Blockchain for Securing Vehicular Networks: A Comprehensive Review

Anil Kumar Biswal[1], Divya Midhun[2], Dharmesh Dhabliya[3]
[1,2]Lincoln University College, Malasiya
[1]Udayanath Autonomous College of Science and Technology, Cuttack
[3]Vishwakarma Institute of Information Technology, Pune
[1]anil.biswal123@gmail.com

Abstract— **Vehicular networks offer capabilities like traffic control, route optimisation, data transmission, entertainment, and additional functionalities. Providing security is a challenge with any large-scale technological integration. To make the vehicular network more secure, blockchain technology has been chosen by numerous research. Decentralisation, transparency, immutability, and public auditing are some of the most important security criteria that it satisfies. This research compiles a list of some of the more noteworthy initiatives that have used this approach in recent years. From an application, security, and blockchain standpoint, we examine about seventy-five blockchain-based security strategies for vehicle networks. From an application standpoint, we look at transportation, parking, data sharing/trading, and resource sharing as some of the many opportunities for safe blockchain-based automotive networks. Both needs and threats related to security are the primary emphasis of the security perspective. Platforms, kinds, and consensus mechanisms of blockchains are the main points of view from a blockchain standpoint. Moreover, we have compiled the most widely used simulation tools for blockchain and vehicle network simulations. In order to provide readers with a more comprehensive understanding of the field, we also go over the function of different cutting-edge new technologies in blockchain-based vehicle networks. We conclude the survey by outlining the most prevalent difficulties and potential avenues for further study in this area.**

Index Terms—**Internet of Things (IoT), Blockchain, Internet of Vehicles (IoV), security, cryptography, authentication**

I. INTRODUCTION

In 2010, there were one billion automobiles on the road. By 2050, experts anticipate that this number might reach 2–2.5 billion, with a significant portion of it coming from connected automobiles in futuristic vehicular networks. As a result of advancements in both hardware and software, modern automobiles are more than just thermomechanical devices [1]. With all the capabilities they offer including GPS, wireless communication, entertainment, enhanced sensing, visual assistance, automatic alarm systems, and more there is a lot of data processing and networking required. The natural progression of technology would be to allow autonomous vehicles to communicate and work together, given that road travel is rarely done by one person. The potential benefits of an interconnected vehicle network are vast, and include things like entertainment, data exchange, route routing, traffic control, and much more. One method for accomplishing this is by using a Vehicular Ad-hoc Network (VANET). Virtual Ad hoc Networks (VANETs) are a subset of Mobile Ad hoc Networks (MANETs) that use roadside infrastructure known as Road Side Units (RSUs) to support constantly moving network nodes. These RSUs have the potential to support a wide range of features, from urgent collision notifications to connecting geographically separate VANETs [2, 3]. Two types of communication are available to vehicles in a VANET: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Experts think that VANET technology can solve many problems, such as motorway management, driver assistance, and accident prevention and safety [4]. To illustrate the point, when an accident occurs, the vehicles can communicate with other vehicles that are further away and may be utilizing the same route. Concerns about road safety are also on the rise. Worldwide, over 1.25 million people lost their lives in traffic accidents in 2015, according to statistics compiled by the Global Health Observatory (GHO) [5]. One promising use of VANETs is their ability to improve traffic management in urban areas, adding to its reputation as a reliable method for improving road safety. The Internet of Vehicles (IoV) is a proposed new paradigm for vehicular networks that could emerge in the future, especially in light of the widespread use of the Internet of Things (IoT) in VANETs. Although there are many benefits to VANET and the Internet of Things (IoT), the increasing number of V2V and V2I communication links does come with certain drawbacks in terms of network security [6, 7]. To that end, a number of studies tackling vulnerabilities in vehicle networks have been suggested for publication [8]. In 2010, there were one billion automobiles on the road. By 2050, experts anticipate that this number might reach 2–2.5 billion, with a significant portion of it coming from connected automobiles in futuristic vehicular networks. As a result of advancements in both hardware and software, modern automobiles are more than just thermomechanical devices [1]. With all the capabilities they offer including GPS, wireless communication, entertainment, enhanced sensing, visual assistance, automatic alarm systems, and more there is a lot of data processing and networking required. The natural progression of technology would be to allow autonomous vehicles to communicate and work together, given that road travel is rarely done by one person. The potential benefits of an interconnected vehicle network are vast, and include things like entertainment, data exchange, route routing, traffic control, and much more. One method for accomplishing this is by using a Vehicular Ad-hoc Network (VANET). Virtual Ad hoc Networks (VANETs) are a subset of Mobile Ad hoc Networks

(MANETs) that use roadside infrastructure, or Road Side Units (RSUs), to support constantly moving network nodes. These networks have a lot of potential uses, from connecting geographically separate VANETs to providing real-time collision alerts [2, 3]. Two types of communication are available to vehicles in a VANET: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Many problems, such as motorway management, driver assistance, and crash prevention and safety [4], are believed to be solvable with the use of VANET technology, according to researchers. To illustrate the point, when an accident occurs, the vehicles can communicate with other vehicles that are further away and may be utilising the same route. Concerns about road safety are also on the rise. Worldwide, over 1.25 million people lost their lives in traffic accidents in 2015, according to statistics compiled by the Global Health Observatory (GHO) [5]. VANETs, which are already being considered as a viable option for improving road safety, may also help with traffic management in densely populated areas. The Internet of Vehicles (IoV) is a proposed new paradigm for vehicular networks that could emerge in the future, especially in light of the widespread use of the Internet of Things (IoT) in VANETs. Although there are many benefits to VANET and the Internet of Things (IoT), the increasing number of V2V and V2I communication links does come with certain drawbacks in terms of network security [6, 7]. To that end, a number of studies tackling vulnerabilities in vehicle networks have been suggested for publication [8].

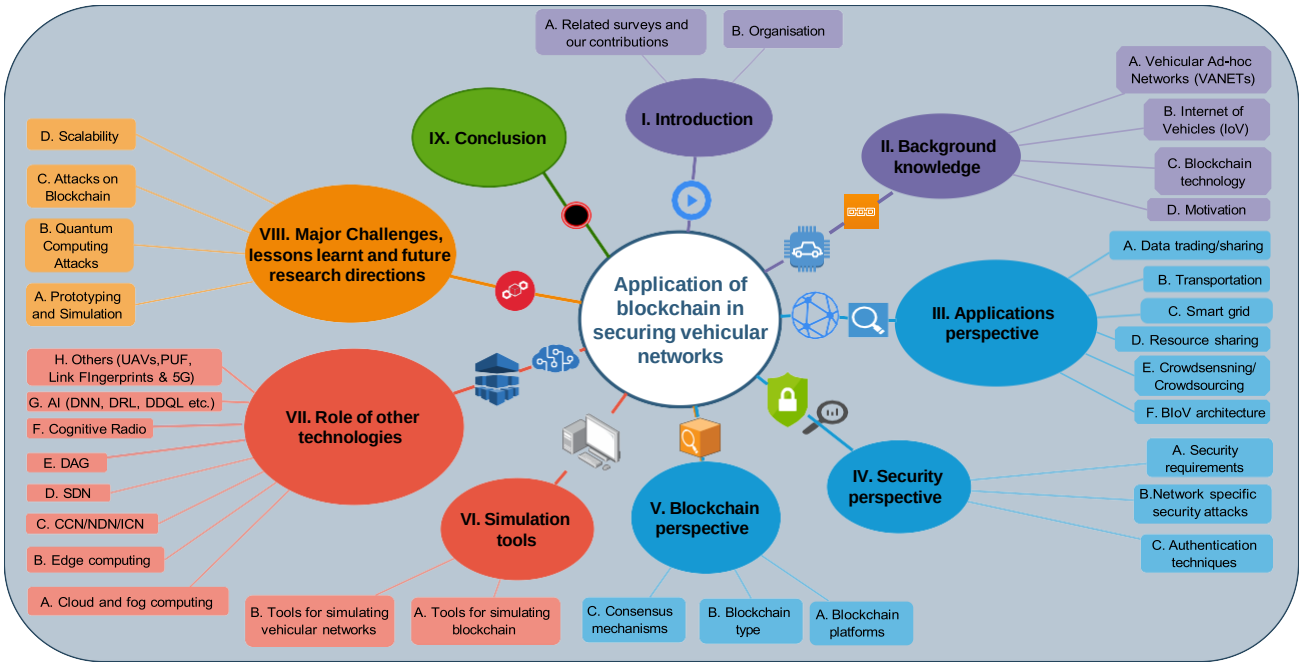

Fig. 1: Overview of this survey.

A. Related Surveys

We begin by comparing and contrasting the current survey with previous research on blockchain in vehicle networks. A brief overview of distributed ledger technologies' potential uses in improving transport by road was provided by Baldini et al. [9]. An additional study by the same authors in [10] examined blockchain's potential uses in the energy industry; electric vehicles were listed as one of those uses. Among the many facets of smart cities covered in Xie et al.'s comprehensive review of blockchain applications in smart cities [11], smart transit stands out. A recent proposal for a thorough evaluation of blockchain applications in the IoV network was made by Mollah et al. [12]. A survey of privacy management strategies for social IoV networks built on the blockchain was provided by the authors in [13]. While some of these studies do touch on the inherent security characteristics of blockchain-based frameworks, the majority of them are more concerned with the frameworks and application areas. Nevertheless, it would be highly appropriate for a study to be conducted at this time that examines security from a more thorough requirement-oriented perspective and delves into the specific ways in which blockchain fulfils those needs. To make this study self-contained for a reader, we have included several views, such as applications and an overview of the ways blockchain platforms have been employed. To sum up, this paper's goal is to provide readers with an overview of the blockchain techniques that have been created to address the security difficulties and requirements in vehicular networks. As mentioned earlier, Table I provides a collection of the most important survey and review studies conducted on blockchain applications in automotive networks in the past several years.

TABLE I: Related surveys on blockchain applications in vehicular networks

Year	Author	Contributions
2019	Xie et al. [11]	Surveys the application of blockchain in smart city scenarios

2019	Butt et al., [13]	Presents a review of blockchain based solutions for managing privacy in social IoV
2020	Baldini et al. [9]	Reviews the use of distributed ledger in road transport evolution
2020	Boa et al. [10]	Surveys the application of blockchain in the energy sector
2020	Mollah et al. [12]	Surveys usage of blockchain in IoV and Intelligent transportation systems (ITS)
2021	This Survey	Surveys the use of blockchain with a focus on security and privacy in VANETs

B. Motivation

Various services, including energy exchange, traffic management, accident avoidance, and an enhanced driving experience, are made possible when vehicles in a network share and access data with one another, with people, with sensors, with infrastructure, or with anything else (V2X). Blockchain technology has two features that make it ideal for usage in vehicle networks. One is the blockchain's internal structure; the technology is built to offer data integrity and security services independently of any one third party's reliability. The functionality of smart contracts is another component. These contracts offer a way to accomplish complicated tasks and enable intelligent interaction among a large number of nodes or vehicles.

A crucial aspect of the IoV is data sharing; constantly, the network generates and distributes massive amounts of data. That data is accessible to vehicles so they may make judgements or upload it to the cloud. Data security issues are inseparable from data. In what follows, this paper will go into detail on the topic of security. The advent of smart contracts has allowed blockchain technology to do much more than just facilitate distributed ledger operations. They can help with electric vehicle energy sharing through smart grid applications (blockchain technology) [14, 15], data trading (sharing computing resources) for Internet of Vehicles (IoV) applications [16–19], and job scheduling (20). For security reasons, they can be employed when only a specific number of nodes require transaction authorisation [16], [21]. The inherent dynamic topology of a vehicular network, in which vehicles join and exit regularly, makes authentication a crucial component of such a network. For VANET authentication, there are a number of useful frameworks provided by studies [21]–[24]. Blockchain technology can also be applied by the IoV in traffic control systems. According to the model provided by Cheng et al. [25], data access control can be implemented using attribute-based blockchains. In this model, only cars that meet specific criteria, such as road and travel direction, are granted access to certain data. To alleviate traffic congestion and offer more controllable coordination between vehicles, platooning is a navigational approach in which many vehicles form groups and drive in those groupings [26].

Each piece of research was evaluated in this poll according to the issue it sought to resolve. Some major areas of focus for the research community's ongoing efforts were identified from that examination. Research in this area going forward will primarily focus on one or more of these priority areas, according to this pattern. Table III shows the main areas of research, along with a few publications that address the problem and offer a solution in those areas.

The main contributions of this work are as follows:

i. The study analyses recent research in the area of blockchain-based vehicular networks from the application perspective, where the studies are classified based on the application area considered.
ii. The study also analyses the research from a security per- spective wherein studies are classified based on security requirements met, security attacks protected against, au- thentication techniques used, and security proofs showed.
iii. Recent advances are also examined from a blockchain perspective, categorised by blockchain platforms and con- sensus.
iv. The study discusses various simulation tools which have been used in blockchain-based vehicular network studies.
v. We also provide some insight on the role of other state-of-the-art technologies including, but not limited to, cloud computing, fog computing, edge computing, Soft- ware Defined Networking (SDN), Named Data Network- ing (NDN), Artificial Intelligence, 5G, etc. in securing blockchain-based vehicular networks.
vi. Based on the survey we present some major challenges and probable future research directions in this field.

C. Organisation

The rest of the paper is organised as follows. In Section II, we present the background knowledge on VANETs, IoV networks, and blockchain technology. We discuss the blockchain- based security frameworks for vehicular networks from an applications perspective in Section III. Section IV discusses the categorisation of the different blockchain-based works from the security perspective. These works are further categorised from the blockchain perspective in section V. A compilation of different simulation tools used is presented in Section VI. We discuss the role of other state-of-the-art technologies in securing blockchain-based vehicular frameworks in Section VII. Section VII-I describes existing challenges/open issues in using blockchain to secure vehicular networks and presents some future research directions. Finally, we conclude the paper in Section IX. The organisational overview of this survey is also shown in Fig. 1.

II. BACKGROUND KNOWLEDGE

This section gives a brief background on VANETs, Internet of Vehicles, and blockchain technology.

TABLE II: Major abbreviations used in the survey.

Notation	Meaning

3GPP	3rd Generation Partnership Project
BFT	Byzantine Fault Tolerance
BIoV	Blockchain-based Internet of Vehicles
CA	Certificate Authority
CCN	Content Centric Networking
DAG	Directed Acrylic Graph
DSRC	Dedicated Short-Range Communications
GPR	Gaussian Process Regression
IoEV	Internet of Electric Vehicles
ITS	Intelligent Transportation Systems
PBFT	Practical Byzantine Fault Tolerance
PKI	Public Key Infrastructure
PoW	Proof of Work
SDN	Software Defined Networking
SoC	State of Charge (of EVs)
TM	Trace Managers
V2CH	Vehicle to Cluster Head
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VANET	Vehicular Ad-hoc Networks
VCC	Vehicular Cloud Computing
VEC	Vehicular Edge Computing
VFS	Vehicular Fog Services
WAVE	Wireless Access in Vehicular Environment
ZKP	Zero Knowledge Proof

A. Vehicular Ad-Hoc Networks

The idea behind a vehicular network is to take wireless technology that is used to network computers and adapt it to vehicles. The technical term for vehicular networks is Vehicular Ad-Hoc Networks (VANETs). Ad-hoc networks do not have a defined infrastructure, thus the network topology must be decided by the nodes in the network through cooperative mechanisms [27]. In other words, there is no central authority and the nodes themselves behave as routers and are responsible for propagating information in the network.

B. Internet of Vehicles

The Internet of Vehicles (IoV) is an expansion of VANET that allows network-enabled vehicles to establish Intelligent Transportation Systems (ITS) based on an IP-connected infrastructure by connecting to the internet or cloud services. Data communication is provided by VANETs, and the Internet of Things encompasses the processing of that data on an extremely large scale to offer vital services. An ideal Internet of cars (IoV) network would improve transportation safety and efficiency on a regional or national level by integrating cars, the road environment, and people. The utilisation of cloud computing, artificial intelligence, big data, and VANETs might all work together to accomplish this. The initial proposal for an IoV network's abstract architecture was made by Yang et al. [28]. You may classify the Internet of Vehicles (IoV) uses into two main groups: safety and business. Essential safety services include, but are not limited to, information on speed limits, emergency braking procedures, and collision avoidance applications. Since these applications are frequently time-sensitive, they necessitate a network with minimal transmission latency. Streaming video, instant messaging, weather and traffic updates, and any other service that improves the driving experience are all examples of commercial uses. The key difference is that commercial applications must not interfere with crucial safety applications, which are hard real-time applications.

The following are a few instances of IoV applications: Lee et al.'s MobEyes is a smart system that uses wireless-enabled vehicles to do event sensing; it does this by constantly generating data summaries from mobile nodes that extract features from their environment and share them with neighbouring nodes. Other proposals include a video-streaming technology that helps drivers see better and supports overtaking in difficult situations [29], an on-board diagnostic system based on GPS and 3G [30], and a video-streaming technology that enhances the visibility of the driver [31].

C. Blockchain Technology

Blockchain is a new technology that is rapidly gaining traction in fields such as finance [32], UAVs [33]–[36], IoT [37]–[40], smart cities [41], [42], smart grids [40], supply
chain management [43], VANETs [44], [45], and many others. It was originally proposed by S. Nakamoto in his whitepa- per [46] on Bitcoin. Blockchain is a type of data structure holding records of digital transactions, formally known as a

distributed ledger. Identical copies of the database exist across multiple different computing machines, called nodes in blockchain terminology, connected in a peer-to-peer network. Transactions being the fundamental units of blockchain, a definite number of transactions are stored in a block, and blocks are continuously appended in sequence to form a chain. It emphasizes the importance of decentralization where the majority of entities participating in the blockchain are assumed to be genuine and take the decision collectively with the help of the process known as a consensus mechanism.

Some of the core ideas on which blockchain is built are outlined below:

1) **Digital Signatures:** Public key cryptography is one of the core concepts of blockchain technology. Each agent is assigned a private key and a public key. Anything encrypted using the private key can only be decrypted using the public key, and vice versa. The public key serves as an address for each node, and each digital asset is associated with its owner's public key [47]. The piece of data that needs to be transferred is signed using the private key. This can be used to authenticate information; if a piece of data is signed cryptographically using a private key, then the only thing that can decrypt it is the same user's public key. Blockchains commonly use elliptic curve digital signature algorithms [48].

2) **Hashing:** Hashing algorithms are arguably the backbone of blockchain technology. The hash function is a type ofcryptographic algorithm which takes an input of variable size and returns an output of fixed length, called a hash. SHA family (SHA-1 and SHA-2) are popular hashing algorithms. There are two conditions a good hash algorithm must obey:
   a) It must be non-invertible; i.e., it should not be possible to retrieve the input given the output.
   b) The chances of two different inputs giving the same output hash must be very small.

   The reason this is useful for security is that a small input change will completely change the hash value, and that makes tampering evident.

3) **Blocks:** Blocks are the constituent elements of blockchains, and they typically consist of a block body and block header. The block body contains transactions and a transaction counter. The block header contains different pieces of information, such as the Merkle tree root, the timestamp, block version, and the previous block's header's hash. These stored hash values provide immutability to the transactions. If a transaction in any block is changed, then it would change the block header, and the hash value will be different from the hash value stored in the successive block, and thus tampering is evident.
   Each block is validated through a consensus algorithm and added using a process that is necessarily expensive or difficult to perform but easy to validate the immutability comes from the belief that malicious entities will not be able to meet the conditions for this hard-to-perform- but-easy-to-validate mining process, and therefore, cannot simply change the hash values of the blocks to cover up any tampering. The mining process needs to be performed for all subsequent blocks if a certain block is modified after creation and added to the chain, which is practically impossible. The blockchain is public, so participating nodes will be able to view but not modify the contents. A string of blocks appended in sequence form the blockchain.

4) **Consensus Algorithm:** Nodes in the peer-to-peer net- work take the responsibility of verifying the transactions and adding them to the blockchain. This process is known as mining and is one of the most important elements of the blockchain network because it is responsible for its decentralized nature. The fundamental idea behind consensus is that nodes must undergo a process that is hard to perform yet easy to validate discouraging malicious entities from acquiring the necessary conditions required to validate invalid transactions.

Putting it all together - suppose Alice desires to send a digital asset to Bob. Then Alice would have to sign the asset using her private key and broadcast a transaction request with the item and Bob's address. A miner, upon receiving the trans- action, would bundle that transaction along with several other transactions in the block body. The miner would also create the block header and subsequently, broadcast the header to other blockchain nodes. These blockchain nodes then perform a pre- decided consensus algorithm. If the block is approved, then it is added as the latest block and all the nodes update the ledger to reflect the change. The fundamental role of the miner in all this is to collect, verify, and package transactions into a block, though the specifics of how they would do are dependent on the type of blockchain and consensus mechanisms agreed upon.

There are two major categories of blockchains - permissioned and permissionless:

i. **Permissionless blockchains** are public and open access; anyone is capable of joining the blockchain and take part in the consensus mechanism. Interested users having an internet connection can join become a part of the network, and participants' identities are hidden which is a security concern.
ii. **Permissioned blockchains** place restrictions on the member nodes in terms of read access or participation in the consensus process, or both. This often helps in computation and network communication overhead, which is a major cause for delay in permissionless networks.

Smart contracts are pieces of computer code that can run on a blockchain to facilitate and enforce the terms of an agreement. First proposed by Nick Szabo [49] in 1997, the concept behind a smart contract is to execute the functions/ tasks of an agreement automatically when the specified conditions of a contract/ agreement are satisfied.

III. Categorisation based on Application Scenarios

In this section, we categorise the different blockchain-based security works surveyed from the application perspective, i.e., based on the application area considered.

A. Data Trading and Sharing

The concept of data trading/ sharing is to treat data as a commodity, with vehicles being able to 'purchase' and 'sell' data from the network. From a very broad point of view, this is the fundamental concept behind all other blockchain-based IoV frameworks; whether it is computational information for resource sharing or battery level information for smart grid applications. Data must be shared for vehicles to coordinate with each other. However, we address it as a separate thrust area to delineate the research that focuses on optimizing data trading/sharing frameworks from research works that take data sharing for granted and focus on other aspects of the network. We classify the data in vehicular networks into four broad categories:

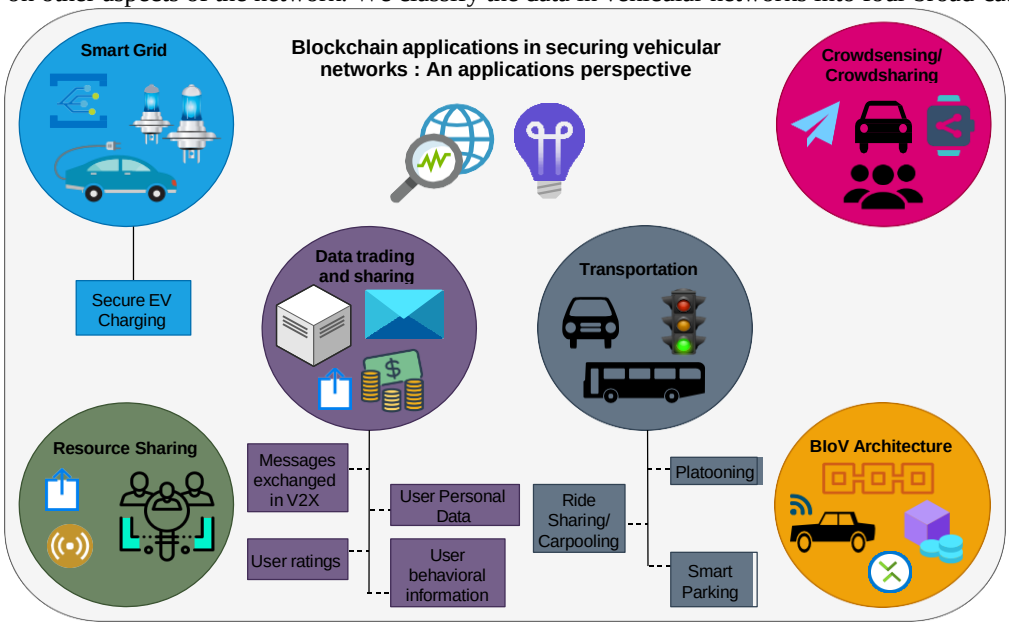

Fig. 3: Overview of the applications perspective section.

- **Messages exchanged:** Vehicles communicate with each other by exchanging messages such as sensor data and traffic-related information.
- **User personal data:** User personal data refers to the user identity, name, e-wallet details, images, and videos - anything that can be used to identify a vehicle. It can also include important parameters of Electric Vehicles (EVs) such as State of Charge (SoC) of battery, battery capacity, and travel schedules, all of which decide the EV type.
- **User behavioural information:** This includes information about the trading preferences of the individuals when participating in a trading network (data trading, resource trading, and energy trading among others), individual's likes and dislikes - any information that can be used to predict how a user will behave.
- **User ratings:** Various frameworks assign trust ratings to the vehicles based on their previous history which can be used by other nodes to evaluate the user's trustworthiness. These ratings need to be secured against false ratings uploaded by malicious vehicles. Such data is shared when a vehicle leaves one vehicular network and joins another network.

B. Transportation

This application area deals primarily with vehicle movement and management. Coordinating vehicles in real-time allows for more effective movement - one might think of how traffic is managed and coordinated even now with traffic lights and signs, and consider how that concept could be extended digitally with extremely specific travel information of vehicles [84]. It opens up possibilities for collaboration that are either too centralized or too computation-heavy for anything other than a distributed system. Some of these possibilities are outlined below: **Ride sharing/Carpooling:** Reducing the number of vehicles on the road is a necessary step towards better environmental conditions and road safety. Two aspects of blockchain, namely, built-in cryptocurrency and smart contracts make it suitable for this task.

- **Platooning:** The concept of cars forming a group and navigating as a group has a couple of advantages. Firstly, it reduces traffic congestion since coordinating a few groups is easier than coordinating several vehicles, and secondly, it reduces the chances of accidents. Blockchain is used in [26] as a transaction framework that achieves this.
- **Smart parking:** Many parking lots are used inefficiently, with a fairly simple parking model involving a flat and hourly rate. These rates are heavily dependent on local demand. That demand could be spread over a larger area, which reduces the number of underutilized parking areas. Conceptually, it is just more efficient resource allocation. Many studies have focused on developing intelligent parking mechanisms [85], [86], for example Zhang et al. proposed a blockchain-based smart parking framework that links customers to available parking lots [58].

C. Smart Grid

This application area deals with EVs [87]. The key feature of smart grids that sets them apart from traditional grids is the applicability of big data analytics. Consumers may also sell energy to the grid, which means extra electricity need not be generated needlessly if demand and supply can be met with the existing resources. Smart grids need to be fault- tolerant with the ability to quickly handle any possible faults. Again, distributed systems come to their rescue. Scalability is a major challenge in this sort of application; since the infrastructure and power distribution complexity scale very disproportionately to the geographic area. Newer blockchain architectures are being proposed to provide scalability [88]. Secure EV charging is the most common application for smart grids. With the advent of electric vehicles, coordinating charging schedules to balance out supply and demand over time in a way that maintains security is the primary focus of these kinds of research works. Blockchain also provides a payment platform for rewarding vehicles that share their energy to the grid, for example, if someone realizes they have excess charge left over after making a trip.

D. Resource Sharing

Cloud computing is the key driving technology of this research area. The paradigm is the same - exchange of compu- tational resources for payment, except with the complexities of vehicular networks and edge computing. Blockchain can be used to construct a distributed open market type of system, rather than rely on computation provided by a single third party. It is assumed that vehicles, unlike typical embedded systems, may be equipped with relatively higher processing capabilities, which allows them to be computational resource providers; they may also behave as consumers, purchasing resources from the RSUs.

E. Crowdsensing/Crowdsharing

Similar to data sharing, crowdsensing applications focus more on optimizing the system for aggregated data collectionrather than point-to-point data trading. Crowdsensing allows service providers to gather data in real-time, and blockchain allows people to contribute (maybe for payment) securely. This is useful especially in the map and location-based services, for example, notifying vehicles of a crash up ahead or road clo- sure. Some form of crowdsourcing is already being practised currently, but it lacks a strong incentive system which limits its usefulness.

F. BIoV Architecture

Every application area analyzed so far has been some inte- gration of blockchain and IoV technologies. But this research area deserves to be mentioned separately since it is slightly different in terms of research focus. Much research work has gone into optimizing the core features of blockchain to make it more adaptable to VANETs. For example, [24] proposed a custom consensus algorithm for vehicular networks, and [80] introduced an energy-efficient clustering protocol specifically for blockchain-enabled vehicular networks. This research di- rection is conceptually distinct from the others in that the primary problem being addressed is not that of providing a service through blockchain use, but that of overcoming existing limitations in blockchain and/or VANETs by changing some of their core features.

Summary: In this section, several blockchain-based IoV frameworks were categorised for different application areas. Scenarios like data trading and sharing, transportation, smart grid, resource sharing, crowdsensing/crowdsourcing and BIoV architecture are discussed in detail, explaining their utility, and each of the frameworks is categorised into one of these groups.

TABLE III: Research problems and proposed solutions of blockchain-based security works for some common application areas.

Application	**Ref.**	**Target issue**	**Solution proposed** *and/or blockchain usage*	**Supporting techniques** *and/or smart contract (SC) usage*
Data trading/ sharing	[50], [51]	Securing communication	• Novel cryptographic primitive: blockchain-based proxy re-encryption. • Combines proxy re-encryption, searchable encrytion, and blockchain.	SC performs ciphertext matching for data searches
	[52]	Reliability and efficiency of data sharing	• Federated learning to fulfill data sharing requests correctly. • Local DAG for storing shared update models, global permissioned blockchain for managing data sharing requests.	Federated learning, DAGs
	[17]	Transaction delays and cold start problems	• Vehicles buy and sell data. To allow new users to participate even with empty accounts, this is formulated as a debt-credit system.	Pricing strategy modelled as a two-stage Stackelberg game
	[53]	NDN data sharing	• Layered model, with NDN routers interfacing with blockchain.	Named Data Networking (NDN)
	[54]	Data sharing in VSNs	• Directed Acrylic Graph (DAG) based blockchain stores data within relevant topic groups in VSNs.	Directed Acrylic Graphs
	[26]	Traffic management, Autonomous driving	• Vehicle platooning based on path matching. • Platoon heads, chosen rotationally by reputation, pay attention to the road while platoon members can relax.	Platoon heads paid in cryptocurrency by members via SCs
	[55]	Ride sharing	• Rider makes a time-locked deposit and provides a set of obfuscated locations; driver also makes a deposit until proof of pick-up.	SCs prevent fraud
	[56]	Lane changing in autonomous vehicles	• Lane changing modelled as a Deep Reinforcement Learning problem. • Secure collective learning framework using blockchain.	Deep Reinforcement Learning (DRL)

Transportation	[16], [57]	Correcting errors in GPS positioning	• LIDAR aided vehicles train a DNN and share positioning error information with other vehicles through blockchain.	SCs ensure accuracy of shared models
	[58]	Smart parking	• Parking owners rent out space using blockchain.	SCs realise fairness; matching, advance payment
	[59]	Carpooling	• Fog computing to match user carpooling requests with potential drivers. • Blockchain stores records, with conditional privacy.	Bloom filters for location anonymity
	[25]	Road congestion, inefficiency	• Blockchain holds travel related information. • Degree of availability of information on the blockchain is based on attributes of a vehicle, like direction of travel.	CP-ABE encryption used instead of ordinary PKCs.
Authentication	[60]	Cross datacenter authentication in fog computing scenario	• Custom privacy preserving authentication scheme for fog computing; easy re-authentication across different locations. • Consortium blockchain stores authentication records of vehicles.	-
	[61]	Conditional privacy - preserving authentication	• Blockchain used to store certificates as transactions. • Messages contain transaction ID that authenticated sender vehicle.	SCs are used to broadcast certificates to the blockchain
	[62]	Performance bottlenecks	• Edge computing proxy vehicles that authenticate vehicle groups.	Proxy authentication
	[63]	Vehicle authentication for accident detection	• Custom certificate-based authentication scheme. • Blockchain holds transactions for accident related information.	Dynamic clustering
	[64]	Lightweight CA for location based services	• Threshold proxy scheme is employed by CAs that play role of distributed nodes inside a consortium type blockchain.	Threshold proxy signature
	[65]	Batch Authentication + Key Management	• Certificateless auth; TA and OBU establish session keys with operations performed explicitly at the cloud side. • Group key generation for efficient and secure V2V communication.	Group key
Smart grid	[14], [66] [67], [68]	Coordinating charging-discharging schedules of vehicles	• Aggregators formulate a schedule based on requests sent as blockchain transactions by EVs. • The schedule is formulated as an optimization problem.	SCs set prices, maximise utility
	[69]	Charging services with focus on privacy	• Blockchain with fog computing to reduce latency. • Selective storage of only sensitive data in the blockchain.	Fog Computing
	[70]	Anonymously rewarding vehicles for selling energy	• Exchange of energy happens for appropriate (secure) payment of blockchain cryptocurrency.	SCs decide remuneration
	[15]	Complete energy trading framework	• Discharging EVs compensated by charging EVs with cryptocurrency. • Incentive compatible Demand-Response paradigm is used.	SCs maximise social welfare, in terms of revenue generated.
Resource sharing	[71]	Edge-based data processing framework in VANETs	• Tasks allocated to containers on edge nodes, based on time and resources needed. Formulated as multi-objective optimization problem. • Containers can be migrated to other edge nodes using blockchain.	Containerization
	[19], [72] [73]	Complete architecture for resource sharing	• Spectrum and computation resources paid for with cryptocurrency.	SCs determine pricing by matching demand and supply
	[74]	Vehicular fog computing with parked vehicles	• Requester uses blockchain currency to pay vehicles for using their computation resources. • Problem formulated as two-stage Stackelberg game.	SCs mediate requesters and performers/providers
	[75]	IDaaS with Vehicular cloud computing	• Identity-as-a-Service model for vehicles and vehicular clouds. • Personally identifiable information encrypted and stored in blockchain.	Encryption with CP-ABE
Crowdsourcing / Crowdsensing	[76]	Vehicle cooperation for crowdsensing tasks	• Vehicle team selection and payment method based on blockchain. • Credit score determined by number of successful completions.	Reverse auction
	[77]	Real time map updates	• Blockchain based credit management system — a privacy preserving incentive mechanism.	optimization problem, reverse auction mechanism
	[78]	Location privacy in crowdsourcing tasks	• Area grid recursively partitioned using quad tree function. • Workers share location data over blockchain; recursive partitioning allows selection of privacy levels. Task requesters access blockchain.	—
BIoV architecture	[79]	Vehicular SDN	• Blockchain used to manage the network commands for control plane securely.	Q-learning to manage system state
	[80]	Large energy consumption in Blockchain enabled IoV	• Model that manages energy consumed for consensus by selectively representing some nodes by their associated cluster head.	Distributed Clustering
	[81]	Performance and security / trust services in VANETs	• Architecture for VANETs that combine SDN, blockchain, and fog computing technologies. • Blockchain provides secure communication.	—
	[82]	Mining cluster selection	• Offloading vehicles and mining clusters are matched based on (1) transmission rate and (2) available cluster resources for mining	—
	[83]	Key management	• Traditional architecture: Different CAs maintain identity information for different regions; crossovers involve inter-CA communication. • Proposed architecture: CAs replaced with a blockchain network.	—

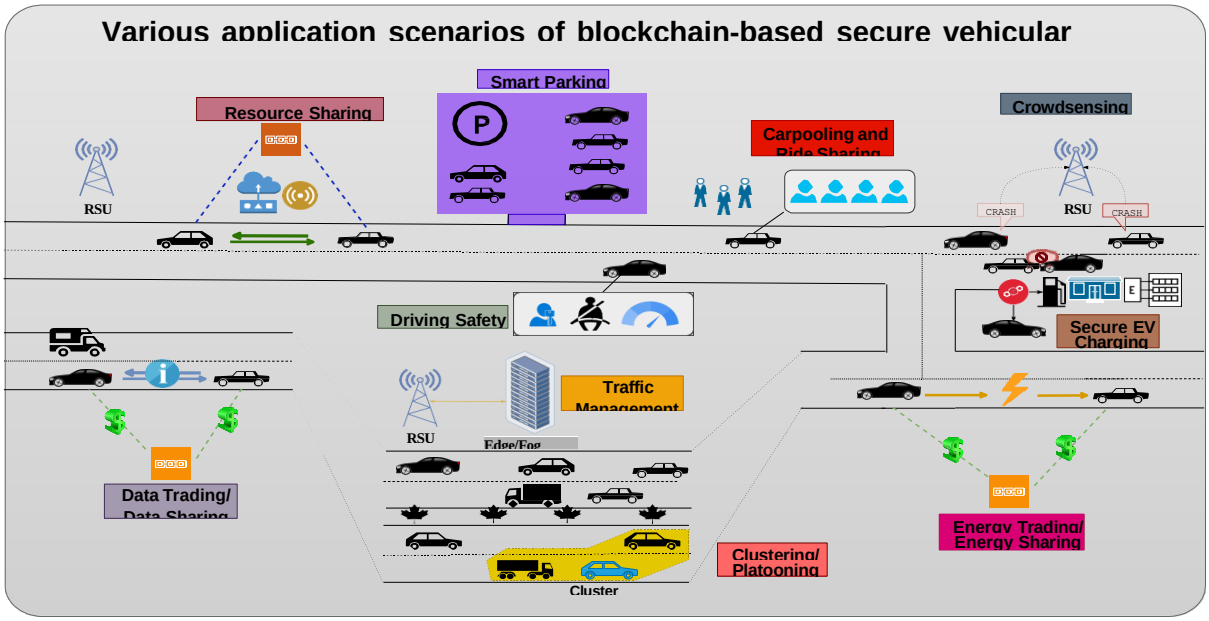

Fig. 4: Thematic view of the various application scenarios in which blockchain is used for ensuring security.

IV. Categorisation based on Security Features

The security perspective section categorises different blockchain-based security works based on the following cate- gory types.

i. Security requirements met
ii. Protection against network-specific security attacks
iii. Authentication techniques
iv. Security proof

The purpose and scope of each category and the definition of fields within them have been defined in the subsequent sections. This will give the readers a holistic view of the research done in vehicular network security using blockchain- based frameworks, and thus help in further research in this area.

A. Security Requirements

A security requirement is a condition which a network should meet to mitigate attacks and vulnerabilities in the network. There have been various studies that have defined different security requirements for vehicular networks [101]– [103]. Blockchain technology implicitly provides some of these security requirements due to its decentralized nature and tamper-proof storage mechanism. Thus, any blockchain- based security framework will meet the following security requirements by default.

1) **Decentralization:** Blockchain eliminates the involvement of any third party by enabling a P2P network where some of the blockchain nodes verify the transactions. This preserves the privacy of the vehicles by eliminating the need for sharing their details with a third party [17]. This property has several applications in vehicular networks such as decentralized communication [89], data sharing [90], and identity management [91] among others.
2) **Tamper resistance:** The data recorded in the blockchain is difficult to tamper with because it is organised in the form of special structures such as hash chain [93], and every block contains the hash of the previous block. This ensures irreversibility and immutability as tampering with the data in any block will change its hash value and will disconnect it from the blockchain. Also, blockchain's distributed nature ensures that the data has not been tampered with at any intermediary stages because of elimination of the third party, i.e., decentralization also leads to tamper resistance [92].
3) **Unforgeability:** It refers to the ability of a network to resist adversaries from forging data or a user's digital signature. The decentralized nature of the blockchain combined with its digitally signed transactions guarantee this and ensure that adversaries are not able to pose as other users [90]. In [93], Li et al. use a blockchain-based fair and anonymous ad dissemination scheme to ensure unforgeability using a popular authentication algorithm called Zero-Knowledge Proof.**Traceability (via cryptographic hash):** Each block in the blockchain contains the cryptographic hash of the previous block, thus ensuring traceability [92], [93]. Each node can trace and verify the correspondence of the data. This will help in tracing any malicious activity or message circulation thus avoiding confusion and accidents in the vehicular network.
4) **Public audit:** Blockchain helps in implementing public audits via its consensus mechanism. The block created by the miners must satisfy the criteria of the consensus mechanism used and should also be independently veri- fied by other nodes in the network. This feature has been used in [94] for authentication purposes in the vehicle to grid energy

trading, and in [17] for publicly auditing transnational data trading in the IoV environment.

Apart from the above security requirements, there are other security requirements that a blockchain-based scheme must satisfy to increase its robustness. In this study, the following is the list of security requirements considered (excluding the ones implicitly provided by blockchain):

1) **Non-repudiation:** It ensures senders cannot deny the transmission of a message and also ensures easy iden- tification of the vehicle nodes in case of accidents. Mit- igation of repudiation attacks comes under this security requirement. It can be met by ensuring the following.
   a) All transmitted messages are signed by a transmitting node via its anonymous public key to ensure that the node cannot claim to be some other node in the network (which can result in a masquerade attack).
   b) The node cannot claim that the message was replayed since the message is timestamped. It is crucial for investigation agencies for finding the chain of events and message details in case of a mishap.
   c) Vehicles cannot falsify their location information due to the implementation of secure positioning solutions.
2) **Privacy preservation:** Frameworks meeting this security requirement ensures that the private information of the participating nodes is not disclosed to the public or malicious parties. Also, the privacy of the drivers should be guaranteed against unauthorized observers [104]. It has mainly two important features:
   a) **Anonymity:** Specific personal details of the nodes such as name and vehicle type should not be disclosed. It prevents malicious parties from tracking the activities of a user by ensuring that for each incoming transac- tion, all possible senders are equiprobable, i.e., untrace- ablility [70] (not to be confused with traceability as a security requirement). Anonymity is generally achieved by using pseudonyms and cryptographic techniques. It leads to mitigation of tracking attacks [23].
   b) **Unlinkability:** It ensures that the attackers cannot link received messages sent from the same sender; or in other words, for any two outgoing transactions, it is impossible to prove that they were sent to the same person [70]. This is similar to forward security [62].

V. **Traceability (via conditional privacy):** By linking a vehicle's pseudonym to its true identity, a government MAJOR CHALLENGES, LESSONS LEARNT AND FUTURE RESEARCH DIRECTIONS

In this section, we discuss the major challenges faced in implementing blockchain-based applications for securing vehicular networks and the potential future research directions to address them.

A. Scalability

Throughput, or the number of transactions validated per second, is a quantitative measure of the scalability of the blockchain system. Bitcoin has a throughput of 7 transac- tions per second - for comparison, VISA has a transaction throughput of 2, 000 transactions per second [182]. Generally, lower throughputs can be improved at higher scales by suitable modifications to the algorithm itself, such as in [98]. Vehicular networks will generate a massive amount of data, and because of the latency-critical environment, the blockchain will have to scale up to a very high standard. Many of the existing standards and protocols were developed for cryptocurrency applications, which are not as time-sensitive. Performance can be increased by choosing the appropriate consensus algorithms and blockchain platforms. For instance, DPoS and DBFT provide a significant improvement in transaction throughput compared to PoS and PBFT respectively. There has been some research on specifically integrating IoV and blockchain consensus. In [114], the authors posit an enhanced DPoS consensus for blockchain-based IoV applications. Hu et al.
[24] propose an IoV-specific byzantine consensus algorithm for authentication. Consortium and private blockchains are also much more efficient than permissionless blockchains since the number of validating nodes is fewer. In this case, there must be a careful consideration of the trade-off between decentraliza- tion and throughput, since consortium and private blockchains are more centralized than permissionless blockchains. Another issue related to scalability is the seamless integration of multiple sensors and devices. As the IoV networks become larger, different sensors and platforms will be used. Ensuring they all work together seamlessly will be a challenge.

B. Privacy

When the vehicular nodes are used for edge computing, sensitive information like travelling route, card information, etc., are offloaded for various tasks [183]. To prevent unwanted parties from accessing such information, the information can be encrypted. However, cypher-text makes the analytics pro- cess time-consuming. A speed-up is required in the privacy- preserving blockchain framework for the querying process in edge computing.

There is a requirement to ensure user privacy due to the sensitive nature of the data while also allowing transparency to comply with the legal requirements like the General Data Protection Regulation (GDPR) [9]. Encryption and compli- mentary access control techniques are required in a distributed ledger to balance privacy and transparency.

C. Quantum Computing Attacks

Quantum computing is a field of research that will have wide applicability in the coming years. Blockchain relies heavily on the one-way property of its cryptographic hashing techniques. With the advent of quantum computing, these techniques may not be as secure as they are currently. Quantum computers offer a vastly different scale of computational power; a few quantum computers

may easily overcome the computing power of an entire network of ordinary blockchain nodes. In an attempt to attack the IoV network using quantum computers, the aim is to affect a part of the network rather than just a single node. This might lead to a loss of trust in the blockchain network. Quantum attacks is an active area of research, and with many other solutions being proposed however, these techniques must be incorporated to make commercially viable systems.

D. Prototyping and Simulation

Blockchain designed to be a decentralized system poses a natural challenge for prototyping and simulation. Several large-scale effects cannot be adequately modelled on a prototype. Existing research works present their findings in the form of small-scale model simulation details, many of which use the best technologies available, however, they do not accurately reflect several unforeseen challenges. For example, it is very difficult to accurately model the randomness that is inherent in vehicular network topologies, even using stochastic mechanisms. Therefore, the research community would be well aided by the development of better simulation tools and prototype tested frameworks [33].

Attacks on Blockchains

The unique nature of a blockchain system opens it up to several attacks that are not of concern in conventional central- ized systems - including, but not limited to 51% attacks, selfish mining, eclipse attacks, DNS attacks, and crypto-jacking [190]. Although blockchain-enabled vehicular edge computing provides benefits like decentralization and transparency, it is vulnerable to several attacks. In the event of a significant number of members of the network being compromised, the network can be hijacked and the transactions can be forged. The attack occurs due to the lightweight consensus protocols used in permissioned blockchain networks. Hence, a scalable and resilient consensus protocol is required for the deployment of different types of chains in the vehicular edge-computing network.

VI. CONCLUSION

In this survey, we thoroughly analyzed several blockchain-based security frameworks for vehicular networks and categorised them from three different perspectives, namely, application perspective, security perspective, and blockchain perspective. From the application perspective, we categorise the frameworks based on different application scenarios such as data trading/sharing, resource sharing, parking, traffic man- agement, etc. From the security perspective, we categorise the frameworks based on the security attacks they protect against, the network security requirements they meet, the authentication techniques they employ, and the security proofs they use. From the blockchain perspective, we classify the different frameworks based on the type of blockchain they use, the type of blockchain platform they employ, and the consensus algorithm used in their scheme. We also discussed various simulation tools/platforms which have been used for simulating and testing these blockchain-based frameworks. Furthermore, most of the blockchain-based security frameworks employ other emerging technologies to meet requirements such as low latency, low computation, data storage, etc. in their schemes along with blockchain. Hence it is important to analyze these frameworks and discuss the role of these other state-of-the-art technologies in securing these networks. Lastly, based on the survey, we list out the major challenges and future research directions in this domain. This survey will act as a guide to the researchers and professionals venturing into the research and development of blockchain-based security solutions for vehicular networks like IoV and VANETs.

REFERENCES

[1] P. K. Sahu, E. H.-K. Wu, J. Sahoo, and M. Gerla, "Bahg: Back- bone-assisted hop greedy routing for vanet's city environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 199–213, 09 2012.

[2] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 04 2016.

[3] M. A. Elsadig and Y. A. Fadlalla, "Vanets security issues and chal- lenges: A survey," *Indian Journal of Science and Technology*, vol. 9, no. 28, pp. 1–8, 07 2016.

[4] A. Mehra, M. Mandal, P. Narang, and V. Chamola, "Reviewnet: A fast and resource optimized network for enabling safe autonomous driving in hazy weather conditions," *IEEE Transactions on Intelligent Transportation Systems*, 08 2020.

[5] "Global Health Observatory (GHO) data," https://www.who.int/gho/ road$ $safety/mortality/en/, 2020, [Online; accessed 14-March-2020].

[6] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 02 2020.

[7] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Computer Communications*, vol. 155, pp. 1–8, 04 2020.

[8] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight authentication and attestation scheme for in-transit vehicles in iov scenario," *IEEE Transactions on Vehicular Technology*, 11 2020.

[9] G. Baldini, J. L. Hernandez-Ramos, G. Steri, R. Neisse, and I. N. Fovino, "A review on the application of distributed ledgers in the evolution of road transport," *IEEE Internet Computing*, 09 2020.

[10] J. Bao, D. He, M. Luo, and K.-K. R. Choo, "A survey of blockchain applications in the energy sector," *IEEE Systems Journal*, 07 2020.

[11] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 02 2019.

[12] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *arXiv preprint arXiv:2007.06022*, 10 2020.

[13] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79 694–79 713, 06 2019.

[14] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601– 4613, 09 2018.

[15] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang, "Blockchain and compu- tational intelligence inspired incentive-compatible demand response in internet of

electric vehicles," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 3, no. 3, pp. 205–216, 05 2019.
[16] Y. Song, Y. Fu, F. R. Yu, and L. Zhou, "Blockchain-enabled internet of vehicles with cooperative positioning: A deep neural network approach," *IEEE Internet of Things Journal*, 02 2020.
[17] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9098–9111, 07 2019.
[18] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, 07 2019.
[19] H. Chai, S. Leng, K. Zhang, and S. Mao, "Proof-of-reputation based- consortium blockchain for trust resource sharing in internet of vehi- cles," *IEEE Access*, vol. 7, pp. 175 744–175 757, 12 2019.
[20] J. Fan, R. Li, and S. Li, "Research on task scheduling strategy: Based on smart contract in vehicular cloud computing environment," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 08 2018, pp. 248–249.
[21] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE access*, vol. 7, pp. 45 061–45 072, 04 2019.
[22] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for vanets," *IEEE Transac- tions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2792–2801, 08 2019.
[23] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preserva- tion in vanets," *IEEE Access*, vol. 7, pp. 117 716–117 726, 08 2019.
[24] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles," *IEEE Access*, vol. 7, pp. 139 703–139 711, 09 2019.
[25] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.-N. Dai, Y. Wu, and W. Wang, "Sctsc: A semicentralized traffic signal control mode with attribute-based blockchain in iovs," *IEEE Transactions on Computa- tional Social Systems*, vol. 6, no. 6, pp. 1373–1385, 04 2019.
[26] C. Chen, T. Xiao, T. Qiu, N. Lv, and Q. Pei, "Smart-contract- based economical platooning in blockchain-enabled urban internet of vehicles," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4122–4133, 11 2019.
[27] M. M. Zanjireh and H. Larijani, "A survey on centralised and dis- tributed clustering routing algorithms for wsns," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 05 2015, pp. 1–6.
[28] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1–15, 11 2014.
[29] C. Olaverri-Monreal, P. Gomes, R. Fernandes, F. Vieira, and M. Fer- reira, "The see-through system: A vanet-enabled assistant for overtak- ing maneuvers," in *2010 IEEE Intelligent Vehicles Symposium*. IEEE, 06 2010, pp. 123–128.
[30] J. Lin, S. Chen, Y. Shih, and S.-H. Chen, "A study on remote on-line diagnostic system for vehicles by integrating the technology of obd, gps, and 3g," *World Academy of Science, Engineering and Technology*, vol. 56, pp. 435–441, 08 2009.
[31] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, "Mobeyes: smart mobs for urban monitoring with a vehicular sensor network," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 52–57, 11 2006.
[32] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Business Review*, vol. 1, no. 9, pp. 2–5, 03 2017.
[33] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Vehicular Commu- nications*, vol. 23, p. 100249, 06 2020.
[34] T. M. Ferna´ndez-Carame´s, O. Blanco-Novoa, M. Sua´rez-Albela, and P. Fraga-Lamas, "A uav and blockchain-based system for industry 4.0 inventory and traceability applications," in *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 4, no. 1, 2018, p. 26.
[35] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi- agent systems consisting of uavs," in *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*. IEEE, 10 2017, pp. 84–89.
[36] K. Lei, Q. Zhang, J. Lou, B. Bai, and K. Xu, "Securing icn-based uav ad hoc networks with blockchain," *IEEE Communications Magazine*, vol. 57, no. 6, pp. 26–32, 06 2019.
[37] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Confer- ence on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 04 2017, pp. 173–178.
[38] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 03 2018.
[39] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 08 2018.
[40] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 01 2019.
[41] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th inter- national conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE, 12 2016, pp. 1392–1393.
[42] J. Sun, J. Yan, and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innovation*, vol. 2, no. 1, pp. 1–9, 12 2016.
[43] Y. Tribis, A. El Bouchti, and H. Bouayad, "Supply chain management based on blockchain: A systematic mapping study," in *MATEC Web of Conferences*, vol. 200. EDP Sciences, 2018, p. 00020.
[44] B. Leiding, P. Memarmoshrefi, and D. 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*, 09 2016, pp. 137–140.
[45] Z. Lu, Q. Wang, G. Qu, and Z. 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, 08 2018, pp. 98–103.
[46] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.
[47] M. Pilkington, "Blockchain technology: principles and applications," in *Research handbook on digital transformations*. Edward Elgar Publishing, 09 2016.
[48] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digi- tal signature algorithm (ecdsa)," *International journal of information security*, vol. 1, no. 1, pp. 36–63, 08 2001.
[49] N. Szabo. (1997) The idea of smart contracts. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html
[50] B. Chen, D. He, N. Kumar, H. Wang, and K.-K. R. Choo, "A blockchain-based proxy re-encryption with equality test for vehicular communication systems," *IEEE Transactions on Network Science and Engineering*, 06 2020.
[51] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, "A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks," *IEEE Transactions on Vehicular Technology*, 12 2019.
[52] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of

vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 02 2020.
[53] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of blockchain in named data networking-based internet-of-vehicles," *IT Professional*, vol. 21, no. 4, pp. 41–47, 07 2019.
[54] W. Yang, X. Dai, J. Xiao, and H. Jin, "Ldv: A lightweight dag- based blockchain for vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5749–5759, 01 2020.
[55] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Transactions on Network Science and Engineering*, 12 2019.
[56] Y. Fu, C. Li, F. R. Yu, T. H. Luan, and Y. Zhang, "An autonomous lane changing system with knowledge accumulation and transfer assisted by vehicular blockchain," *IEEE Internet of Things Journal*, 05 2020.
[57] C. Li, Y. Fu, F. R. Yu, T. H. Luan, and Y. Zhang, "Vehicle position correction: A vehicular blockchain networks-based gps error sharing framework," *IEEE Transactions on Intelligent Transportation Systems*, 01 2020.
[58] C. Zhang, L. Zhu, C. Xu, C. Zhang, K. Sharif, H. Wu, and H. West- ermann, "Bsfp: Blockchain-enabled smart parking with fairness, re- liability and privacy protection," *IEEE Transactions on Vehicular Technology*, 04 2020.
[59] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4573–4584, 08 2018.
[60] Y. Yao, X. Chang, J. Misˇic´, V. B. Misˇic´, and L. Li, "Bla: Blockchain- assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3775– 3784, 01 2019.
[61] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "Bcppa: A blockchain-based conditional privacy-preserving authentication proto- col for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 06 2020.
[62] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data trace- ability in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4221–4232, 01 2020.
[63] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. H. Park, "Blockchain-enabled certificate-based authentication for vehicle acci- dent detection and notification in intelligent transportation systems," *IEEE Sensors Journal*, 07 2020.
[64] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Blockchain- based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks," *IEEE Internet of Things Journal*, 02 2020.
[65] H. Tan and I. Chung, "Secure authentication and key management with blockchain in vanets," *IEEE Access*, vol. 8, pp. 2482–2498, 12 2019.
[66] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Transactions on Smart Grid*, 12 2019.
[67] Y. Wang, Z. Su, and N. Zhang, "Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3620– 3631, 04 2019.
[68] Y. Li and B. Hu, "A consortium blockchain-enabled secure and privacy- preserving optimized charging and discharging trading scheme for electric vehicles," *IEEE Transactions on Industrial Informatics*, 04 2020.
[69] H. Li, D. Han, and M. Tang, "A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing," *IEEE Systems Journal*, 07 2020.
[70] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "Bbars: Blockchain- based anonymous rewarding scheme for v2g networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3676–3687, 01 2019.
[71] G. Singh, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K. R. Choo, "Blocked: Blockchain-based secure data processing framework in edge envisioned v2x environment," *IEEE Transactions on Vehicular Technology*, 02 2020.
[72] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain- based on-demand computing resource trading in iov-assisted smart city," *IEEE Transactions on Emerging Topics in Computing*, 02 2020.
[73] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach," *IEEE Transactions on Network Science and Engineering*, 06 2020.
[74] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 426–441, 02 2020.
[75] Y. Yao, X. Chang, J. Misˇic´, and V. B. Misˇic´, "Lightweight and privacy- preserving id-as-a-service provisioning in vehicular cloud computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2185– 2194, 12 2019.
[76] J. Wang, X. Feng, T. Xu, H. Ning, and T. Qiu, "Blockchain based model for nondeterministic crowdsensing strategy with vehicular team- cooperation," *IEEE Internet of Things Journal*, 06 2020.
[77] C. Lai, M. Zhang, J. Cao, and D. Zheng, "Spir: A secure and privacy- preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 416–428, 11 2019.
[78] J. Zhang, F. Yang, Z. Ma, Z. Wang, X. Liu, and J. Ma, "A decentral- ized location privacy-preserving spatial crowdsourcing for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 08 2020.
[79] L. Zhang, M. Luo, J. Li, M. H. Au, K.-K. R. Choo, T. Chen, and S. Tian, "Blockchain based secure data sharing system for internet of vehicles: A position paper," *Vehicular Communications*, vol. 16, pp. 85–93, 04 2019.
[80] V. Sharma, "An energy-efficient transaction model for the blockchain- enabled internet of vehicles (iov)," *IEEE Communications Letters*, vol. 23, no. 2, pp. 246–249, 11 2018.
[81] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 11 2019.
[82] F. Jameel, M. A. Javed, S. Zeadally, and R. Ja¨ntti, "Efficient mining cluster selection for blockchain-based cellular v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, 07 2020.
[83] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intel- ligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 08 2017.