plane. Micro-blockchains are deployed in each small region that can construct the

Table 5
Level of implementation of existing papers.

S.No.	Papers	Simulation of performances	Real implementation (platform) based on
1.	Kandah et al. 2019 [135]	**No simulation and only conceptual level**	–
2.	Zhang et al. 2019 [98]	MIRACL lib	**Ethereum**
3.	Zhang et al. 2019 [99]	MNT Elliptic Curves	–
4.	Yang et al. 2019 [100]	NS-3 simulator	–
5.	Li et al. 2018 [101]	Extension of VANETsim, Curves NIST	–
6.	Shrestha et al. 2019 [102]	**No simulation and only conceptual level**	–
7.	Yang et al. 2018 [103]	Matlab	–
8.	Lu et al. 2018 [2]	Protocol is implemented using Python	–
9.	Kang et al. 2018 [3]	Data-set from San Francisco Yellow Cabs	–
10.	Kang et al. 2019 [104]	CVX tool	–
11.	Shrestha et al. 2018 [105]	**No simulation and only conceptual level**	–
12.	Singh et al. 2017 [136]	**No simulation and only conceptual level**	–
13.	Singh et al. 2017 [106]	**No simulation and only conceptual level**	–
14.	Chai et al. 2019 [107]	Deep deterministic policy gradient model	–
15.	Javed et al. 2020 [108]	Remix IDE	**Ethereum**
16.	Lu et al. 2020 [109]	CNN	–
17.	Jiang et al. 2018 [137]	Matlab	–
18.	Lu et al. 2018 [110]	Based on computation, transmission and storage overheads	–
19.	Shi et al. 2020 [138]	Based on computation overheads	–
20.	Rathee et al. 2019 [139]	NS-2 simulator	–
21.	Wang et al. 2019 [111]	OMNeT++	–
22.	Noh et al. 2020 [112]	BAN-logic	–
23.	Kong et al. 2020 [113]	JPBC Lib	–
24.	Lin et al. 2020 [140]	Rinkeby, NS-2	**Ethereum**
25.	Deng et al. 2020 [141]	Based on computation overheads and web3j tool	**Ethereum**
26.	Song et al. 2020 [114]	DNN	–
27.	Dwivedi et al. 2020 [115]	**No simulation and only conceptual level**	–
28.	Leiding et al. 2016 [142]	**No simulation and only conceptual level**	–
29.	Liang et al. 2019 [116]	Classical back propagation neural network model	–
30.	Ming et al. 2020 [143]	MIRACL crypto SDK	–
31.	Javaid et al. 2020 [117]	Solidity, Remix IDE	**Ethereum**
32.	Iftikhar et al. 2020 [118]	Ganache, Metamask, IPFS	**Ethereum**
33.	Firdaus et al. 2021 [119]	SUMO, NS-3	**Hyperledger sawtooth**
34.	Ma et al. 2021 [120]	OMNeT++	**Rinkeby ethereum test network**
35.	Wang et al. 2020 [121]	**No simulation and only conceptual level**	–
36.	Javaid et al. 2019 [144]	Geth, Remix IDE,	**Ethereum**
37.	Li et al. 2020 [122]	Based on storage overhead and time consumption	**Hyperledger fabric**
38.	Zhang et al. 2020 [145]	SUMO	–
39.	Vangala et al. 2020 [123]	AVISPA	–
40.	Bagga et al. 2020 [124]	MIRACL lib, ROR model, AVISPA	**Hyperledger sawtooth**
41.	Ma et al. 2020 [125]	OMNeT++	**Rinkeby ethereum test network**
42.	Liu et al. 2020 [126]	SUMO V0.32.0	–
43.	Akhter et al. 2021 [146]	Ganache emulator, Metamask	**Truffle, ethereum**
44.	Shen et al. [127]	MIRACL lib	–
45.	Liu et al. 2019 [128]	Golang	–
46.	Li et al. 2019 [129]	OPNET	**Ethereum**
47.	Khalid et al. 2021 [130]	IPFS, Solidity	**Ethereum**
48.	Singh et al. 2020 [131]	Smart contracts	**Ethereum**
49.	Feng et al. 2019 [132]	Relic lib	**Hyperledger fabric**
50.	Chen et al. 2020 [133]	MIRACL lib	**Hyperledger fabric**
51.	Li et al. 2019 [134]	VANETsim, JPBC lib	**Parity Ethereum-based testing network**

local intrusion policies for vehicles. It provides the incentive to the nodes which collect the data. The control plane deals with the identity authentication procedure and deploying the intrusion detection policy for involved vehicles and managers. To solve the storage capability constraint problem, authors in [118] proposed an incentive and data storage scheme for VANETs by exploiting the benefits of the blockchain and IPFS. Authors store the event information in the IPFS and reputation (or trust) value of vehicles in the blockchain, respectively. In addition to this, the vehicle's incentive mechanism is also provided in the literature that motivates the validation of events. In Tables 6 and 7, we summarize the existing blockchain-based incentive mechanisms with their strength and weaknesses, respectively.

3.2. Data-sharing mechanisms

Due to the advanced technologies and rapid development of vehicular applications, intelligent vehicles generate a large amount of data. For example, intelligent vehicles can generate 1 GB of data per second from various devices such as cameras, a global positioning system (GPS), radar, etc. Moreover, the vehicles and other active segments of the network collect the data and share interested information. The interested information includes the traffic-related information (such as weather or road conditions on-road), parking lot occupancy, quality of vehicular services, etc. Sharing vehicular information improves drivers' safety and provides higher quality services to other segments of the VANET system. The resource constraints devices are the first and foremost problem associated with the data-sharing process in the VANET system. These devices cannot support large-scale data sharing and cannot store huge amounts of data. The malicious vehicles broadcast the falsified information to others; as a result, predictive action initiated by the other entities of the system is wrong. This problem needs to be considered when designing a trustful system.

To solve the problems such as message reliability when one vehicle sends any event information to other vehicles in ITS and for vehicle's identity validation in the VANET system, Xiaohong Zhang et al. [99] proposed the data security sharing and storage system based on the consortium blockchain (DSSCB). The proposed model considers the three types of data sharing: vehicle-to-vehicles, vehicle-to-RSU, and RSU-to-RSU. The sensing nodes (SNs) have participated in the information

Table 6
Comparison table based on different parameters of existing incentive work in VANETs.

S.No.	Ref.	Services	Block chain type	Blockchain specific challenge addressed	Miner node	Main characters	Technology
1.	Zhang et al. 2019 [98]	Vcoin system	Not Investigated	Mining incentive problem, Smart Contracts, PoW Consensus mechanism	RSUs	RSU, Vehicle, TMA, LED, Tracer	Ethereum blockchain, Smart contracts, Multi-signature, MIRACL lib
2.	Li et al. 2018 [101]	CreditCoin system	PRB	BFT Consensus mechanism, Mining Incentives	VEHs, RSUs	Vehicle, RSU, Trusted authority, Cloud server	Blockchain, Authentication, Combined public-key
3.	Yang et al. 2018 [103]	Trust-level mechanism	Not Investigated	PoW consensus mechanism	RSUs	Vehicle, RSU	Blockchain, Matlab
4.	Lu et al. 2018 [2]	Reputation-based system	Not Investigated	PoW consensus mechanism	VEHs	Certificate authority, LEA, Vehicle, RSU	Blockchain, Authentication
5.	Singh et al. 2017 [136]	Punish–reward mechanism	Not Investigated	Consensus, Mining incentives	Not Investigated	Vehicle, VCC, IVTP	Blockchain, Cryptocurrency
6.	Javed et al. 2020 [108]	Reputation-based system	PRB	Proof-of-authority consensus algorithm, smart contracts	Not Investigated	RSU, Edge vehicular nodes, Cache server, IVTP	IPFS, Caching technology, Ethereum, Remix IDE
7.	Deng et al. 2020 [141]	Electronic payment-toll collection	Not Investigated	Smart contracts	RSUs	RSU, Vehicle, LEA	Blockchain, Smart contracts, ECDSA256.
8.	Liang et al. 2019 [116]	Dynamic intrusion detection for V2X	Not Investigated	PoW, PBFT consensus	RSUs, Macro station	RSU, Vehicle, Trusted authority, Macro station	Micro-blockchain
9.	Iftikhar et al. 2020 [118]	Incentive mechanism-event validation	PB	PoA Consensus	RSU	RSU, vehicle, Certificate authority, Blockchain	Remix IDE with Ganache and Metamask, IPFS

PB: Public Blockchain, PRB: Permissioned Blockchain, VEHs: Vehicles, RSUs: Roadside Units.

interaction (exchange of event messages) process, and they are also rewarded for doing this task. The preselected nodes (PSNs) are also equipped with local storage devices, record pools, and smart contracts. The smart contracts are used as a triggering condition when storing the data in the PSN and providing the rewards to the SN nodes.

To ensure the correctness of traffic events in intelligent traffic management (ITM) based system, Yao-Tsung Yang et al. [100] proposed the blockchain-based traffic event validation model by utilizing the proof-of-event (PoE) consensus mechanism. In their work, RSUs have collected the traffic events and initialized the PoE consensus mechanism among the nearby passing vehicles to verify the event's validity. Suppose more numbers (above the threshold value) of passing vehicles confirmed the event. In that case, the new block for that particular event is created by initiated RSUs and stored in the local blockchain of RSUs. They suggest two blockchains: local blockchain and global blockchain. The RSUs maintain the local blockchain, and all the local blockchains are synchronized to create one global blockchain. The LEA is responsible for maintaining the global blockchain. The proposed scheme resolves the scalability issue due to the use of both local and global blockchains. The issue with the proposed method is with smart contracts. Smart contracts and the underlying mechanism are not investigated.

In the IoV environment, malicious users may compromise the connected and autonomous vehicles (CAV) and mislead the complete communication. As a result, the wrong information is acquired by the CAV. To solve this, Rathee et al. [139] proposed a blockchain-based scheme that provides secrecy to the CAV. During the movement of customers from one place to another, vehicle serial numbers, vehicles rating, etc., are captured by the sensor devices, validated by the peers, and permanently stored in the blockchain network. The proposed methodology reduces the user's fake request and alteration in the user's data, and this system achieves 79% of the success rate.

The vehicles in the IoV environment share their resources to improve the capability and efficiency of the system. The vehicles are not followed any fixed topology, and due to their mobility, maintaining the trust among the vehicles and RSU is one of the challenging tasks. To solve this problem, Chai et al. [107] proposed the consortium blockchain-based resource sharing framework, which is further based on the proof-of-reputation (PoR) consensus algorithm.

In the IoV, data-shared by the intelligent vehicles may be used for the collaborative analysis that enhances the driving experience and improves the service quality. Motivated by this fact, authors in [109] proposed a new architecture by integrating the hybrid blockchain and federated learning mechanism for data-sharing in IoV. The hybrid blockchain is the combination of permissioned blockchain and a local directed acyclic graph. The permissioned blockchain is maintained by the RSU, whereas a directed acyclic graph was utilized by the vehicles for efficient data-sharing. The delegated-PoS (DPoS) consensus mechanism was suggested in the permissioned blockchain. Node selection, local training, and global aggregation are the three phases of a federated learning scheme. Deep reinforcement learning further improves learning efficiency.

Similarly, authors in [137] study the centralized management approach for the storage of large data and conclude that the centralized approach is not recommended for the storage of large big data. They provide a solution for it by using blockchain technology. The blockchain is an effective technology for distributing and securing large amounts of data. The authors suggest the number of blockchains according to the different data types shared among the vehicular nodes. They provide an effective model for vehicle data transmission and give a detailed theoretical analysis.

Vehicular edge computing networks are one of the ideal candidates that provide massive storage resources. But, this also suffers from data

Table 7
Strengths, weaknesses and attacks counteracted of existing blockchain-based incentive works for VANETs.

S.No.	Ref.	Strengths	Weaknesses	Attack counteracted
1.	Zhang et al. 2019 [98]	(1) Solve the scalability issue, by providing the parent and auxiliary blockchain (2) Provides the Punish–reward based solution according to the announcement messages	Not achieved the sufficient transaction rate if two entities from two different regions perform the transaction	Rogue key attack
2.	Li et al. 2018 [101]	(1) Reputation points based incentive protocol (2) Protocol is reliable for forwarding the announcement messages (3) Offers an average time of 130 ms per transaction and 92.4 ms per 100 transaction for transaction and consensus part respectively	(1) Mining Incentive problems are fully addressed (2) key-management and decentralized authentication protocol has not incorporated in the presented solution	Sybil attack, Replay attack, Message modification attack, Man-in-the-middle attack
3.	Yang et al. 2018 [103]	(1) In this model, vehicles validate the messages based on the bayesian inferences and it further compute the rating of the neighboring vehicles (2) Along with vehicle's message, vehicles trust value also considered for the block validation	Credibility of neighboring vehicles is not considered in this model which can plays an important role to establish a decentralized trust management system	Impersonation, message modification and spoofing attacks
4.	Lu et al. 2018 [2]	(1) For preventing the distribution of forged messages, a reputation evaluation algorithm (reputation score) has designed (2) proof-of-presence and proof-of-absence protocol has used for maintaining the certificate and revocation transparency	(1) Smart contracts mechanism and mining incentive problems are not investigated (2) the authentication process is weak; no such computation has done during the authentication	Not investigated
5.	Singh et al. 2017 [136]	(1) Adopt reward based intelligent vehicle communication system (2) to support their arguments, layering architecture has proposed	ny kind of simulation to validate the results has not done	Not investigated
6.	Javed et al. 2020 [108]	(1) The IPFS is used to store the vehicles data (2) To increase throughput and reduce latency, proof-of-authority consensus has used (3) caching system has introduced to store frequently used services	(1) The cost of authenticating vehicles and store the data in IPFS increases with the increase data-size (2) the authenticity of a vehicular node depends on its reputation value; weak authentication model	Vulnerabilities of smart contract, Man-in-the-middle attack
7.	Deng et al. 2020 [141]	(1) Smart contract based automatic electronic toll collection system (2) with the use of smart contract, all transactions are automatically executed	(1) No authentication model has proposed between vehicle and RSU (2) this model can be used for the limited scenario	Replay attack
8.	Liang et al. 2019 [116]	Micro-blockchain is deployed in each region to construct the local intrusion detection strategy for vehicles	Analysis and comparison with existing intrusion detection systems has not done	Not investigated
9.	Iftikhar et al. 2020 [118]	(1) Storage constrain issues are resolved by using a distributed storage mechanism, (IPFS) (2) to provide the correct event and its validation, an incentive scheme has developed	(1) Privacy-preserving authentication protocol has not provided (2) execution of IPFS in the blockchain plate-form has not done	Not investigated

leakage and SPoF. To resolve this issue, authors in [119] proposed two smart contracts (local storage smart contracts and record pool smart contracts) and consortium blockchain-assisted enabled framework for data storage and sharing in vehicular edge computing network. Furthermore, the incentive mechanism is also utilized that motivates the vehicles to contribute to the data-sharing system. Similarly, Ma et al. [120] proposed attributed-based encryption and a blockchain-enabled system for sharing the announcement messages in the VANET system. Along with this, they also leverage the concept of IPFS for storing the announcement message in a distributed manner. Here, the vehicle uploaded the announcement message in the IPFS, and once it gets the hash, the encrypted hash (using a symmetric key algorithm) is handover to the RSU.

To overcome the problems of the centralized transportation system, Wang et al. [121] presented the consortium blockchain and proxy re-encryption-based system for securely sharing the data. In this scheme, the onboard units send the ciphertext to the RSU, and the verification is based on the ripple consensus mechanism. The authors proposed four smart contracts for achieving the same in the distributed-manner. Authors in [144] proposed a smart contract-assisted blockchain scheme for driving trust management and sharing the data in VANET. Their scheme utilizes the public key infrastructure (PKI) and certificate authority that registers the intelligent vehicle and revokes it if necessary. In addition to this, they also use the physical unclonable functions (challenge–response protocol) for achieving data reliability. Their protocol resists several internal as well as external attacks. In Tables 8 and 9, we summarize the existing blockchain-based data sharing schemes with their strengths as well as weaknesses.

3.3. Trust establishment

VANET system comprises various types of nodes, including the RSU, base station, vehicles, and connected objects such as smartphones. Different types of communication technologies such as Bluetooth, cellular networks, Wi-Fi, etc., are used to connect these heterogeneous nodes. The nodes establish a connection with other nodes by using these communication technologies and exchanging information. In the VANET system, malicious nodes can also connect with the honest nodes and send the wrong information. As a result, it disturbs the communication process. Establishing trust among the nodes is an important factor, and it can solve the flooding of falsified information. Whenever any of the intelligent nodes exchange the data with others, it is necessary to verify

Table 8
Comparison table based on different parameters of existing data sharing work in VANETs.

S.No.	Ref.	Idea	Block chain type	Blockchain specific challenge addressed	Miner node	Main characters	Technology
1.	Zhang et al. 2019 [99]	To solve the problems of message reliability and for vehicle's identity validation in VANET system, the DSSCB mechanism proposed	CB	Mining incentive problem, Smart Contracts, PBFT Consensus mechanism	RSUs	RSU, Vehicle, Storage server	Consortium blockchain, Authentication, Smart contracts, Cryptocurrency
2.	Yang et al. 2019 [100]	To ensure the correctness of traffic events, blockchain-based traffic event validation model by utilizing the PoE consensus mechanism proposed	PRB	PoE consensus mechanism	Not Investigated	RSU, Vehicle, LEA	Blockchain, Authentication, NS-3 simulator
3.	Kang et al. 2018 [3]	Integrate the vehicular network with mobile edge computing along with the smart contracts enabled consortium blockchain	Not Investigated	Consensus, Smart Contracts	RSUs	RSU, Vehicle, Cloud, Base station, Central authority	Smart contracts, Similar to bitcoin blockchain
4.	Chai et al. 2019 [107]	Consortium blockchain-based resource sharing framework for IoV environment based on the proof-of-reputation (PoR) algorithm	CB	Smart contract and consensus algorithm.	RSU	RSU, Vehicle	Consortium blockchain, Smart contracts
5.	Lu et al. 2020 [109]	Permissioned blockchain, DAG, and federated learning based data sharing scheme	PRB	DPoS consensus algorithm, DAG	Not Investigated	RSU, Vehicle, Server	CNN, Blockchain
6.	Jiang et al. 2018 [137]	Blockchain-based distributed and secure storage of data in IoV	Not Investigated	Multi-blockchain architecture	Not Investigated	RSU, Vehicle, Toll station, Gas station, Charging station	Blockchain, Matlab
7.	Rathee et al. 2019 [139]	Blockchain-based scheme for securing connected and autonomous vehicles in IoV for tracking the cab location	Not Investigated	Not investigated by the authors	Not Investigated	Autonomous vehicle, IoT	Blockchain, NS-2 simulator
8.	Firdaus et al. 2021 [119]	Consortium blockchain and smart contracts enabled data storage and sharing scheme for vehicular edge computing network	CB	PBFT Consensus, Smart contracts	RSU	RSU, vehicle, Trusted authority, Local storage, and record pool:	SUMO, NS-3, Hyperledger sawtooth
9.	Ma et al. 2021 [120]	Attributed-based encryption and IPFS enabled announcement sharing scheme for VANET	PB	Proof-of-storage consensus,	RSU	RSU, vehicle, Trusted authority, Policy management center, IPFS	Rinkeby ethereum external test network, Omnet++
10.	Wang et al. 2020 [121]	The ciphertext-policy attribute-based proxy re-encryption algorithm and consortium blockchain-enabled data sharing scheme for ITS	CB	Ripple consensus, Smart contract	RSU	RSU, vehicle, Trusted authority, Service sectors (Insurance company, Traffic police)	Blockchain
11.	Javaid et al. 2019 [144]	Physical unclonable functions and ethereum smart contracts enable data sharing scheme for VANET	PB	Smart contract	RSU	RSU, vehicle, Certificate authority	Geth, Remix IDE, Solidity

PB: Permissionless Blockchain, CB: Consortium Blockchain, PRB: Permissioned Blockchain, VEHs: Vehicles, RSUs: Roadside Units.

and validate the trust of the nodes. It can also help the system to take corrective measures.

As discussed above, trust plays a crucial role when several nodes are connected and share information. In the continuation of it, authors in [135] proposed the multi-layered, blockchain-based trust-building and authentication framework to maintain the trust relationship among the network entities. In their scheme, vehicles are represented in the lowest level, and vehicles form the group (Based on region, proximity, etc.), called a platoon. The vehicles within the same platoon exchange the event messages among each other. They analyze the message and based on the validation result, event-generating vehicles get the trust value from the other vehicles. The updated trust value is also uploaded in the platoon blockchain. The RSUs are considered at the upper level. The vehicles within the proximity transferred the platoon blockchains to the RSUs. The RSUs add the platoon blockchains in the primary blockchain and broadcast the updated primary blockchain to

Table 9
Strengths, weaknesses and attacks counteracted of the existing blockchain-based data sharing work in VANETs.

S.No.	Ref.	Strengths	Weaknesses	Attack counteracted
1.	Zhang et al. 2019 [99]	(1) Data transaction speed is high (2) combination of public and private blockchain has used for sharing the vehicular data; applicable for real-time scenarios (3) block confirmation time is reduced up-to 60%	(1) High computation time is required (2)The mechanism behind the incentive of SNs are not fully investigated (3) the blockchain implementation has not analyzed	Not investigated
2.	Yang et al. 2019 [100]	(1) Solve the scalability issue, by providing the local blockchain (maintained by RSUs) and global blockchain (maintained by LEA) (2) selfish nodes can identify easily due to incorporation of proof-of-event consensus	(1) Complete decentralized architecture is missing (2) Smart contract mechanism are not investigated (3) the overall computation and communication overheads has not analyzed	Not investigated
3.	Kang et al. 2018 [3]	(1) Adopt reputation mechanism for data sharing among vehicles (2) smart contract has utilized for secure sharing of vehicular data (3) consortium blockchain for data storage; applicable for real-time scenarios	(1) Weak vehicle's authentication has provided (2) The implementation of this model under the suitable blockchain platform has not analyzed	Majority attack, Message modification attack
4.	Chai et al. 2019 [107]	(1) Differentiated pricing scheme matches the demand and supply condition of resources (2) Differentiated pricing scheme achieves 30% increase compared to the unified pricing schemes and (3) less computation overhead due to the proof-of-reputation consensus mechanism	The overall computation overhead and throughput of the system based on the proof-of-reputation mechanism has not evaluated	Double-spending attack, Majority attack
5.	Lu et al. 2020 [109]	(1) Deep reinforcement learning is adopted to improve the node selection efficiency (2) federated learning model reduces the load and addresses the privacy concern of service providers (3) final parameters of learned model is added to the blockchain which is further verified by the participants	(1) The implementation of the scheme under the blockchain platform has not investigated (2) the efficiency under the node selection and throughput of the system has not evaluated	Majority attack
6.	Jiang et al. 2018 [137]	(1) multi-blockchain network model; complete decentralization is achieved (2) Provide only in-depth theoretical analysis	(1) Does not consider real time traffic scenario (2) Not applicable for real time applications	Not investigated
7.	Rathee et al. 2019 [139]	(1) User's fake request is reduced by the system and 79% of success rate is achieved by the protocols (2) the model is validated under the attacking scenario with different attacking possibilities	(1) The underlying mechanism behind the retrieving the information from the blockchain has not analyzed (2) security analysis has not investigated (3) the vehicle and IoT devices has low computation and storage capability; they cannot maintain the blockchain	Physical capturing attack, Message modification attack, Man-in-the-middle attack
8.	Firdaus et al. 2021 [119]	(1) The cryptographic primitive guarantees the vehicle's identity anonymity (2) transaction throughput is high (3) incentive model encourages the nodes to participate in the data sharing	(1) The authentication model for vehicles and RSU has not analyzed (2) the evaluation of smart contract has not investigated	Message modification attack, Majority attack
9.	Ma et al. 2021 [120]	(1) Storage-coin which is based on the proof-of-storage mechanism is used to provide a reward for concerned RSU (2) provides fully distributed storage model (3) provides mathematical model for security of blockchain	(1) Computationally expensive model (2) complete decentralization for vehicle and RSU authentication has not achieved	Majority attack
10.	Wang et al. 2020 [121]	(1) Applicable for real time scenario in ITS (2) The communication overhead for system parameters and for ciphertext is 400 bits and $60(2l+4)bits$ where l is the number of attributes in the access attribute (3) block generation time is relatively low than other existing systems	(1) Computationally expensive model (2) the effective evaluation of model under the blockchain platforms has not investigated	Replay attacks, Collusion attacks, Majority attack
11.	Javaid et al. 2019 [144]	(1) Utilization of physical unclonable functions increases the security of the system (2) enhances the storage capacity of the model	(1) Complete decentralized architecture for sharing the data is missing (2) key management and authentication protocol have not discussed	Message modification attack, Physical attack, Majority attack

the other RSUs. So that other RSUs also synchronize with the updated primary blockchain, and consistent blockchain exists among all the RSUs. The proposed framework considers the three types of trust named as direct trust among vehicles, indirect trust among vehicles, and reputational trust among vehicles and two blockchains named platoon blockchain and primary (global) blockchain. Each platoon maintains the blockchain, and vehicles are elected as a miner node. The vehicle with the trust value higher than the threshold-trust value is elected as

Table 10
Comparison table based on different parameters of the existing trust establishment work in VANETs.

S.No.	Ref.	Application	Trust model	Block chain type	Blockchain specific challenge addressed	Miner node	Main characters	Technology
1.	Kandah et al. 2019 [135]	Multi-layered trust building system	EM	Not Investigated	Miner selection for Platoon blockchain	VEHs, RSU	RSU, Vehicle	Blockchain
2.	Shrestha et al. 2019 [102]	Exchange control	HM	PB	Consensus Mechanism (PoW)	VEHs	RSU, Vehicle	Blockchain
3.	Yang et al. 2018 [103]	Credibility of the vehicle's message	HM	Not Investigated	PoW consensus mechanism	RSUs	RSU, Vehicle	Blockchain, Matlab
4.	Kang et al. 2019 [104]	Exchange control — DPoS consensus mechanism	Reputation and contract theory	Not Investigated	DPoS consensus mechanism, Incentive mechanism	RSUs	RSU, Vehicle	Blockchain, CVX tool
5.	Shrestha et al. 2018 [105]	Message dissemination	HM	PB	PoW consensus mechanism	VEHs	RSU, Vehicle	Blockchain
6.	Singh et al. 2017 [106]	Exchange control — intelligent vehicle trust point based	EM	Not Investigated	PoD consensus	VEHs	Vehicle, IVTP	Blockchain, Vehicle cloud computing, Digital signature
7.	Lu et al. 2018 [110]	Anonymous reputation system	EM	Not Investigated	Proof-of-presence, proof-of-absence	VEHs	Certificate authority, LEA, RSU, Vehicle	Blockchain, Authentication
8.	Javaid et al. 2020 [117]	Exchange control — PUF, certificate, and PoW consensus mechanism	Not Investigated	PB	Consensus, Smart contracts	RSUs	RSU, Vehicle, Server, PUF	Ethereum blockchain, Solidity, Remix IDE
9.	Li et al. 2020 [122]	Trust management-Dirichlet distribution	Not Investigated	PRB	Improvement of PBFT consensus	RSU, Regional authority	Local service provider, Regional authority, RSU, vehicle	Hyperledger fabric
10.	Zhang et al. 2020 [145]	Multi-layered trust building system	HM	Not Investigated	Both vehicle and RSU participate in trust management	RSU	RSU, vehicle	SUMO

PB: Permissionless Blockchain, PRB: Permissioned Blockchain, EM: Entity-centric Model, HM: Hybrid Model, VEHs: Vehicles, RSUs: Roadside Units.

a miner for adding the new block (mainly, the trust value of vehicles within the platoon) in the platoon blockchain. The RSUs maintain the primary blockchain, and here, RSUs are elected as a miner. According to the authors, all the RSUs have computational enough power, and any RSUs are elected as a miner for the primary blockchain. The benefit of the above scheme is that they use the entity-centric trust model to ensure data ownership. But, the underlying consensus mechanism and mining incentive problems are not fully investigated by the authors.

Researchers classified the trust scheme into three categories; data-centric, entity-centric, and hybrid (a combination of data-centric and entity-centric). In the hybrid model, the node which is sharing the content and the type of content are both considered. The authors suggested the same approach in [105]. They proposed the hybrid-trust model to solve the message dissemination problem in the VANET environment. Both the parameters (event message and vehicle's trust level) are used to create a new block, which is stored in the local and public blockchain. The proposed method uses the PoW consensus mechanism to validate a new block. Here, vehicles act as miner nodes, and to perform this task, vehicles are also rewarded. Authors in [110] used two blockchains based on the proof-of-presence and proof-of-absences algorithm. To provide incentives to the vehicles, the reputation management algorithm has been proposed. The protocol adopts cryptographic primitives to achieve vehicles' authentication. The authors do not address the underlying smart contract mechanism.

Blockchain technology was initially drafted for cryptocurrency. Trust is the prime motivation for the formation of cryptocurrency. After successfully accepting cryptocurrency, researchers suggest and draft the new idea in several different applications that can adopt blockchain technology. Researchers are suggesting novel ideas on the top of blockchain technology that can enhance the throughput and efficiency of the existing applications. In [102] researchers adopt the hybrid model, and by using this model, they analyze how the messages are exchanged between vehicles and RSU. The blocks in the blockchain-based VANET system are built based on the event messages and trustworthiness of the particular node, similar to the transactions in the bitcoin-cryptocurrency system. Their blockchain-based VANET system works only for a particular country. Hence, there would be a separate public and local blockchain for each country. Utilizing the local and public blockchain, they resolve the scalability issue, which is the first consideration of every architecture. Their proposal suggests the PoW consensus mechanism for validating and verifying a new block. The event messages are broadly classified into two types — beacon messages and safety event messages. RSU provides the location certificates to the vehicles which are in the communication range. For getting the location certificates, vehicles first verify the authenticity of their presence. If the proof of location is done, RSU provides the location certificates to the nearby vehicles. They do not consider the smart contracts technique.

Moreover, in [106], authors proposed the intelligent vehicle trust point-based framework for the communication of vehicles using the blockchain technology in the ITS system. The suggested protocol focuses on fast and secured communication among intelligent vehicles. Yang et al. [103] proposed the blockchain technology-enabled decentralized trust management framework for the VANET system. In their proposed model, if any vehicle gets the information related to any critical event, the same vehicle sends the event information to its neighboring vehicles. Now, the task of neighboring vehicles is to validate the event message, and based on the validation result, calculate the rating value of a particular vehicle. After this, the neighboring vehicles uploaded the above information to their neighboring RSUs. Based on this, the RSUs generate the trust value offset of vehicles by using the weighted aggregation method and take the appropriate decision to create a new block. RSUs act as miners in their proposed protocol, and they use both PoW and PoS consensus mechanisms. After this, the RSUs synchronize the updated trust value offset and new block with the other RSUs, and finally, they create a consistent and reliable database. In their consensus mechanism, the RSUs who have more stakes could participate in the block generation process. But, along with stakes, the proposed scheme also considers the trust value offset of the participated RSUs. According to the authors, the RSU, with the considerable trust value offset, is more likely to win the mining procedure and publish the new block in the blockchain network. The computation overhead of this scheme may be increased because they use both the PoW and PoS consensus mechanisms. The authors have not investigated the smart contracts mechanism.

The authors adopted a similar approach but a different consensus mechanism in [104]. The authors proposed the enhanced DPoS consensus mechanism for blockchain-enabled IoV based on the reputation and contract theory. In their work, RSUs act as miner nodes, and there are two types of miners present in their IoV environment. The first one is termed as an active miner, and the other one is termed as a stand-by miner. Their whole work is divided into two-stage. In the first stage, the proposed protocol selects miners (both active and stand by miners), and in the second phase, after generating the block from active miners, block verification is done by the stand by miners. The selection of the miner's node is made by utilizing the reputation mechanism (based on both past interactions and recommended opinions from other vehicles). The reputation mechanism was based on the multi-weight subjective logic model. The stand-by miners who verify the newly generated block get a reward or incentive. The contract theory is used to prevent internal collusion among the active miners. The working of the suggested enhanced DPoS mechanism for blockchain-enabled IoV was divided into seven steps, namely, system initialization, miner candidate joining, reputation calculation, miner selection, block manager generation, consensus process, and reputation updating. In their work, authors use asymmetric cryptography and the elliptic curve digital signature algorithm for the system's initialization. The smart contracts mechanism and heterogeneity of vehicle communication messages are not fully investigated. Scalability issues might arise if the number of vehicles and block generation rate is high in the IoV environment.

The roadside infrastructure and autonomous vehicles are the key components of IoV. It provides new innovative services such as an intelligent traffic management system and enables autonomous vehicles to broadcast messages that can improve the road safety and efficiency of the transportation system. But, due to the no-trusted environment, it is not easy to evaluate the credibility of received messages. Authors in [117] try to overcome this challenge. They used physical unclonable functions (PUF), smart contracts, certificates, and a dynamic-PoW consensus algorithm for establishing the trust in IoV. The smart contracts provide a secure framework that can block malicious vehicles and register with trusted ones. PUF assigns a unique identity to each vehicle, and RSU issues the certificate that is useful to maintain the trust among the vehicles. PKI and blockchain smart contracts are used for vehicle registration. The dynamic PoW provides scalability according to the traffic generated by the vehicles.

The high mobility nature of vehicles raises security problems to the VANET system. Authors in [122] proposed a blockchain-based trust management model that can preserve the location of vehicles. Their scheme allows the vehicles to use certificates for further requesting the location-based services without revealing the private information of vehicles based on the anonymous cloaking region. In addition to this, in their proposed model, there is no direct communication between the vehicles, whereas the vehicles are participating in the construction of an anonymous cloaking region, and this participation reflects the trust value of vehicles. To improve the overall travel safety (traffic-related messages) and efficiency of the vehicular network, authors in [145] proposed a blockchain and artificial intelligence-enabled trust management system for the vehicular networks. In their model, the vehicle exchanges the messages with other vehicles, and the deep learning algorithm is used to compute the trust value of vehicles and RSU. Furthermore, the RSU validate the authenticity of vehicle and message based on blockchain technology. Tables 10 and 11 respectively summarize the existing blockchain-based trust models with their strengths and weaknesses.

3.4. Authentication mechanism

An authentication mechanism is an important challenge in the VANET system. In the existing schemes (without blockchain-based VANET), mainly used PKI based solutions, and the sensitive parameters are stored in the central server (such as the cloud). The PKI solutions would be expensive solutions for the VANET system because of the limited capability of nodes. On the other hand, the adversary directly launches various kinds of attacks on the central server and tries to get sensitive information. SPoF, privacy, and trust are the main issues associated with the central system. This gives enough motivation to the researchers to put their efforts into the design of the blockchain-based authentication mechanism.

Zhang et al. [98] proposed a security model consist of the following entities: RSUs, Vehicles, traffic management authority (TMA), issuers, tracers, and LEA. The TMA is an authority that issues the public key to every entity in the system. For each region, an issuer is employed, which is selected by the TMA. The task of the issuer is to issue the credentials to the vehicles within the region by using the fair blind signature scheme (FBSS) algorithm. The TMA also employs the tracer to identify the announcement message is correct or fake. If fake, then the task of the tracer is to find the true identity of the false message generator by using the threshold-secret sharing scheme. The tracer and issuer work under the supervision of the LEA. If the tracer or the issuer does anything wrong, other vehicles might directly report to the LEA.

Researchers used different authentication protocols that provide the node authentication and ensure the integrity, non-repudiation, and reliability of the vehicle's data. In the continuation of it, the author in [99] used the consortium blockchain for secure sharing and storage of vehicle's data along with the elliptic curve-based digital signature method. In the suggested framework, two types of nodes exist in the consortium blockchain-based network. The first type of nodes are called PSNs, (RSUs) act as PSN nodes, and the second type of nodes are called SNs, vehicles act as SN nodes. PSN nodes have participated in the block generation process. In other words, PSN nodes are responsible for the consensus mechanism. SN nodes have not participated in the PBFT-based consensus mechanism. All the PSNs work under the traffic authority. If PSN gets any abnormal activity in the network, they directly report to traffic authority. The identity of the vehicle and shared message between any of the entities mentioned above are easily verified due to the elliptic curve-based signature technique. The proposed protocol can achieve decentralization of data, tamper-proof, and unforgeable data due to the use of a consortium blockchain-based system, and protect the user's identity due to the use of the digital signature method.

Kang et al. [3] integrate the vehicular network with mobile edge computing to solve the data-sharing problem by utilizing the smart contracts enabled consortium blockchain. Their data sharing scheme is based on the reputation of vehicles, which is further based on the three-weight subjective logic model. Their vehicular edge computing network comprises three layers: user layer, edge layer, and cloud layer. The vehicles with OBU are deployed in the user layer. The OBU collect the data from vehicles and upload it into the nearby RSUs. In the

Table 11
Strengths, weaknesses and attacks counteracted of the existing blockchain-based trust establishment work in VANETs.

S.No.	Ref.	Strengths	Weaknesses	Attack counteracted
1.	Kandah et al. 2019 [135]	(1) Adopt an entity-centric trust model for ensuring data ownership and integrity (2) utilizes direct, indirect and reputation trust for providing the decentralized trust system	(1) Only theoretical analysis of model is presented (2) the inherent cryptographic mechanism are not discussed	Colluding attack
2.	Shrestha et al. 2019 [102]	(1) Both node and message trustworthiness has utilized (2) focus on scalability of the VANET system	(1) block generation and confirmation time is high (2) the underline mining mechanism has not discussed (3) does not evaluate the model using simulators	Double spending attack
3.	Yang et al. 2018 [103]	(1) vehicle and RSU both participate in the formation of new block (2) More trust is achieved	(1) Computation overhead can increases (2) this scheme supports weak authentication model (3) the proposed model is designed for limited scenarios	Impersonation attack
4.	Kang et al. 2019 [104]	(1) Adopt contract theory based incentive mechanism to provide rewards to the stand by miners (2) miner selection is based on reputation based voting system (3) this model decreases collusion among the stakeholders	The accuracy for miner selection can be increased with the consideration of more weights	Majority attacks
5.	Shrestha et al. 2018 [105]	(1) Adopt event message and vehicles' trust level for generating a new block (2) real time scenario has considered	(1) Only theoretical analysis of model is presented (2) does not analyzed the cryptographic mechanism behind this model (3) does not investigated the implementation of blockchain	Double spending attack
6.	Singh et al. 2017 [106]	(1) Real scenario has considered to show the effectiveness of model (2) reward based system; encourages vehicles to participate in the system	(1) vehicles has low computing and storage capabilities; may not participate as blockchain node (2) does not analyze the model using the simulators	Not investigated
7.	Lu et al. 2018 [110]	(1) Unlinkability between real identity and public key is provided by the model (2) multi blockchain model; enhance the scalability of the system	(1) The underlying smart contracts mechanism are not addressed (2) this model provides weak authentication of vehicles (3) does not provide complete decentralized solution	Not investigated
8.	Javaid et al. 2020 [117]	(1) Case study has considered to show the effectiveness of the model (2) mathematical modeling has done to provide the security of blockchain	Computation overhead is high	Physical capturing attack, Message modification attack, Majority attack
9.	Li et al. 2020 [122]	(1) Vehicle uses certificate to request the location based services without revealing its real identity (2) hyperledger fabric blockchain platform has used to show the effectiveness of the model	Does not discussed the token incentive	Sybil attack, Bad-mouthing attack
10.	Zhang et al. 2020 [145]	(1) Deep learning model has used to evaluate the trust of nodes (2) real time traffic scenario has adopted	(1) Overall computational complexity to validate the hash values based on blockchain is $O(n)$ (2) does not analyze the privacy concern of vehicles deeply	Bad-mouthing attack, Message modification attack

middleware layer, RSUs are deployed. The RSUs are combined to form the vehicular edge cluster. The cloud layer coordinates all the vehicular edge clusters, and the data are permanently stored.

The self-organization of vehicles in the IoV environment leads the malicious attackers to mislead the communication process. As a result, the safety of mobile services is an open challenge in IoV. To address this challenge, Wang et al. [111] proposed an authentication scheme for IoV, which is further based on the consensus algorithm of the blockchain mechanism. The proposed consensus algorithm is used to authenticate a new vehicle's nodes. Moreover, the new key distribution scheme is also used to join a new vehicle node, and it is constructed based on the blockchain mechanism. A new intelligent smart contract based on the rayleigh algorithm is used to join a new node. The suggested smart contract easily distinguishes the good nodes and bad nodes. The contract immediately blocks the malicious nodes if found. The open-source framework of veins is used for simulation. This framework is based on OMNeT++ and SUMO. According to the author's simulation result, the encryption process takes 9 ms, the verification process (in RSU) takes 3 ms to 5 ms. On the other hand, communication overhead is 17 kB for registration of vehicles and 8 kB for verification reports at RSU.

Similarly, Noh et al. [112] proposed a message authentication scheme for connected vehicles to preserve the anonymity of vehicles and decentralization of information (such as traffic jam information) based on the blockchain mechanism. The traditional public–private keys and message authentication codes are used for the authentication process. The PoW and PBFT algorithms are utilized to achieve the consensus. Due to the certificate (key) management limitations in the public-key infrastructure protocols, the existing conditional privacy-preserving authentication solutions are not ready for deployment in a vehicular network. Motivated to this, authors in [140] proposed a blockchain-based conditional privacy-preserving authentication protocol that is specifically designed for the ethereum blockchain. To show the anonymity and traceability of the proposed solution, it is implemented in the Rinkeby ethereum test network. The message verification and communication cost was 0.014368 s, and the communication cost was264 bytes.

Secured communication is essential when the IoV entities exchange information with each other. To achieve this, authors in [123] proposed a blockchain-assisted certificate-based authentication protocol for IoV entities which is further useful to achieve the various kinds of notifications in ITS. Based on this authentication process, vehicles securely notify the important events to others (such as RSU, cluster heads, and cloud servers). In their scheme, the edge servers are responsible for creating the partial block, whereas the cloud servers are responsible for full block creation and verification using the PBFT consensus mechanism. Similarly, Bagga et al. [124] presented a blockchain-assisted batch authentication protocol for IoV envisioned smart city. In their scheme, vehicle-to-vehicle authentication allows the vehicles to authenticate their neighboring vehicles, whereas batch authentication allows the RSU to authenticate a group of cluster vehicles. At this end, a common key is established between the RSU and vehicles in the particular cluster. In addition to this, the Real-Or-Random (ROR) oracle model with the hyperledger sawtooth blockchain platform is used to implement the same.

To provide more safety in the transportation system, Ma et al. [125] presented the blockchain-assisted decentralized key management protocol for VANET that automatically realizes the registration, updation, and revocation of users' public keys. In addition to this, they also proposed a mutual authentication protocol based on the bivariate polynomial function. The advantage of their protocol is that it provides complete independence from the PKI system; no certificate is required for the same. Their protocol is resilient against public key tampering, denial-of-service (DoS), collusion, and various internal and external attacks. Traditionally, pseudonymous authentication schemes are used to achieve unlinkable authentication. But, this mechanism requires multiple interactions with the trusted third party. To solve this issue, and to remove the trusted third party completely from the system, authors in [126] presented the blockchain-assisted unlinkable authentication in VANET. To ensure the unlinkability and traceability of vehicles' identity, the multiple pseudonyms identity of the vehicle is associated with their real identity, and the service manager verifies the same in case of disputation. In Tables 12 and 13, we summarize the existing blockchain-based authentication protocols in VANETs with their strengths and weaknesses.

3.5. Privacy-preserving mechanism

Preserving the privacy of intelligent nodes involved in the VANET system is paramount. Intelligent vehicles generate a huge volume of data, including important information such as road accidents, environmental hazards, etc. The adversary launches the attacks, such as tracking attacks, to know the real identity of the node. Once the real identity of the node is exposed, it is very easy for the adversary to enter and do the mal-functioning in the system. Therefore, it is essential to keep the identity of the node very securely. The existing traditional system adopted various methods and techniques to achieve the user's privacy. The inherent property of blockchain easily achieves the pseudonymity of nodes. As a result, the real identity of nodes is never revealed.

Authors in [138] used the important cryptographic primitives are used to achieve pseudonymity among the vehicles, RSU, and users. The authors used the blockchain mechanism to accomplish the following two purposes (1) to ensure reliable data-sharing among the communicating parties (2) to provide tamper-proof multimedia data. The theoretical security analysis confirmed that this method achieves identity authentication, data integrity verification, and identity privacy protection. Traceability which is an important security feature is also achieved by the proposed scheme when malicious users send illegal data. Privacy protection, reliability and integrity, traceability, and high efficiency are the design goals behind this paper.

The vehicles in the vehicular sensor network (VSEN) are equipped with sensor devices. These devices collect a large amount of data and submit it to the remote cloud server causing more computation and communication costs. Ming et al. [143] suggested a privacy-preserving data-sharing scheme for fog-assisted VSEN. Moreover, fog computing is used for local data-sharing with minimum latency. The computation overhead for vehicles is 1.9255 ms in the data collection phase and 5.5237 ms in the data query phase. On the other hand, the communication cost is 172B in the data collection phase and 320B in the query phase. Similarly, in [106] authors adopt the proof-of-driving (PoD) based consensus algorithm for validation purpose. If more than 50% of vehicles correctly validate the messages, validation was successful. This scheme has done easy verification of the received message. Here, each intelligent vehicle generates its public and private keys. The key pair is stored in the blockchain. The blockchain act as the public ledger for all the intelligent vehicle. They utilize the digital signature mechanism before broadcasting the messages to the nearby intelligent vehicles.

Traditionally, the VANET system follows a centralized architecture. In this system, data privacy is ensured by using various encryption techniques based on the sender's (vehicle or RSU) private information. The sender's private information is generally stored in the central server. As a result, it can often be targeted by attackers. In [112] authors proposed a novel scheme. In this scheme, a block is generated by the local trusted authority based on the PoW consensus algorithm. Once the block is generated, the local trusted authority and vehicles perform the block verification process based on the PBFT consensus algorithm. The block confirmation process is performed by the root trusted authority and local trusted authority. The BAN-logic, which is one of the formal verification methods, is used to verify the proposed protocol. For a better understanding of results, the PBFT algorithm is also compared with the other two algorithms: loop-fault tolerance and Hotstuff.

Li et al. [101] proposed a blockchain-based privacy-preserving incentive announcement network for vehicles in smart cities. Their work focus on the reliable broadcasting of the announcement message in the VANET system without revealing the vehicle's identity. The proposed system consists of a trusted authority, trace manager, vehicles, RSUs, and cloud application server. The trusted authority provides the public parameters (keys) to the vehicles. The trace manager traces the malicious vehicles. RSUs are responsible for the consensus voting mechanism. The cloud application server stores non-cryptographic information. The vehicles and RSUs have participated in the consensus mechanism in their work, and the authors use the BFT consensus mechanism to validate a block. The proposed BFT protocol may not work if more malicious vehicles are present in the network. The authors do not investigate the underlying smart contract mechanism.

In [113], authors try to resolve two major challenges associated with the vehicular network. The first one considers the verifiable collection of vehicular sensory data with privacy preservation. The second challenge relates to a reliable and efficient way of sharing sensory data. Considering these two challenges, authors in [113] proposed a permissioned blockchain-based privacy-preserving scheme for the verifiable sharing of sensory data. An identity-based signcryption scheme with the 2-DNF cryptosystem is used for batch authentication of sensory nodes and the verifiable computation of collected data. The proposed system considers only three entities; RSU, vehicles, and server. The communication overhead for the server-to-RSU and RSU-to-server is $(260 + 16 * 3)B$ and $(260 * 3)B$ respectively. $((16 * 3) + (k + 2) * 260)B$ is the total communication overhead between the RSU and user, where k is the number of vehicles that send the sensory data.

Authors in [146] proposed a multilevel blockchain-assisted privacy-preserving authentication protocol for VANET. In their system, two authentication centers are present. The global authentication center

Table 12
Comparison table based on different parameters of the existing authentication work in VANETs.

S.No.	Ref.	Approach	Block chain type	Blockchain specific challenge addressed	Miner node	Main characters	Technology
1.	Zhang et al. 2019 [98]	FBSS	Not Investigated	Mining incentive problem, Smart Contracts, PoW Consensus mechanism	RSUs	Vehicle, RSU, TMA, LED, Tracer	Ethereum blockchain, Smart contracts, Multi-signature, MIRACL lib
2.	Zhang et al. 2019 [99]	Elliptic curve	CB	Mining incentive problem, Smart Contracts, PBFT Consensus mechanism	RSUs	RSU, Vehicle, Storage server	Consortium blockchain, authentication, Smart contracts, Cryptocurrency
3.	Kang et al. 2018 [3]	Elliptic curve digital signature	Not Investigated	Consensus, Smart Contracts	RSUs	RSU, vehicle, Cloud, Base station, Central authority	Blockchain, Similar to bitcoin blockchain
4.	Wang et al. 2019 [111]	Identity Authentication	Not Investigated	Smart contract, BFT and Ripple consensus algorithm	Not Investigated	RSU, Vehicle, Cloud	Blockchain, Smart contracts, PKI, OMNeT++
5.	Noh et al. 2020 [112]	Message authentication codes	PRB	PoW and PBFT consensus algorithm	Local trusted authority	Trusted authority (RTA, LTA), RSU, Vehicle	Blockchain, BAN-logic, Authentication
6.	Lin et al. 2020 [140]	ECDSA	PB	Smart contracts	Not Investigated	RSU, Vehicle, Certificate authority	Ethereum blockchain, Smart contracts, Solidity, Rinkeby, NS-2
7.	Vangala et al. 2020 [123]	ECDSA	Not Investigated	PBFT consensus	Cloud server	Vehicles, RSU, Edge servers, Cloud servers, the Registration authority	Node.js language with VS CODE, AVISPA
8.	Bagga et al. 2020 [124]	ECDSA	PB	PBFT consensus	Fog server	Vehicles, RSU, Fog servers, Cloud servers, Trusted authority	Hyperledger sawtooth, MIRACL library, Real-Or-Random (ROR) random oracle model, AVISPA
9.	Ma et al. 2020 [125]	Symmetry of bivariate polynomial function	PB	PoW consensus, Smart contracts	RSU	Vehicle service provider, vehicles, RSU	OMNeT++ 4.7, Rinkeby ethereum external test-network,
10.	Liu et al. 2020 [126]	Homomorphic encryption	CB	PBFT consensus	Service manager	Audit department, Service manager, RSU, Vehicles	SUMO V0.32.0

PB: Permissionless Blockchain, CB: Consortium Blockchain, PRB: Permissioned Blockchain, VEHs: Vehicles, RSUs: Roadside Units.

stores the vehicle's sensitive information, whereas the local authentication center maintains the blockchain and handover mechanism between the clusters of vehicles. In addition to this, they also suggested the modified control packet format that can overcome the various shortcoming of the traditional medium access control protocol, and the RSA-1024 digital signature algorithm is utilized to achieve further security, confidentiality, and integrity of data packets. Location-based services (LBS) are one of the important application areas of vehicular networks. The online certificate authority maintains the efficiency and security of LBS, where resource-constrained vehicles interact with the certificate authority very frequently. The authors in [127] proposed a consortium blockchain-enabled lightweight threshold certificate authority-based solution that preserves the privacy of LBS in the vehicular network. The threshold proxy signature scheme allows the vehicles to authenticate themselves. The protocol also resists man-in-the-middle attacks and provides conditional anonymity for vehicles identity.

According to the authors in [128], trust and privacy are two crucial factors to build a secure network in VANET. In [128], they proposed blockchain-assisted trust management and conditional privacy-preserving announcement solution for VANET. The vehicle's reputation score is used to calculate the message reliability, and an identity-based group signature scheme is used to achieve the conditional privacy of vehicles. In addition to this, the combination of the PoW and PBFT consensus algorithm is used to achieve better security in the VANET system. Authors in [129] provide a blockchain-assisted identity and location preserving mechanism in the VANET. To achieve this, they proposed three-different algorithms named undirected graph generation (UGG) algorithm, identity privacy protection (IPP) algorithm, and location privacy protection (LPP) algorithm, which is further based on the dynamic threshold encryption, and k-anonymity unity. The (m,r) threshold secret sharing scheme is used to protect the privacy of vehicular identity. Tables 14 and 15 summarize the existing blockchain-based privacy-preserving solutions in VANETs with their strengths and weaknesses.

3.6. Smart-contracts based system

Blockchain is one innovative technology that can transform many applications, including supply chain, land record, healthcare, energy,

Table 13
Strengths, weaknesses and attacks counteracted of the existing blockchain-based authentication work in VANETs.

S.No.	Ref.	Strengths	Weaknesses	Attack counteracted
1.	Zhang et al. 2019 [98]	(1) Multi-model blockchain has considered (2) increases throughput of the parent blockchain (3) the system can trace the true identity of vehicles (4) incentive system based on the punish–reward mechanism	(1) Does not evaluate the transaction rate if the transaction has done between the nodes of different region (2) Key generation protocol are not fully investigated	Rogue key attack
2.	Zhang et al. 2019 [99]	(1) Protect the user's identity due to the use of digital signature method and (2) little-weight scalable due to the consortium blockchain (3) batch verification of messages are provided	(1) Computationally expensive scheme (2) does not investigate the mathematical validation of single and batch verification of messages	Not investigated
3.	Kang et al. 2018 [3]	(1) Adopt reputation mechanism for data sharing among vehicles (2) smart contract has utilized for secure sharing of vehicular data (3) consortium blockchain for data storage; applicable for real-time scenarios	(1) Selection of Miner Nodes are not addressed (2) does not support strong authentication protocol	Majority attack, Message modification attack
4.	Wang et al. 2019 [111]	(1) Dynamic addition of new node based on the smart contract and blockchain is provided (2) variant of byzantine fault tolerance model is used for node authentication procedure with less computation and communication overhead	(1) Does not analyze the security analysis of the model under the threat model (2) does not investigate the revocation of certificate	Not investigated
5.	Noh et al. 2020 [112]	(1) Strong consensus protocol has provided (2) distributed authentication of messages are provided	(1) More computation overhead (2) vehicles have low storage capability; not an advisable option to become a node of blockchain	Impersonation attack, Man-in-the-middle attack, Message modification attack
6.	Lin et al. 2020 [140]	(1) Supports batch verification of messages (2) does not require to store the number of keys (3) key derivation mechanism based on blockchain has provided	No real word scenario has considered	Majority attack, Message modification attack, Replay attack, Man-in-the-middle attack
7.	Vangala et al. 2020 [123]	(1) This scheme generates the session keys between the vehicle-cluster head and cluster head-RSU (2) Moderate computation and communication overhead	(1) More time is required to create a new block (1) limited event scenario has considered	Replay attack, Man-in-the-middle attack, Impersonation attack, Privileged-insider attack, Physical capture attack
8.	Bagga et al. 2020 [124]	(1) Supports batch verification of messages (2) support ephemeral secret leakage attack (3) in each cluster, group key is established (4) moderate block verification time	(1) More time is required to create a new block (2) computationally expensive scheme	Replay attack, Man-in-the-middle attack, Impersonation attack, Privileged-insider attack, Physical capture attack
9.	Ma et al. 2020 [125]	(1) Supports smart contract for public key management (2) supports authentication and key agreement (3) Support execution of smart contract under the external test-net	Does not analyze insider and sybil attacks	Collusion attack, public key tampering attack
10.	Liu et al. 2020 [126]	(1) Supports unlinkable authentication of multiple messages (2) supports distributed authentication of vehicles (3) supports moderate block confirmation time	(1) Does not resist from collusion attack (2) does not analyze the model through the simulations (3) No real word scenario has considered	Man-in-the-middle, Replay attack

etc. Many blockchain platforms, such as ethereum, support smart contracts. Smart contracts are a few lines of codes or programs that can permanently reside on every blockchain node and execute automatically when predefined conditions are met. It removes the barrier associated with physical contracts and provides trust and transparency to the system. The researchers suggested blockchain-enabled smart contracts for automation such as money is directly transferred to the user, toll collection, parking-slot fee collection, etc. Various programming languages such as solidity are available for writing smart contracts. Oyente, SmartCheck, ChainSecurity, etc., are a few of the openly available tools that can verify the security of the developed smart contracts against the commonly known attacks and vulnerabilities.

Authors in [3] suggest the two smart contracts, named DSSC and ISSC, which are deployed on the vehicular network to provide the secure and decentralized sharing of data. The DSSC is used for the distributed data storage among the edge nodes. The proof-of-storage is used for this. The ISSC is used for information sharing among the edge nodes. The PoW is used for this. They utilize asymmetric cryptography and Elliptic curve digital signature to preserve the identity of the vehicle and for the block authentication process. RSUs act as the miner nodes and the consensus mechanism is executed on the preselected RSUs. But how to select the miner node is out of the scope of this paper.

To match the supply and demand of the resources, authors in [107] suggested the smart contracts-based system. The trustworthiness of the vehicles decides its reputation value which is further used in the PoR algorithm. In their scheme, RSUs are considered as blockchain nodes, so only RSUs are considered for the consensus process. The benefit of this algorithm is that less computational power is required compared to the other consensus algorithm such as PoW. On the other hand, it also motivates the vehicles to participate in the resource-sharing process. The differentiated resource pricing scheme is used for the same purpose.

Very few authors develop their smart contracts-based system and evaluate it. Most of the authors only provide theoretical analysis. The deployment of smart contracts on various blockchain platforms and vulnerabilities associated with the smart contracts are not discussed.

Table 14
Comparison table based on different parameters of the existing privacy-preserving work in VANETs.

S.No.	Ref.	Services	Block chain type	Blockchain specific challenge addressed	Miner node	Main characters	Technology
1.	Li et al. 2018 [101]	Preserve Vehicle identity	PRB	BFT Consensus mechanism	VEHs and RSUs	Vehicle, RSU, Trusted authority, Cloud server	Blockchain, Authentication, Incentive, Combined public-key
2.	Singh et al. 2017 [106]	Pseudonymity	Not Investigated	PoD consensus	VEHs	Vehicle, IVTP	Blockchain, Vehicle cloud computing, Digital signature
3.	Shi et al. 2020 [138]	Pseudonymity	Not Investigated	Not investigated by the authors	Not Investigated	Electric vehicle, RSU, Trusted authority	Ethereum blockchain, Authentication
4.	Noh et al. 2020 [112]	Anonymity of vehicles	PRB	PoW and PBFT consensus algorithm	Local trusted authority	Trusted authority (RTA, LTA), RSU, Vehicle	Blockchain, BAN-logic, Authentication
5.	Kong et al. 2020 [113]	Location privacy	PRB	BFT consensus algorithm	RSUs	RSU, Vehicle, Server, Trusted authority	Blockchain, Homomorphic 2-DNF, Identity-based signcryption
6.	Ming et al. 2020 [143]	Anonymity of vehicles	Not Investigated	Not investigated by the authors	Not Investigated	Trusted authority, Fog nodes, Cloud center, Vehicle	Blockchain, Elliptic curve (authentication), MIRACL crypto SDK
7.	Akhter et al. 2021 [146]	Preserve Vehicle identity	Not Investigated	Not investigated by the authors	Not Investigated	Vehicles, RSU, Authentication center	Truffle, Ganache emulator, Metamask
8.	Shen et al. 2020 [127]	Conditional anonymity for vehicles identity	CB	Incentive mechanism	RSU	Vehicles, RSU	MIRACL library, Blockchain
9.	Liu et al. 2019 [128]	Conditional privacy of vehicles identity	PRB	PoW and PBFT consensus	RSU	Trusted authority, Vehicles, RSU	Golang, Python
10.	Li et al. 2019 [129]	Preserve the vehicular identity	PRB	PoW consensus	Agent node	Vehicles, RSU, CA server (or) data storage server, Agent node:	OPNET, Ethereum

PRB: Permissioned Blockchain, CB: Consortium blockchain VEHs: Vehicles, RSUs: Roadside Units.

In the continuation of this, Javed et al. [108] proposed the blockchain-based secure data sharing and data storage system for vehicles which are distributed at different locations in the vehicular network. The proposed approach utilizes the proof-of-authority consensus mechanism to validate a new transaction instead of the PoW algorithm. The amount of GAS consumed by the proof-of-authority is less in comparison to the PoW. It also utilizes the caching system that frequently stores the used services. The simulation results show that the proposed system consumed less GAS (decreased by almost 15% to 20%) when using proof-of-authority instead of PoW.

The low accuracy model of vehicular GPS directly impacts on system's robustness and security. To improve vehicular GPS, authors in [114] proposed a novel framework based on cooperative positioning and blockchain. The deep neural network with multi-traffic signs is used to reduce the positioning of common vehicles. The deep learning-based distance calculation and prediction algorithm are also used to compute the distance between lidar-aided intelligent vehicles and traffic signs. Smart contracts are designed to evaluate the positioning error of vehicles. As a result, the correct data requester will be selected and rewarded. The authors proposed two smart contracts, one for DNN model parameters sharing and the second for positioning error sharing. The simulation result validates the proposed scheme in terms of distance prediction and vehicular positioning error.

In [115], the authors proposed the blockchain-based event information-sharing mechanism for a smart city. They proposed the two-phase validation scheme. The first phase deals with the transaction (event) validation protocol, whereas the block validation scheme is discussed in the second phase of the proposed system. Because of the more computational and storage power than vehicles, RSU creates the block and maintains the blockchain ledgers. A novel smart contract mechanism for the secure sharing of events is also discussed in the paper. The authors suggest PUF to achieve vehicle authentication. The total communication cost for phase-1 and phase-2 is 896 bits and 2816 bits, respectively, under consideration for one vehicle and one RSU. The authors only discuss the theoretical aspect of exchange control for IoV. The evaluation of smart contracts is not discussed by the authors.

In [142], the authors addressed the various drawbacks of a centralized VANET system and suggested the proposal for the self-managed VANET structure. The proposal includes the challenge–response-based authentication procedure and ethereum blockchain. They developed an ethereum smart contracts system that mostly focused on the subscription process. Mandatory applications such as vehicle insurance, traffic regulation, and vehicle tax can be developed on top of this framework.

The traditional VANET system utilizes a third party for managing the data that can improve the transportation system. As a result, they use the conventional centralized data storage mechanism (such as cloud

Table 15
Strengths, weaknesses and attacks counteracted of the existing blockchain-based privacy-preserving work in VANETs.

S.No.	Ref.	Strengths	Weaknesses	Attack counteracted
1.	Li et al. 2018 [101]	(1) Reputation points based incentive protocol (2) Protocol is reliable for forwarding the announcement messages (3) a real scenario has considered to show the effectiveness of the scheme	(1) key-management and decentralized authentication protocol has not incorporated in the presented solution (2) The BFT protocol may not work if more number of malicious vehicles are present in the network	Sybil attack, Replay attack, Message modification attack, Man-in-the-middle attack
2.	Singh et al. 2017 [106]	Reward based system; encourages vehicles to participate in the system (2) supports moderate verification model	(1) Vehicles has low computing and storage capabilities; may not participate as blockchain node (2) does not analyze the model using the simulators	Not investigated
3.	Shi et al. 2020 [138]	(1) Supports identity privacy protection and identity authentication (2) this model can be used for decentralized authentication of vehicles	Does not support location privacy protection model	Message modification attack, Replay attack
4.	Noh et al. 2020 [112]	(1) Strong consensus protocol has provided (2) supports distributed authentication of messages (3) supports multi-vehicular network model	(1) More computation overhead (2) vehicles have low storage capability; not an advisable option to become a node of blockchain (3) the formal analysis of the model not provided	Impersonation attack, Man-in-the-middle attack, Message modification attack
5.	Kong et al. 2020 [113]	(1) Supports identity based signcryption to preserve the vehicle's privacy (2) supports access rights for permissioned blockchain (3) supports high mobility of vehicles	(1) Supports high computation overhead (2) not simulated the model under the vehicular network environment	Modification attack
6.	Ming et al. 2020 [143]	(1) Supports location privacy, identity privacy, and unlinkability of messages (2) supports fog computing paradigm to reduce the computational overhead at the server side	(1) Does not support full decentralization (2) no simulation under the real environment has provided	Modification attack, Replay attack, Impersonation attack, Man-in-the-middle attack
7.	Akhter et al. 2021 [146]	(1) Supports multi-blockchain model (2) Supports distributed authentication protocol and cluster-based medium access control (3) provide more scalability	(1) Does not investigate the underline cryptographic protocols supported by the scheme (2) does not support the reputation mechanism and abnormal behaviors of vehicles	Replay attack, Man-in-the-middle attack, Modification attack, Sybil attack
8.	Shen et al. 2020 [127]	With the involvement of offline the certificate authority, the constant complexity $0(1)$ is required to achieve the conditional privacy of vehicle identity	Does not investigate, which kind of incentive mechanism has utilized	Man-in-the-middle attack, Background analysis attack
9.	Liu et al. 2019 [128]	(1) Supports identity based group signature scheme to achieve privacy (2) The logistic regression is used for the calculation of vehicle's trust, and further identification of malicious vehicles	(1) Vehicle message reliability is depends on its reputation value; not a fully trusted system (2) block generation and confirmation time is high	Anti-forgery attack, Replay attack, Integrity attack, Majority attack
10.	Li et al. 2019 [129]	(1) Supports privacy of vehicle's identity (2) supports forming of vehicular groups (3) Connectivity and average distance are used for measuring the effectiveness of the k-anonymity unity algorithm that is further used to preserve the location of vehicles	(1) Does not analyze the authentication and key-agreement protocols (2) does not analyze the smart contracts in details	Not investigated

servers) for storing it. In order to solve this issue, authors in [130] proposed a solution that utilizes the notion of IPFS. IPFS is a kind of distributed database that can solve the storage issues associated with the traditional system. In their system, RSU first verifies the data that was sent by the vehicles. After verifying it, they store the data in the IPFS. In addition to this, the authors also use each vehicle's reputation value and an incentive mechanism based on the correctness of events signed by the vehicles. Their system utilizes the ethereum enabled smart contracts through which the address of data is stored in the Blockchain. The authors utilize the Oyente tool to check smart contracts' security, such as Transaction-ordering dependence, Re-entrancy Vulnerability, and many more. The smart contracts are implemented using the solidity language, and Ganache and Metamask are also used for testing purposes. Moreover, the smart contracts are deployed both in local (Javascript VM) and external test networks.

To establish trust among the untrusted vehicles and better efficiency, consistency, and privacy in the VANET system, Singh et al. [131] presented the smart contracts enable decentralized and adaptive trust management system for the IoV environment. Their scheme utilizes the notion of blockchain sharding (divide the transaction loads on the full blockchain node into the several sub-blockchain nodes) that reduces the load on the blockchain, and at the same time, increases the transaction throughput. In addition to the sharding mechanism, the authors also considered the incentive mechanism and smart contracts that strengthen the trust management of their system. The certificate authority (or) traffic authority is responsible for deploying smart contracts in their system. The RSU acts as a miner node, and under the

Table 16
Comparison table based on different parameters of the existing smart contracts work in VANETs.

S.No.	Ref.	Services	Block chain type	Blockchain specific challenge addressed	Miner node	Main characters	Technology
1.	Kang et al. 2018 [3]	DSSC & ISSC	Not Investigated	Consensus, Smart Contracts	RSUs	RSU, Vehicle, Cloud, Central authority, Base station	Similar to bitcoin blockchain, Smart contracts
2.	Chai et al. 2019 [107]	Demand and supply of resources	CB	Smart contract and consensus algorithm.	RSU	RSU, Vehicle	Consortium blockchain, Smart contracts
3.	Javed et al. 2020 [108]	Ethereum (solidity) and IPFS-based secure system	PRB	Proof-of-authority consensus algorithm, Smart contracts	Not Investigated	RSU, Edge computing nodes, Cache server, IVTP	IPFS, Caching technology, Ethereum, RemixIDE
4.	Song et al. 2020 [114]	Improving vehicle global positioning system accuracy	Not Investigated	DPoS consensus, smart contracts, Incentive	RSUs	Intelligent vehicle, Road segment, DL model, RSU	Blockchain, Smart contracts, Deep learning
5.	Dwivedi et al. 2020 [115]	Exchange control — application in smart cities	PRB	PoW consensus, smart contracts	Vehicle, RSUs	Vehicle, RSU, Cloud server	Blockchain, Smart contracts
6.	Leiding et al. 2016 [142]	Ethereum blockchain-traffic regulation and vehicle tax application	PB	Smart contracts, Incentive	RSUs	Vehicle, RSU	Ethereum blockchain
7.	Khalid et al. 2021 [130]	Data storage (IPFS) and incentive provisioning (reputation value) system	PB	Smart contracts, Incentive	RSU	Certificate authority, RSU, Vehicles	Ethereum Blockchain, IPFS, Solidity
8.	Singh et al. 2020 [131]	Detection and revocation of misbehaving nature of vehicles	PRB	Smart contracts, Incentive	Traffic authority, RSU	Traffic authority, RSU, Regional authority, Vehicles, a Certificate authority	Ethereum Blockchain, Smart contracts
9.	Feng et al. 2019 [132]	Credibility of transmitted messages, and conditional anonymity for vehicles private information	PRB	Smart contracts	RSU	Trusted authority, RSU, Vehicles	Blockchain, Smart contracts
10.	Chen et al. 2020 [133]	Improvement of data sharing scheme for vehicular system	Not Investigated	Smart contracts	Not Investigated	A trust center, data owners, data users	Blockchain, Hyperledger fabric v1.4.2

PB: Permissionless Blockchain, PRB: Permissioned Blockchain, CB: Consortium Blockchain, PRB: Permissioned Blockchain, RSUs: Roadside Units.

simulation work, they recorded the average execution time and average throughput time for 1-miner, N/2-miner, and N-miners and deployed it to the private blockchain network.

To achieve the credibility and accuracy of the transmitted messages in the VANET system, authors in [132] proposed a blockchain-assisted novel framework that preserves the privacy of vehicles and does the authentication of vehicles automatically. Their scheme does not require any registration center except the initialization phase, deployment of smart contracts, and revocation. The smart contracts are written in JavaScript and deployed under the Hyperledger Fabric-based consortium blockchain platform. Authors in [133] proposed a Blockchain-assisted proxy re-encryption with the equality test for the vehicular system. Their system uses smart contracts that provide transparency in the matching process. It supports the equality test under dynamic authorization and ciphertexts in the multi-user model by combining proxy re-encryption and Public-key encryption functions with the equality test. In addition to this, the suggested smart contracts are implemented by using the hyperledger fabric v1.4.2 blockchain platform.

The dissemination of fake advertisements is one of the biggest challenges in the vehicular network. On the one side, the vehicles broadcast fake advertisements in the network to obtain higher rewards. On the other side, many vehicles are not participating in this process due to their privacy problems. As a result, there is a trade-off between these two. To solve this problem, authors in [134] proposed a blockchain-assisted fair and anonymous scheme for the dissemination of advertisement in vehicular networks. The Merkle hash tree with the proof-of-ad-receiving property provides fairness in the system. In addition to this, the smart contracts are used by the authors for providing the dissemination reward (punish and reward mechanism) to the vehicles, and the zero-knowledge proof technique is used to protect the privacy of the vehicle. Tables 16 and 17 summarize the existing blockchain-based smart contract-based systems designed for VANET applications with their strength and weaknesses.

4. Discussion on relevant security attacks

This Section presents the relevant security attacks possible in the VANET system. The state-of-the-art research used cryptographic primitives with blockchain to show that the VANET system is free from various attacks. Tables 7, 9, 11, 13, 15, and 17 summarize how different attacks were mitigated based on their category and problem formulation.

Table 17
Strengths, weaknesses and attacks counteracted of the existing blockchain-based smart contracts work in VANETs.

S.No.	Ref.	Strengths	Weaknesses	Attack counteracted
1.	Kang et al. 2018 [3]	(1) Adopt reputation mechanism for data sharing among vehicles (2) smart contract has utilized for secure sharing of vehicular data (3) consortium blockchain for data storage; applicable for real-time scenarios	(1) Does not evaluate the supporting smart contracts (2) the vulnerability associated with the smart contracts have not addressed	Majority attack, Modification attack
2.	Chai et al. 2019 [107]	(1) Differentiated pricing scheme matches the demand and supply condition of resources (2) less computation overhead due to the proof-of-reputation consensus mechanism	(1) Only theoretical model of smart contracts have presented (2) does not evaluate the smart contract vulnerabilities	Double-spending attack, Majority attack
3.	Javed et al. 2020 [108]	(1) Supports off-chain storage of vehicular data (1) Supports depth analysis of suggested smart contract (3) supports security and vulnerability analysis of smart contract	Does not supports the evaluation of smart contract under the external test networks	Vulnerabilities of smart contract, Man-in-the-middle attack
4.	Song et al. 2020 [114]	(1) Supports smart contract for data sharing and reward mechanism (2) Supports deep neural network based distance calculation, prediction and vehicle error positioning scheme	(1) Does not evaluate the cryptographic mechanism behind the data sharing (2) does not evaluate the supporting smart contracts	Not investigated
5.	Dwivedi et al. 2020 [115]	(1) Supports detection of event and its validation (2) Supports smart contracts as state machine model for sharing of events	(1) Only theoretical model of smart contracts have presented (2) does not evaluate the smart contract vulnerabilities (3) does not compare the computation and communication overhead with the other schemes	Integrity attack
6.	Leiding et al. 2016 [142]	Supports ethereum blockchain enabled self-managed VANET system	(1) Only theoretical analysis of the model has presented (2) smart contract and its implication has not discussed	Not investigated
7.	Khalid et al. 2021 [130]	(1) Supports off-chain storage of vehicular data (2) supports formal analysis of the smart contracts (3) support evaluation of smart contract (4) supports incentive and reputation model	(1) Does not analyze and compare the incentive model with others (2) Does not supports the evaluation of smart contract under the external test networks	Replay attack, Vulnerabilities of smart contract
8.	Singh et al. 2020 [131]	(1) Supports sharding blockchains enabled an adaptive trust management (2) Supports high transaction throughput (3) supports testbed setup implementation of blockchain	Does not evaluate, which test-net is used to deploy and run the smart contracts	Not investigated
9.	Feng et al. 2019 [132]	(1) Supports hyperledger fabric based smart contracts (2) Supports attributed-based encryption	(1) Supports high computational overhead (2) deeper analysis of hyperledger fabric based smart contracts and associated vulnerability has not discussed	Offline password guessing attack, Replay attack, Impersonation attack
10.	Chen et al. 2020 [133]	(1) Supports proxy re-encryption with the equality test (2) Supports hyper-ledger fabric as blockchain platform (3) supports smart contracts that automated the system	(1) More computational complexity involve (2) the various vulnerability associated with the suggested smart contracts is not discussed	Not investigated

- **Sybil attack:** In a Sybil attack, the attacker generates numerous nodes' identities, and using these multiple identities, the attacker tries to disseminate the fake messages across the decentralized peer-to-peer network. Using this, the attacker first attempts to control the network, launches the various fake messages, and carries out illegal activities (for instance, refusing the transactions) [147]. The attacker creates an illusion for the honest nodes by generating multiple identities and flooding the same messages in the network. The honest nodes believe that the message is correct, and accordingly, they take action. The adoption of blockchain in the VANET is one of the fittest solutions to mitigate this attack. Once the vehicle has registered in the blockchain system, it cannot acquire multiple identities. Moreover, the blockchain can be used as an authentication of vehicles. If vehicles (or attackers) get a fake identity, they are easily caught by the other parties of the blockchain.
- **Node impersonation attack:** Under the node impersonation attack, the attacker tries to steal vehicles' private information (for instance, vehicles identity) and pretends like a legitimate vehicle. The attacker and legitimate user of the vehicle use the same information to send the messages to other vehicles and RSUs. Once the attacker successfully launches this attack, it can change the trustworthy messages of legitimate vehicles. It is also possible that both the legitimate vehicle and attacker send different messages using the same information. As a result, the receiving vehicles and RSUs get confused and do not take the appropriate actions; chaos for choosing the trustworthy message. In order to handle this attack, various cryptographic mechanisms (for instance, identity-based cryptography) are utilized in the VANETs. The blockchain mechanism on the top of the cryptographic mechanism provided more security and trust such that it is almost impossible for the attacker to impersonate vehicles and RSU. Moreover, under the adoption of the blockchain mechanism, the peer nodes are completely anonymous when messages are transmitted over the public channel. The attacker cannot guess the identity and other private information based on the public information (hardness problems of cryptographic mechanisms such as ECDLP).

- **Man-in-the-middle attack:** In the man-in-the-middle attack, the attacker positions itself between two authorized entities who are continuously engaging in the data-sharing process. When the message has transmitted over the public channel, the attacker steals the information, modifies it, and then places the modifying information to the public channel. As a result, receiving authority does not get the original message, and finally, it takes the wrong decision. To mitigate this attack, researchers utilize the various cryptographic primitives and algorithms (for instance, hash functions). They assured that the messages and sensitive private information do not share in the plain-text format over the public channel. As a result, it is difficult for the attacker to modify the partial (or) entire message. On the other side, the receiver first recomputes the few parameters to get the original message. The blockchain mechanism strengthens the VANET system, and chances for launching the man-in-the-middle attack are less. In the worst case, the attacker needs more than half of the network's total bandwidth to launch this attacker, which is an infeasible task.
- **Replay attack:** Replay attacks are carried out when an attacker with unauthorized access joins a network, accesses a message from a public channel, and then transmits a copy of that message to the intended recipient. In this assault, the attacker poses as a valid user, and the recipient is led to believe that s/he is receiving the same message twice from the same source. The system's authenticity and confidentiality are targeted using this attack. Time-stamp and session key are the best methods to prevent this attack. Under the time-stamp method, the message is encapsulated with the time-stamp. If the message is received within a certain limit, it is accepted. Whereas, once the communicating parties have used the session key, it cannot be reused. Blockchain mechanism with the support of various cryptosystems prevents this attack because a unique time-stamp has attached in every transaction and block.
- **Vulnerabilities of smart contract:** Smart contracts are the predefined scripts deployed on the decentralized applications and built on top of the blockchain consensus protocols. It provides a conflict-free and transparent environment, making it possible for the users to reach the final agreements. One of the most significant concerns related to smart contracts is the security of the code that powers them [148]. While developing smart contract-based applications, it is important that the code must be kept safe and secure. Because if any security flaws exist in code, it might put the application and its users at risk. Furthermore, the organization may suffer from huge financial losses. Various security tools such as SmartCheck, Oyente, Securify, etc., are available to check the vulnerabilities associated with the smart contracts. SmartCheck is a static analysis and pattern-based tool that was created using the Java programming language. It performs syntactical and lexical analysis on solidity code. It makes use of XPath to determine whether or not a vulnerability pattern exists in the code. There are a variety of security concerns related to code being checked, such as costly loop, DoS by external contract, reentrancy attack, and so forth. On the other hand, the Oyente analyzer performs symbolic execution on contract functions and determines whether or not the code is susceptible to vulnerabilities. It divides the vulnerabilities into the following categories: timestamp-dependent vulnerabilities, transaction-ordering vulnerabilities, re-entrance handling vulnerabilities, and poorly handled exceptions vulnerabilities.
- **Privileged insider attack:** Under the privileged insider attack, an attacker is a network privileged user who has been granted access to cryptographic information about the entities that have been deployed in the network. This information includes certificates and private keys. Detecting this kind of attacker is difficult because if it gets private keys or other sensitive information, it can launch various attacks and change the message stored in the servers. However, with the usage of the latest cryptosystem and technologies, it is possible to mitigate this attack. The blockchain is the ideal candidate for this. In the blockchain-based system, all the network entities maintain the same copy of the ledger. Therefore, as a privileged-insider user, if the attacker tries to modify the payload information of any block, it must modify the entire ledger of blockchain, starting from the current block index up to the last block, which is computationally not feasible for an attacker. Furthermore, the underlying cryptosystem ensures that the sensitive information does not share with any other entity, including the registration authority at the registration phase (in case of permissioned blockchain).
- **Physical capture attack:** The attacker may physically seize the vehicles on a physical capture attack because of the antagonistic environment. The attacker utilizes the power analysis attacks [149] for extracting the stored parameters from the OBU of the compromised vehicle. To prevent the vehicle from this attack, the actual parameters required for the login and authentication in the system should not store in the OBU of the vehicles. It is essential that the vehicle computes the different and new parameters based on the actual parameters and then stores them. As a result, the parameters obtained from the power analysis attack are not helpful for login and authentication in the system. Finally, the attacker cannot communicate with the other vehicles and RSU of the system. The research community is developing protocols with the combination of the underlying cryptosystem, ECC, and distributed ledger technology, blockchain by which they can mitigate this attack.
- **Message modification attack:** The message modification (or) substitution is a kind of attack where the attacker modifies the messages exchanged during the V2V and V2I communication from the public channel. This attack focuses on the integrity of the message, and if the attacker has successfully launched this attack, the message's integrity no longer remains. Due to this reason, this attack is also called an integrity attack. The cryptographic primitives hash functions with the support of a robust encryption scheme can mitigate this attack. Furthermore, In the blockchain mechanism, messages (or transactions) are verified by more than half of the peer's nodes. After achieving the consensus from peer nodes, the message is stored in the blockchain. Therefore, the attacker needs to change the messages sent to every peer's nodes in order to launch this attack.
- **Majority attack:** When the attacker or the group of Sybil nodes under the attacker's influence acquires the majority of the network hash rate, s/he can launch the majority attack to manipulate the blockchain. The majority attack is a very powerful attack for the blockchain-based applications because if the attacker gets the majority of the network's hash rate, it can launch a number of attacks [150] such as (i) an attacker provide it consensus for the invalid transactions, and as a result, the invalid transaction is included in the blockchain (ii) an attacker can launch the double-spending attack, i.e., the same transaction spent twice on the different account addresses (iii) split the blockchain network using forking mechanism, etc. The underlying blockchain structure with a strong consensus mechanism can mitigate this attack. The authors [117,120] provide a mathematical model to prove that their incorporated model is free from majority attack. Due to the attacker's influence, the majority attack is also called a 51% attack.

5. Highlighted issues

Blockchain-as-a-service (BaaS) allows industries (or companies) to integrate blockchain with their business model. The integration of blockchain technology in the VANET system has the potential to transform the transportation system and significantly alters the many applications that can build on top of blockchain and VANET. In this empirical study, we have discussed the various blockchain-based state-of-the-art mechanisms that finally increase the security and trust in the IoV-enabled transportation system.

- **Apply AI/ML approach:** Along with the blockchain mechanism, some of the existing schemes applied the artificial intelligence and machine learning (AI/ML) technique [109,114,145] for solving the existing problems such as increasing the trust in the vehicular system, improving the accuracy of GPS, etc. while, other mechanism used only the blockchain for sharing the data (announcement messages). The machine learning algorithm evaluates the users' past activities (or vehicles) through the device (or OBU) for estimating the trust of the vehicles while sharing the sensitive information with RSU and nearby vehicles, which could enhance the efficiency and reliability of the transportation system.
- **Evaluation metrics:** In the state-of-the-art research, authors used the various kind of simulators such as SUMO [119,145], NS simulator [139] (NS-2, NS-3), Matlab [137], solidity [117], Ganache, etc. for evaluating their protocols and the same is compared with the existing schemes. Therefore, it is essential to standardize the evaluation metrics compared to the existing ones. However, only a few of the studies used the blockchain evaluation metrics (or platforms) ethereum [140], hyperledger fabric [133], and sawtooth, but none of these platforms are widely accepted as an evaluating standard.
- **Balancing data-sharing & trust:** One of the primary goals of IoV-enabled transportation is to secure sharing of vehicle data to other intelligent units so that if an adversary presents in the public channel, it cannot get the real information from the public channel. Blockchain is one innovative technology that provides trust among untrusted entities and achieves strong security. Although several studies based on incentives for the honest node [101,118], reputation and contract theory [104,108], PUF and certificates [117], have been proposed for achieving more trust in the VANET system. Most of the proposal is only at the early stage, and their real implementations still need to be developed. However, it is very challenging to design an appropriate incentive mechanism for VANET that can fulfill the requirements of diverse applications.
- **Resource constraints devices:** In VANETs, vehicles are equipped with resource-constrained devices which have limited computing and storage capability, poor network connection capability, and low battery power. However, the blockchain consensus algorithm such as PoW [98,125] requires high computing power and energy consumption, and message propagation latency is high in PBFT [116,123] consensus. Furthermore, the large size of blockchain data is infeasible for deploying across resource-constrained devices. As a result, it is impossible to store all blockchain data on each device. In addition to this, blockchain is mainly designed for an application with a strong network connection, whereas the devices in the VANETs suffers from the poor and unstable network connection.
- **Security vulnerability:** The integration of blockchain technology in the VANET can improve the system's security through encryption, digital signature, and hashing mechanism. But, the security of the system is still a major concern due to the vulnerability of the devices, and open wireless medium makes the devices suffer from various security breaches such as jamming, etc. Moreover, the traditional heavy-weight encryption algorithms are not feasible for the resource constraints devices, and very challenging to manage the keys of the devices in a blockchain-enabled distributed environment. In addition, the blockchain mechanism has its own security vulnerability, such as defects on smart contracts programs. Some of the well-known attacks on Ethereum smart contracts include reentrancy attacks, over and underflow attacks, short address attacks, etc.
- **Incentive mechanism in ITS:** The intelligent transportation system (ITS) is one of the applications of VANETs where intelligent vehicles share crucial information (such as traffic jams, road accidents, etc.) with other vehicles and road infrastructures (RSUs). The goal of ITS is to increase the efficiency of the transportation system and the safety of passengers. Many authorities (TMA, LEA, etc.) are involved in the current ITS. All these authorities take their independent decisions (lack of trust), making it more complicated. The emerging blockchain technology can overcome the limitations of ITS. With the utilization of blockchain in the ITS system, the upgraded blockchain-enabled ITS (B-ITS) operates in a decentralized manner. The authorities in B-ITS provide their consensus before recording any information into the blockchain. In B-ITS, when the honest nodes (vehicle's user) send the safety information, they must be incentivized. The existing incentive mechanism, which is based on the computationally difficult task (in the case of bitcoin), compensation for executing the contracts (in case of ethereum), and Vcoin system [98] may not fulfill the requirement of ITS because of its limitations such as resource constraints devices. Moreover, the incentive decrements mechanism discourages the nodes from contributing to the data-sharing process. Therefore, to ensure the stability of the blockchain system, it is crucial to design a proper incentive mechanism. The reputation and credit-based incentive mechanism can be a good option for VANET applications.
- **Scalability of B-ITS:** The scalability of the blockchain platforms limits the applicability of the blockchain in many different applications, including the VANET itself. Generally, scalability is measured in terms of the throughput of the transaction per second against the number of devices and their workload in the system. The bitcoin blockchain system executes only seven transactions per second, whereas the ethereum blockchain system processes nearly 15–20 transactions per second. Therefore, because of the poor scalability of the existing platform, they are not suitable for the VANET. The scalable consensus algorithm (a combination of PoW and PBFT) and directed acyclic graph-based blockchain structures are ideal candidates that can provide more scalability in the blockchain system.

6. Discussion on research issues

After the completion of literature reviews on the blockchain-based VANET system, we found the following potential research challenges, which are discussed below.

- In the vehicular ad-hoc network, security, and privacy of data, broadcast by the vehicles is the primary concern. The goal of the VANET system is to spread life-threatening messages across the network in a short period with accuracy. The event messages need to be transmitted securely to other entities so that only the legitimate vehicles can perform further processing. Malicious and unauthorized vehicles have not performed any activity on the event messages. The existing VANET system uses different cryptographic methodologies to solve the problem mentioned above. Some authors adopt the blockchain mechanism to provide more security and trust in the VANET system. Ref. [2,100,102] use the blockchain mechanism to provide the trust and correctness of the traffic events in the VANET system. But, in their work, the smart contracts mechanism and mining incentive problems are not fully addressed.

- Authentication of legitimate vehicles and managing the key pair is the next problem in the VANET system. Authentication of vehicles is necessary such that unauthorized vehicles are not sent false event messages to their neighboring vehicles. Authors, in [2,110] adopt the cryptographic primitives to preserve the vehicles identity and for vehicles authentication process. But, due to the number of vehicles are increasing day by day, managing the vehicle's key-pair is the big challenge in the VANET system.
- Presently, many researchers are focusing on the blockchain-based VANET system to secure the event messages exchange among the vehicles. The inherent feature of blockchain is suitable for the VANET system. The blockchain mechanism provides immutable records and creates a trust-less environment for sharing the vehicle's event messages. The consensus mechanism and smart contracts are the two main functions of blockchain technology. But, only a few of them, Refs. [3,98,99] suggested the consensus and smart contracts mechanism for the block verification and validation. Research in this direction is needed.
- Several existing VANET system is based on the data-centric model. The data-centric model considers only the event messages which are broadcasted by the vehicles. But, for the enhanced security, both the data-centric and entity-centric models, i.e., hybrid models, need to use in the VANET. Several researchers' Ref. [3,103,105] suggested the hybrid model based on the blockchain mechanism to preserve the privacy and security of the vehicle's messages. More research is needed to provide better trust in the VANET system.
- Scalability is one more issue that is associated with the blockchain-based VANET system. The number of vehicles is increasing at an exponential rate. Authors in [98,100,102] are tried to solve the above-mentioned issue by utilizing the more than one blockchain. But, still, the existing blockchain-based VANET system is not grappling with this problem. To deal with this problem, a proper framework is needed, which is scalable.
- The selection of miner node and mining incentives is the next issue associated with the blockchain-based VANET system. The miner node has to solve the cryptographic puzzle to validate a new block and add the new block to the existing blockchain. Some author's in [105,106] suggest vehicles as miner node whereas in [103,104] suggest RSU as miner node. In [101,135] suggest both vehicles and RSU work as the miner node. A better solution is needed, which solves the above-stated chaos and the mining incentive issue.
- The vehicles are more moveable in the VANET system. The mobility of vehicles is high as a comparison to other ad-hoc networks. Due to the vehicle's mobility, designing a proper access control mechanism for vehicles is challenging. Hence, the mobility nature of vehicles is also taken into account when designing the blockchain-based VANET system.
- The automated task is performed by the IoV-enabled autonomous vehicles. The OBU of the vehicles has strict network functionality, so it cannot scale up well when integrated with the decentralized blockchain network. The devices have limited computational power; as a result, most of them cannot engage in the consensus and mining procedures. In addition, they cannot have the required storage space to launch the complete copy of the blockchain [151]. Therefore, the limited degree of decentralization is achieved by the vehicular network. The permissioned blockchain platform such as hyperledger sawtooth is well-suited for resource-constrained devices because it defines the limited role of the nodes according to its limited functionality, and here, no need to store a full copy of the blockchain. Whereas, under the public blockchain, a computationally capable gateway [152] is required to push a transaction in the blockchain network.
- For applications beyond the cryptocurrencies, such as the IoV-based smart city applications, it is impossible to achieve full decentralization and high-speed transaction services. The mainstream financial systems have a higher transaction processing time as compared with the blockchain systems. The throughput of the PayPal system is the average of 193 transactions per second, whereas Visa achieves the same for 1667 transactions [153]. The popular permissionless cryptocurrencies (such as bitcoin and ethereum) have a throughput of only 3 to 20 transactions per second [154]. On the other hand, the cryptocurrencies based on the permissioned blockchain mechanism have a high transaction throughput but do not provide full decentralization for the system. In those systems, blockchain is run by an organization that is under centralized control. Therefore, it is inherently a trade-off between decentralization and transaction throughput.
- In recent years, AI/ML mechanisms have provided a revolutionary development for the IoV-enabled autonomous and connected vehicles, ultimately delivering efficiency and robustness in the transportation system. The machine learning algorithms work well in the presence of the teemingness amount of data available for tuning to the system, which results in intelligent decision-making to carry out the automated task. The autonomous vehicles collect the data from anonymous data sources through the various sensors, send it to the edge devices for further processing based on the AI/ML algorithm, and then store the optimized data in the blockchain. With the adoption of blockchain technology, many users contribute to the open data repositories (which improves the accuracy of machine learning models) to get more incentives from the system. Moreover, it provides enough opportunity for the researchers to leverage the blockchain and machine learning algorithm to enhance applications based on big data.
- The inherent features of blockchain provide enough security and trust to its application domains, but the security and execution of smart contracts are weak links in the underlying technology. The loopholes of the improper execution of smart contracts programs lead the adversary to launch various attacks such as DAO attack [12], overflow attack, Reentrancy attacks [155], etc. The security issue of smart contracts poses a new security challenge to the researchers and developers and encourages them to come up with a solution that automatically detects a common security vulnerability of the smart contracts. A direction of research when integrating the blockchain with the VANET system is developing the security standards for smart contracts so that there are no loopholes present in the smart contracts that could compromise the security of smart devices in the IoV.

7. Concluding remarks and future research

In this paper, we systematically reviewed the literature relating to the application of blockchain in VANET and classified existing blockchain-based solutions for vehicular applications.

We also identified a number of potential research opportunities based on the review of the existing literature. Not surprisingly, *security and privacy*, for example, those relating to the vehicle (owner), remain a key challenge, particularly as vehicles become more digitized and systems are more interconnected. It is also important to note that vehicles in the future may also include unmanned vehicles (e.g., aerial, ground, and water), and infrastructure components may not be fixed (e.g., roaming RSUs or transportation units). For example, how do we efficiently authenticate vehicles without incurring significant costs in storing and managing key pairs, particularly as the VANET system scales up and vehicles join and leave dynamically? As we noted in this paper, a large number of blockchain-based systems have been proposed to secure event message exchange within the VANETs, but no system is perfect or foolproof. For example, how do we maximize security and privacy protection without making the system impractical due to poor performance or complex user-design? Also, how do we integrate the integration of different blockchain systems operated by different organizations and for different purposes (e.g., blockchain-based VANET system with the blockchain-based smart grid system and blockchain-based building/facility management system?

As we noted in the preceding paragraph, performance is another key consideration in the design of practical blockchain-based solutions. One potential future research direction is designing an efficient and effective way of selecting miner nodes and determining mining incentives, particularly taking into consideration the dynamic nature of VANETS. Also, how can we better utilize AI to facilitate decision-making, say predictive analytics, which can improve users' quality of service/experience?

Declaration of competing 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.

Acknowledgments

The authors would like to thank the anonymous reviewers and the editor for their constructive feedback.

References

[1] Hien Phuong Luong, Manoj Panda, Hai L. Vu, Bao Quoc Vo, Beacon rate optimization for vehicular safety applications in highway scenarios, IEEE Trans. Veh. Technol. 67 (1) (2017) 524–536.

[2] Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, Zhenglin Liu, A privacy-preserving trust model based on blockchain for vanets, IEEE Access 6 (2018) 45655–45664.

[3] Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, Sabita Maharjan, Shengli Xie, Yan Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Internet Things J. (2018).

[4] Yasser Toor, Paul Muhlethaler, Anis Laouiti, Arnaud De La Fortelle, Vehicle ad hoc networks: Applications and related technical issues, IEEE Commun. Surv. Tutor. 10 (3) (2008) 74–88.

[5] Zhaojun Lu, Gang Qu, Zhenglin Liu, A survey on recent advances in vehicular network security, trust, and privacy, IEEE Trans. Intell. Transp. Syst. 20 (2) (2018) 760–776.

[6] Shanzhi Chen, Jinling Hu, Yan Shi, Ying Peng, Jiayi Fang, Rui Zhao, Li Zhao, Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G, IEEE Commun. Stand. Mag. 1 (2) (2017) 70–76.

[7] Anil Kumar Sutrala, Palak Bagga, Ashok Kumar Das, Neeraj Kumar, Joel JPC Rodrigues, Pascal Lorenz, On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of vehicles deployment, IEEE Trans. Veh. Technol. 69 (5) (2020) 5535–5548.

[8] Seunghwan Son, Joonyoung Lee, Yohan Park, Youngho Park, Ashok Kumar Das, Design of blockchain-based lightweight V2I handover authentication protocol for VANET, IEEE Trans. Netw. Sci. Eng. (2022).

[9] Sanjeev Kumar Dwivedi, Ruhul Amin, Satyanarayana Vollala, Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET, IEEE/CAA J. Autom. Sin. 8 (12) (2021) 1913–1922.

[10] Sanjeev Kumar Dwivedi, Priyadarshini Roy, Chinky Karda, Shalini Agrawal, Ruhul Amin, Blockchain-based internet of things and industrial IoT: A comprehensive survey, Secur. Commun. Netw. 2021 (2021).

[11] Akanksha Kaushik, Archana Choudhary, Chinmay Ektare, Deepti Thomas, Syed Akram, Blockchain—Literature survey, in: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE, 2017, pp. 2145–2148.

[12] Nicola Atzei, Massimo Bartoletti, Tiziana Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, Springer, 2017, pp. 164–186.

[13] Lakshmi Siva Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2017, pp. 1–5.

[14] Sarah Bouraga, A taxonomy of blockchain consensus protocols: A survey and classification framework, Expert Syst. Appl. 168 (2021) 114384.

[15] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A Hoque, A survey of consensus algorithms in public blockchain systems for crypto-currencies, J. Netw. Comput. Appl. (2021) 103035.

[16] Florian Tschorsch, Björn Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2084–2123.

[17] Merve Can Kus Khalilov, Albert Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2543–2585.

[18] Mauro Conti, E. Sandeep Kumar, Chhagan Lal, Sushmita Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3416–3452.

[19] Iuon-Chang Lin, Tzu-Chun Liao, A survey of blockchain security issues and challenges., IJ Netw. Secur. 19 (5) (2017) 653–659.

[20] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar, A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. 126 (2019) 45–58.

[21] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017).

[22] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[23] Yang Lu, The blockchain: State-of-the-art and research challenges, J. Ind. Inf. Integr. 15 (2019) 80–90.

[24] Tiago M. Fernández-Caramés, Paula Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[25] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, Antonio Puliafito, Blockchain and iot integration: A systematic survey, Sensors 18 (8) (2018) 2575.

[26] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, Mubashir Husain Rehmani, Applications of blockchains in the Internet of Things: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1676–1717.

[27] Shaoan Xie, Zibin Zheng, Weili Chen, Jiajing Wu, Hong-Ning Dai, Muhammad Imran, Blockchain for cloud exchange: A survey, Comput. Electr. Eng. 81 (2020) 106526.

[28] Shubhani Aggarwal, Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Kim-Kwang Raymond Choo, Albert Y Zomaya, Blockchain for smart communities: Applications, challenges and opportunities, J. Netw. Comput. Appl. 144 (2019) 13–48.

[29] Kim-Kwang Raymond Choo, Zheng Yan, Weizhi Meng, et al., Blockchain in industrial IoT applications: Security and privacy advances, challenges, and opportunities, 2020.

[30] Konstantinos Christidis, Michael Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[31] Hong-Ning Dai, Zibin Zheng, Yan Zhang, Blockchain for internet of things: A survey, IEEE Internet Things J. 6 (5) (2019) 8076–8094.

[32] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, Kim-Kwang Raymond Choo, Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5 (1) (2018) 31–37.

[33] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, Helge Janicke, Blockchain technologies for the internet of things: Research issues and challenges, IEEE Internet Things J. 6 (2) (2018) 2188–2204.

[34] Bin Hu, Zongyang Zhang, Jianwei Liu, Yizhong Liu, Jiayuan Yin, Rongxing Lu, Xiaodong Lin, A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems, Patterns 2 (2) (2021) 100179.

[35] Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, Aruna Seneviratne, Integration of blockchain and cloud of things: Architecture, applications and challenges, 2019, arXiv preprint arXiv:1908.09058.

[36] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.

[37] Zeli Wang, Hai Jin, Weiqi Dai, Kim-Kwang Raymond Choo, Deqing Zou, Ethereum smart contract security research: survey and future research opportunities, Front. Comput. Sci. 15 (2) (2021) 1–18.

[38] Kimchai Yeow, Abdullah Gani, Raja Wasim Ahmad, Joel JPC Rodrigues, Kwangman Ko, Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues, IEEE Access 6 (2017) 1513–1524.

[39] Weiqin Zou, David Lo, Pavneet Singh Kochhar, Xuan-Bach D Le, Xin Xia, Yang Feng, Zhenyu Chen, Baowen Xu, Smart contract development: Challenges and opportunities, IEEE Trans. Softw. Eng. (2019).

[40] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, Debiao He, Blockchain in healthcare applications: Research challenges and opportunities, J. Netw. Comput. Appl. 135 (2019) 62–75.

[41] Partha Pratim Ray, Dinesh Dash, Khaled Salah, Neeraj Kumar, Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases, IEEE Syst. J. (2020).

[42] Shuyun Shi, Debiao He, Li Li, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey, Comput. Secur. (2020) 101966.

[43] Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Comput. Appl. (2021) 1–16.

[44] Ruizhe Yang, F Richard Yu, Pengbo Si, Zhaoxin Yang, Yanhua Zhang, Integrated blockchain and edge computing systems: A survey, some research issues and challenges, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1508–1532.

[45] Pronaya Bhattacharya, Sudeep Tanwar, Rushabh Shah, Akhilesh Ladha, Mobile edge computing-enabled blockchain framework—a survey, in: Proceedings of ICRIC 2019, Springer, 2020, pp. 797–809.

[46] Abdulla Chaer, Khaled Salah, Claudio Lima, Pratha Pratim Ray, Tarek Sheltami, Blockchain for 5G: opportunities and challenges, in: 2019 IEEE Globecom Workshops (GC Wkshps), IEEE, 2019, pp. 1–6.

[47] Ishan Mistry, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges, Mech. Syst. Signal Process. 135 (2020) 106382.

[48] Tejasvi Alladi, Vinay Chamola, Reza M Parizi, Kim-Kwang Raymond Choo, Blockchain applications for industry 4.0 and industrial IoT: A review, IEEE Access 7 (2019) 176935–176951.

[49] Umesh Bodkhe, Sudeep Tanwar, Karan Parekh, Pimal Khanpara, Sudhanshu Tyagi, Neeraj Kumar, Mamoun Alazab, Blockchain for industry 4.0: A comprehensive review, IEEE Access 8 (2020) 79764–79800.

[50] Umesh Bodkhe, Dhyey Mehta, Sudeep Tanwar, Pronaya Bhattacharya, Pradeep Kumar Singh, Wei-Chiang Hong, A survey on decentralized consensus mechanisms for cyber physical systems, IEEE Access 8 (2020) 54371–54401.

[51] Rajesh Gupta, Sudeep Tanwar, Neeraj Kumar, Sudhanshu Tyagi, Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review, Comput. Electr. Eng. 86 (2020) 106717.

[52] Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M Parizi, Kim-Kwang Raymond Choo, A systematic literature review of blockchain cyber security, Digit. Commun. Netw. 6 (2) (2020) 147–156.

[53] Raja Wasim Ahmad, Haya Hasan, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Mohammed Omar, Blockchain for aerospace and defense: Opportunities and open research challenges, Comput. Ind. Eng. 151 (2021) 106982.

[54] Amna Qureshi, David Megías Jiménez, Blockchain-based multimedia content protection: Review and open challenges, Appl. Sci. 11 (1) (2021) 1.

[55] Xi Li, Zehua Wang, Victor Leung, Hong Ji, Yiming Liu, Heli Zhang, Blockchain-empowered data-driven networks: A survey and outlook, 2021, arXiv preprint arXiv:2101.12375.

[56] Huawei Huang, Wei Kong, Sicong Zhou, Zibin Zheng, Song Guo, A survey of state-of-the-art on blockchains: Theories, modelings, and tools, ACM Comput. Surv. 54 (2) (2021) 1–42.

[57] Jiabin Bao, Debiao He, Min Luo, Kim-Kwang Raymond Choo, A survey of blockchain applications in the energy sector, IEEE Syst. J. (2020).

[58] David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, Yaser Jararweh, A survey on blockchain for information systems management and security, Inf. Process. Manage. 58 (1) (2021) 102397.

[59] Zhiyan Chen, Claudio Fiandrino, Burak Kantarci, On blockchain integration into mobile crowdsensing via smart embedded devices: A comprehensive survey, J. Syst. Archit. (2021) 102011.

[60] Arunima Ghosh, Shashank Gupta, Amit Dua, Neeraj Kumar, Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects, J. Netw. Comput. Appl. 163 (2020) 102635.

[61] Naveed Ul Hassan, Chau Yuen, Dusit Niyato, Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions, IEEE Ind. Electr. Mag. 13 (4) (2019) 106–118.

[62] Navid Khoshavi, Gabrielle Tristani, Arman Sargolzaei, Blockchain applications to improve operation and security of transportation systems: A survey, Electronics 10 (5) (2021) 629.

[63] Jing Liu, Zhentian Liu, A survey on security verification of blockchain smart contracts, IEEE Access 7 (2019) 77894–77904.

[64] Umer Majeed, Latif U Khan, Ibrar Yaqoob, SM Ahsan Kazmi, Khaled Salah, Choong Seon Hong, Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges, J. Netw. Comput. Appl. (2021) 103007.

[65] Arzoo Miglani, Neeraj Kumar, Vinay Chamola, Sherali Zeadally, Blockchain for internet of energy management: Review, solutions, and challenges, Comput. Commun. 151 (2020) 395–418.

[66] Urvish Thakker, Ruhi Patel, Sudeep Tanwar, Neeraj Kumar, Houbing Song, Blockchain for diamond industry: Opportunities and challenges, IEEE Internet Things J. (2020).

[67] Junfeng Xie, Helen Tang, Tao Huang, F Richard Yu, Renchao Xie, Jiang Liu, Yunjie Liu, A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2794–2830.

[68] Wenli Yang, Erfan Aghasian, Saurabh Garg, David Herbert, Leandro Disiuta, Byeong Kang, A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future, IEEE Access 7 (2019) 75845–75872.

[69] Zhihao Yu, Liang Song, Linhua Jiang, Omid Khold Sharafi, Systematic literature review on the security challenges of blockchain in IoT-based smart cities, Kybernetes (2021).

[70] Amritraj Singh, Kelly Click, Reza M Parizi, Qi Zhang, Ali Dehghantanha, Kim-Kwang Raymond Choo, Sidechain technologies in blockchain networks: An examination and state-of-the-art review, J. Netw. Comput. Appl. 149 (2020) 102471.

[71] Xiaoqiong Xu, Gang Sun, Long Luo, Huilong Cao, Hongfang Yu, Athanasios V Vasilakos, Latency performance modeling and analysis for hyperledger fabric blockchain network, Inf. Process. Manage. 58 (1) (2021) 102436.

[72] Sudeep Tanwar, Qasim Bhatia, Pruthvi Patel, Aparna Kumari, Pradeep Kumar Singh, Wei-Chiang Hong, Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward, IEEE Access 8 (2019) 474–488.

[73] Neeraj Kumar, N Gayathri, Md Arafatur Rahman, B Balamurugan, Blockchain, Big Data and Machine Learning: Trends and Applications, CRC Press, 2020.

[74] Khaled Salah, M Habib Ur Rehman, Nishara Nizamuddin, Ala Al-Fuqaha, Blockchain for AI: Review and open research challenges, IEEE Access 7 (2019) 10127–10149.

[75] Rajesh Gupta, Anuja Nair, Sudeep Tanwar, Neeraj Kumar, Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges, IET Commun. (2021).

[76] Aparna Kumari, Rajesh Gupta, Sudeep Tanwar, Neeraj Kumar, Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions, J. Parallel Distrib. Comput. 143 (2020) 148–166.

[77] Yang Liu, Debiao He, Mohammad S Obaidat, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, et al., Blockchain-based identity management systems: A review, J. Netw. Comput. Appl. (2020) 102731.

[78] Mohammad Dabbagh, Kim-Kwang Raymond Choo, Amin Beheshti, Mohammad Tahir, Nader Sohrabi Safa, A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities, Comput. Secur. 100 (2021) 102078.

[79] L. Ante, F. Steinmetz, I. Fiedler, Blockchain and energy: A bibliometric analysis and review, Renew. Sustain. Energy Rev. 137 (2021) 110597.

[80] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, Yonggang Wen, A survey on consensus mechanisms and mining management in blockchain networks, 2018, arXiv preprint arXiv:1805.02707.

[81] Satoshi Nakamoto, et al., Bitcoin: A peer-to-peer electronic cash system, 2008.

[82] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, Where is current research on blockchain technology?—a systematic review, PLoS One 11 (10) (2016) e0163477.

[83] Ahmed Afif Monrat, Olov Schelén, Karl Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151.

[84] Yang Lu, Blockchain and the related issues: a review of current research topics, J. Manage. Anal. 5 (4) (2018) 231–255.

[85] Erikson Júlio De Aguiar, Bruno S Faiçal, Bhaskar Krishnamachari, Jó Ueyama, A survey of blockchain-based strategies for healthcare, ACM Comput. Surv. 53 (2) (2020) 1–27.

[86] Mohammad S Obaidat, Sanjeev Kumar Dwivedi, Ruhul Amin, Kuei-Fang Hsiao, Blockchain enabled electronics medical system proposed framework with research directions, in: 2021 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2021, pp. 1–5.

[87] Ashik Khaleel, Kiran K. Nair, N. Praveen, A review on distributed management systems using blockchain., Int. J. Psychosoc. Rehabil. 24 (1) (2020).

[88] Bhabendu K Mohanta, Debasish Jena, Soumyashree S Panda, Srichandan Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, Int. Things (2019) 100107.

[89] Sanjeev Kumar Dwivedi, Ruhul Amin, Satyanarayana Vollala, Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism, J. Inf. Secur. Appl. 54 (2020) 102554.

[90] Arijit Saha, Ruhul Amin, Sourav Kunal, Satyanarayana Vollala, Sanjeev K Dwivedi, Review on "Blockchain technology based medical healthcare system with privacy issues", Secur. Priv. 2 (5) (2019) e83.

[91] Sara Rouhani, Ralph Deters, Security, performance, and applications of smart contracts: A systematic survey, IEEE Access 7 (2019) 50759–50779.

[92] Supriya Thakur Aras, Vrushali Kulkarni, Blockchain and its applications–A detailed survey, Int. J. Comput. Appl. 180 (3) (2017) 29–35.

[93] Florian Idelberger, Guido Governatori, Régis Riveret, Giovanni Sartor, Evaluation of logic-based smart contracts for blockchain systems, in: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer, 2016, pp. 167–183.

[94] Xiao He, Bohan Qin, Yan Zhu, Xing Chen, Yi Liu, SPESC: A specification language for smart contracts, in: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Vol. 1, IEEE, 2018, pp. 132–137.

[95] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun, A review on consensus algorithm of blockchain, in: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2017, pp. 2567–2572.

[96] Yang Xiao, Ning Zhang, Wenjing Lou, Y. Thomas Hou, A survey of distributed consensus protocols for blockchain networks, IEEE Commun. Surv. Tutor. (2020).

[97] Giang-Truong Nguyen, Kyungbaek Kim, A survey about consensus algorithms used in blockchain, J. Inf. Process. Syst. 14 (1) (2018).

[98] Lei Zhang, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, Shengwei Tian, Blockchain based secure data sharing system for Internet of vehicles: A position paper, Veh. Commun. 16 (2019) 85–93.

[99] Xiaohong Zhang, Xiaofeng Chen, Data security sharing and storage based on a consortium blockchain in a vehicular Ad-hoc network, IEEE Access 7 (2019) 58241–58254.

[100] Yao-Tsung Yang, Li-Der Chou, Chia-Wei Tseng, Fan-Hsun Tseng, Chien-Chang Liu, Blockchain-based traffic event validation and trust verification for VANETs, IEEE Access 7 (2019) 30868–30877.

[101] Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, Zonghua Zhang, Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles, IEEE Trans. Intell. Transp. Syst. 19 (7) (2018) 2204–2220.

[102] Rakesh Shrestha, Rojeena Bajracharya, Anish P Shrestha, Seung Yeob Nam, A new-type of blockchain for secure message exchange in VANET, Digit. Commun. Netw. (2019).

[103] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, Victor CM Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet Things J. 6 (2) (2018) 1495–1505.

[104] Jiawen Kang, Zehui Xiong, Dusit Niyato, Dongdong Ye, Dong In Kim, Jun Zhao, Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory, IEEE Trans. Veh. Technol. 68 (3) (2019) 2906–2920.

[105] Rakesh Shrestha, Rojeena Bajracharya, Seung Yeob Nam, Blockchain-based message dissemination in vanet, in: 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), IEEE, 2018, pp. 161–166.

[106] Madhusudan Singh, Shiho Kim, Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain, 2017, arXiv preprint arXiv:1707.07442.

[107] Haoye Chai, Supeng Leng, Ke Zhang, Sun Mao, Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles, IEEE Access 7 (2019) 175744–175757.

[108] Muhammad Umar Javed, Mubariz Rehman, Nadeem Javaid, Abdulaziz Aldegheishem, Nabil Alrajeh, Muhammad Tahir, Blockchain-based secure data storage for distributed vehicular networks, Appl. Sci. 10 (6) (2020) 2011.

[109] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, Yan Zhang, Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles, IEEE Trans. Veh. Technol. 69 (4) (2020) 4298–4311.

[110] Zhaojun Lu, Qian Wang, Gang Qu, Zhenglin Liu, Bars: a blockchain-based anonymous reputation system for trust management in vanets, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 98–103.

[111] Xiaoliang Wang, Pengjie Zeng, Nick Patterson, Frank Jiang, Robin Doss, An improved authentication scheme for internet of vehicles based on blockchain technology, IEEE Access 7 (2019) 45061–45072.

[112] Jaewon Noh, Sangil Jeon, Sunghyun Cho, Distributed blockchain-based message authentication scheme for connected vehicles, Electronics 9 (1) (2020) 74.

[113] Qinglei Kong, Le Su, Maode Ma, Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain, IEEE Trans. Intell. Transp. Syst. (2020).

[114] Yanxing Song, Yuchuan Fu, F. Richard Yu, Li Zhou, Blockchain-enabled internet of vehicles with cooperative positioning: A deep neural network approach, IEEE Internet Things J. 7 (4) (2020) 3485–3498.

[115] Sanjeev Kumar Dwivedi, Ruhul Amin, Satyanarayana Vollala, Rashmi Chaudhry, Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities, Comput. Electr. Eng. 86 (2020) 106719.

[116] Haoran Liang, Jun Wu, Shahid Mumtaz, Jianhua Li, Xi Lin, Miaowen Wen, MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X, IEEE Commun. Mag. 57 (10) (2019) 77–83.

[117] Uzair Javaid, Muhammad Naveed Aman, Biplab Sikdar, A scalable protocol for driving trust management in internet of vehicles with blockchain, IEEE Internet Things J. (2020).

[118] Muhammad Sohaib Iftikhar, Nadeem Javaid, Omaji Samuel, Muhammad Shoaib, Muhammad Imran, An incentive scheme for VANETs based on traffic event validation using blockchain, in: 2020 International Wireless Communications and Mobile Computing (IWCMC), IEEE, 2020, pp. 2133–2137.

[119] Muhammad Firdaus, Kyung-Hyune Rhee, On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks, Appl. Sci. 11 (1) (2021) 414.

[120] Jianfeng Ma, Tao Li, Jie Cui, Zuobin Ying, Jiujun Cheng, Attribute-based secure announcement sharing among vehicles using blockchain, IEEE Internet Things J. (2021).

[121] Di Wang, Xiaohong Zhang, Secure data sharing and customized services for intelligent transportation based on a consortium blockchain, IEEE Access 8 (2020) 56045–56059.

[122] Bohan Li, Ruochen Liang, Di Zhu, Weitong Chen, Qinyong Lin, Blockchain-based trust management model for location privacy preserving in VANET, IEEE Trans. Intell. Transp. Syst. (2020).

[123] Anusha Vangala, Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Young Ho Park, Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems, IEEE Sens. J. (2020).

[124] Palak Bagga, Anil Kumar Sutrala, Ashok Kumar Das, Pandi Vijayakumar, Blockchain-based batch authentication protocol for Internet of Vehicles, J. Syst. Archit. (2020) 101877.

[125] Zhuo Ma, Junwei Zhang, Yongzhen Guo, Yang Liu, Ximeng Liu, Wei He, An efficient decentralized key management mechanism for VANET with blockchain, IEEE Trans. Veh. Technol. 69 (6) (2020) 5836–5849.

[126] Jiao Liu, Xinghua Li, Qi Jiang, Mohammad S Obaidat, Pandi Vijayakumar, Bua: A blockchain-based unlinkable authentication in vanets, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–6.

[127] Huajie Shen, Jun Zhou, Zhenfu Cao, Xiaolei Dong, Kim-Kwang Raymond Choo, Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks, IEEE Internet Things J. 7 (7) (2020) 6610–6622.

[128] Xingchen Liu, Haiping Huang, Fu Xiao, Ziyang Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs, IEEE Internet Things J. 7 (5) (2019) 4101–4112.

[129] Hui Li, Lishuang Pei, Dan Liao, Gang Sun, Du Xu, Blockchain meets vanet: An architecture for identity and location privacy protection in vanet, in: Peer-To-Peer Networking and Applications, Vol. 12, (5) Springer, 2019, pp. 1178–1193.

[130] Adia Khalid, Muhammad Sohaib Iftikhar, Ahmad Almogren, Rabiya Khalid, Muhammad Khalil Afzal, Nadeem Javaid, A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs, Inf. Process. Manage. 58 (2) (2021) 102464.

[131] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, Kayhan Zrar Ghafoor, Danda B Rawat, Sukumar Nandi, Blockchain-based adaptive trust management in internet of vehicles using smart contract, IEEE Trans. Intell. Transp. Syst. (2020).

[132] Qi Feng, Debiao He, Sherali Zeadally, Kaitai Liang, BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks, IEEE Trans. Ind. Inf. 16 (6) (2019) 4146–4155.

[133] Biwen Chen, Debiao He, Neeraj Kumar, Huaqun Wang, Kim-Kwang Raymond Choo, A blockchain-based proxy re-encryption with equality test for vehicular communication systems, IEEE Trans. Netw. Sci. Eng. (2020).

[134] Ming Li, Jian Weng, Anjia Yang, Jia-Nan Liu, Xiaodong Lin, Toward blockchain-based fair and anonymous ad dissemination in vehicular networks, IEEE Trans. Veh. Technol. 68 (11) (2019) 11248–11259.

[135] Farah Kandah, Brennan Huber, Anthony Skjellum, Amani Altarawneh, A blockchain-based trust management approach for connected autonomous vehicles in smart cities, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2019, pp. 0544–0549.

[136] Madhusudan Singh, Shiho Kim, Blockchain based intelligent vehicle data sharing framework, 2017, arXiv preprint arXiv:1708.09721.

[137] Tigang Jiang, Hua Fang, Honggang Wang, Blockchain-based internet of vehicles: Distributed network architecture and performance analysis, IEEE Internet Things J. 6 (3) (2018) 4640–4649.

[138] Kexin Shi, Liehuang Zhu, Can Zhang, Lei Xu, Feng Gao, Blockchain-based multimedia sharing in vehicular social networks with privacy protection, Multimedia Tools Appl. (2020) 1–21.

[139] Geetanjali Rathee, Ashutosh Sharma, Razi Iqbal, Moayad Aloqaily, Naveen Jaglan, Rajiv Kumar, A blockchain framework for securing connected and autonomous vehicles, Sensors 19 (14) (2019) 3165.

[140] Chao Lin, Debiao He, Xinyi Huang, Neeraj Kumar, Kim-Kwang Raymond Choo, BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. (2020).

[141] Xinyang Deng, Tianhan Gao, Electronic payment schemes based on blockchain in VANETs, IEEE Access 8 (2020) 38296–38303.

[142] Benjamin Leiding, Parisa Memarmoshrefi, Dieter Hogrefe, Self-managed and blockchain-based vehicular ad-hoc networks, in: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, 2016, pp. 137–140.

[143] Yang Ming, Xiaopeng Yu, Efficient privacy-preserving data sharing for fog-assisted vehicular sensor networks, Sensors 20 (2) (2020) 514.

[144] Uzair Javaid, Muhammad Naveed Aman, Biplab Sikdar, DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–5.

[145] Chenyue Zhang, Wenjia Li, Yuansheng Luo, Yupeng Hu, AIT: An AI-enabled trust management system for vehicular networks using blockchain technology, IEEE Internet Things J. (2020).

[146] AFM Akhter, Mohiuddin Ahmed, AFM Shah, Adnan Anwar, Ahmet Zengin, A secured privacy-preserving multi-level blockchain framework for cluster based VANET, Sustainability 13 (1) (2021) 400.

[147] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, David Mohaisen, Exploring the attack surface of blockchain: A comprehensive survey, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1977–2008.

[148] Satpal Singh Kushwaha, Sandeep Joshi, Dilbag Singh, Manjit Kaur, Heung-No Lee, Systematic review of security vulnerabilities in ethereum blockchain smart contract, IEEE Access (2022).

[149] Thomas S. Messerges, Ezzat A. Dabbish, Robert H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.

[150] Rakesh Shrestha, Seung Yeob Nam, Regional blockchain for vehicular networks to prevent 51% attacks, IEEE Access 7 (2019) 95033–95045.

[151] Kamanashis Biswas, Vallipuram Muthukkumarasamy, Securing smart cities using blockchain technology, in: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2016, pp. 1392–1393.

[152] Ali Dorri, Marco Steger, Salil S. Kanhere, Raja Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Commun. Mag. 55 (12) (2017) 119–125.

[153] Jan Vermeulen, Bitcoin and Ethereum vs Visa and PayPal–Transactions per second, Vol. 22, My Broadband, 2017.

[154] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al., On scaling decentralized blockchains, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 106–125.

[155] Yongfeng Huang, Yiyang Bian, Renpu Li, J Leon Zhao, Peizhong Shi, Smart contract security: A software lifecycle perspective, IEEE Access 7 (2019) 150184–150202.

Sanjeev Kumar Dwivedi received his B.Tech Degree from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Madhya Pradesh in Computer Science and Engineering Department in 2010 and M.Tech Degree from Pondicherry University, Puducherry in Distributed Computing System Specialization (CSE Department) in 2013 respectively. Currently, he is pursing Ph.D. in the Department of CSE from Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, Chhattisgarh, India. He has a total academic experience of 4 years. He has published few research papers on blockchain in peer reviewed international journals such as IEEE/CAA Journal of Automatica Sinica, Journal of Information Security and Applications (Elsevier), and Computers & Electrical Engineering (Elsevier). His current research interests include Information Security, Cryptography, VANET Security, Blockchain Technology.

Ruhul Amin received his doctoral (Ph.D.) degree in Computer Science and Engineering from the Indian Institute of Technology(ISM) Dhanbad, Jharkhand, India, in 2017, as well as B.Tech and M.Tech both in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, India in 2009 and 2013, respectively. Presently, he is an Assistant Professor in the Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India. He is an Associate Editor of "Security and Privacy" and Security and communication networks published by John Wiley and Hindwai respectively. His research interest includes cryptography and network security, authentication protocol, WSN security, IoT security, and currently more focusing on blockchain technology.

Ashok Kumar Das received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He also worked as a visiting faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA. His current research interests include cryptography, network security, security in vehicular ad hoc networks, smart grids, smart homes, Internet of Things (IoT), Internet of Drones, Internet of Vehicles, Cyber–Physical Systems (CPS) and cloud computing, intrusion detection, blockchain and AI/ML security. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He was/is on the editorial board of IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), Journal of Cloud Computing (Springer), Cyber Security and Applications (Elsevier), IET Communications, KSII Transactions on Internet and Information Systems, and International Journal of Internet Technology and Secured Transactions (Inderscience). He is a senior member of the IEEE.

Mark T. Leung received a Ph.D. degree and a M.Bus. degree, both in operations management, from Indiana University, as well as a M.B.A. degree in finance (specializing in mathematical financial economics) from University of California. He is the Associate Dean of Undergraduate Studies in the Carlos Alvarez College of Business at The University of Texas at San Antonio (UTSA). His current research interests include artificial intelligence, autonomous machine learning, predicitive analytics, financial forecasting and algorithmic trading, supply chain system design, and operational analysis. He was a recipient of the UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award, The University of Texas System Chancellor's Council Outstanding Teaching Award for two times, The University of Texas System Regents' Outstanding Teaching Award, the Endowed 1969 Commemorative Award for Overall Faculty Excellence, and the Patrick J. Clynes Excellence in Service Faculty Award. He is on the editorial boards of Intelligent Systems in Accounting, Finance and Management, Systems, Modern Economy, Theoretical Economics Letters, and Archives of Behavioral Sciences. He has published in a variety of peer-reviewed international journals including Decision Sciences, Decision Support Systems, European Journal of Operational Research, Computers and Operations Research, Expert Systems with Applications, Journal of Banking and Finance, and International Journal of Production Economics.

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio. He is the founding co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, the founding Chair of IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies, an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021 - 2023), and a Web of Science's Highly Cited Researcher (Computer Science - 2021, Cross-Field - 2020). He is the recipient of the IEEE Systems, Man, and Cybernetics' Technical Committee on Homeland Security Research and Innovation Award in 2022, and the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), as well as best paper awards from IEEE Systems Journal in 2021, IEEE Computer Society's Bio-Inspired Computing Special Technical Committee Outstanding Paper Award for 2021, IEEE DSC 2021, IEEE Consumer Electronics Magazine for 2020, Journal of Network and Computer Applications for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015.

Satyanarayana Vollala received Ph.D. in CSE from National Institute of Technology, Tiruchirappalli, Tamilnadu, India, in 2017, as well as a Master of Technology in Computer Science and Engineering from Jawaharlal Nehru Technological University-Hyderabad, Andhra Pradesh. He is currently an Assistant Professor in the Department of CSE, Dr. Shyama Prasad Mukherjee International Institute of Information Technology Naya Raipur, Chhattisgarh, India, and a Co-PI of the 'Energy Efficient Implementation of Multi-modular Exponential Techniques for Public-key Cryptosys-tems' project, sponsored by ICPC, DST, India. His research interest includes Hardware security and theoretical computer science.