应用综合调查
用于保护车载网络的区块链

Tejasvi Alladi IEEE *高级会员* Vinay Chamola IEEE *高级会员* Nishad Sahu
Vishnu Venkatesh、Adit Goyal 和 Mohsen Guizani， *IEEE 研究员*

摘要— 车载网络承诺诸如交通管理、路线调度、数据交换、娱乐等功能。任何大规模的技术集成都会带来提供安全性的挑战。区块链技术已成为许多研究的热门选择，以使车辆网络更加安全。它的特性满足了一些基本的安全要求，例如去中心化、透明、防篡改和公共审计。这项研究列出了过去几年在这个方向上的一些显着努力。我们从应用程序、安全性和区块链的角度分析了大约 75 个基于区块链的车载网络安全方案。应用视角侧重于使用基于区块链的安全车辆网络的各种应用，例如交通、停车、数据共享/交易，资源共享。安全视角侧重于安全要求和攻击。区块链视角侧重于区块链实施中使用的区块链平台、区块链类型和共识机制。我们还编译了用于模拟区块链和模拟车辆网络的流行模拟工具。此外，为了让读者对研究领域有更广阔的了解，我们讨论了各种最先进的新兴技术在基于区块链的车辆网络中的作用。最后，我们通过列出该领域的一些常见挑战和未来研究方向来总结调查。和区块链实施中使用的共识机制。我们还编译了用于模拟区块链和模拟车辆网络的流行模拟工具。此外，为了让读者对研究领域有更广阔的了解，我们讨论了各种最先进的新兴技术在基于区块链的车辆网络中的作用。最后，我们通过列出该领域的一些常见挑战和未来研究方向来总结调查。和区块链实施中使用的共识机制。我们还编译了用于模拟区块链和模拟车辆网络的流行模拟工具。此外，为了让读者对研究领域有更广阔的了解，我们讨论了各种最先进的新兴技术在基于区块链的车辆网络中的作用。最后，我们通过列出该领域的一些常见挑战和未来研究方向来总结调查。

索引词——物联网 (IoT)、区块链、车联网 (IoV)、安全、密码学、身份验证。

一、引言

吨 HE NUMBER 辆在道路上行驶的车辆达到 2010 年为 10 亿。专家预测，到 2050 年，这一数字可能达到 2 - 25 亿，其中很大一部分将形成包括联网车辆的未来车辆网络流量。现代车辆不再仅仅是热机械机器，而是复杂的硬件和软件的结合 [1]。它们具有 GPS 设施、无线通信设备、娱乐系统、先进的传感机制、视觉辅助设备、自动警报系统以及更多功能，因此涉及大量数据处理和连接。由于在道路上行驶很少是一项单独的努力，因此技术发展的下一个合乎逻辑的步骤是使各个车辆能够相互通信和协调。连接的车辆网络承诺诸如交通管理、路线调度、数据交换、娱乐等功能。车载自组织网络（VANET）是实现这一目标的一种方式。VANET 是一种移动 Ad-hoc 网络 (MANET)，设计用于由称为路侧单元 (RSU) 的路侧基础设施支持的不断运动的网络节点，理论上可用于在任何地方提供多种功能从紧急碰撞通知到互连地理上独立的 VANET [2]、[3]。VANET 中的车辆可以通过车辆到车辆 (V2V) 通信相互通信，并通过车辆到基础设施 (V2I) 通信与 RSU 通信。研究人员认为，借助 VANET 技术，我们可以克服许多问题，包括但不限于碰撞预防和安全 [4]、驾驶员辅助和高速公路管理。例如，在发生事故的情况下，车辆可以将信息广播给可能计划使用相同路线的远处车辆。道路安全也日益受到关注。据全球卫生观察站 (GHO) 数据显示，全球道路交通死亡人数约为 125 万 [5]。VANET 被认为是一种有效的道路安全解决方案，也有可能为城市场景中的高效交通管理做出贡献。此外，随着物联网在 VANET 中的采用，一种称为车联网 (IoV) 的新范式正在被讨论为未来的车辆网络。然而，在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也存在不利之处 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车辆网络中的安全问题[8]。2010 年，道路上行驶的车辆数量达到 10 亿辆。–到 2050 年将达到 25 亿，其中很大一部分将形成由联网车辆组成的未来车辆网络流量。现代车辆不再仅仅是热机械机器，而是

稿件于 2021 年 8 月 3 日收到；2021 年 12 月 24 日修订；2022 年 3 月 17 日接受。出版日期 2022 年 3 月 21 日；当前版本的日期为 2022 年 5 月 24 日。*(Tejasvi Alladi 和 Vinay Chamola 对这项工作做出了同等贡献。)(通讯作者：Vinay Chamola。)*

Tejasvi Alladi 在印度 Pilani, Pilani 333031 的 Birla Institute of Technology and Science 计算机科学和信息系统系工作（电子邮件：tejasvi.alladi@pilani.bits-pilani.ac.in）。

Vinay Chamola 和 Nishad Sahu 就职于 Birla Institute of Technology and Science, Pilani, Pilani 333031, India 电气和电子工程与 APPCAIR 系（电子邮件：vinay.chamola@pilani.bits-pilani.ac.in；h20160215@pilani.bits-pilani.ac.in；f20171154@pilani.bits-pilani.ac.in）。

Vishnu Venkatesh 在 WCB Robotics Pvt. 有限公司，印度海得拉巴（电子邮件：vishnu.c.venkatesh@gmail.com）。

Adit Goyal 在印度诺伊达 201304 的 Jaypee 信息技术学院计算机科学与 IT 系工作（电子邮件：aditgoyal@hotmail.com）。

Mohsen Guizani 就职于阿联酋阿布扎比穆罕默德·本·扎耶德人工智能大学 (MBZUAI) 机器学习系（电子邮件：mguizani@ieee.org）。

数字对象标识符 10.1109/COMST.2022.3160925

表一

车载网络中区块链 A 应用的相关调查_ _

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

是复杂的硬件和软件的结合[1]。它们具有 GPS 设施、无线通信设备、娱乐系统、先进的传感机制、视觉辅助设备、自动警报系统以及更多功能，因此涉及大量数据处理和连接。由于在道路上行驶很少是一项单独的努力，因此技术发展的下一个合乎逻辑的步骤是使各个车辆能够相互通信和协调。连接的车辆网络承诺诸如交通管理、路线调度、数据交换、娱乐等功能。车载自组织网络（VANET）是实现这一目标的一种方式。VANET 是一种移动 Ad-hoc 网络 (MANET)，专为网络节点而设计，这些网络节点在称为路侧单元 (RSU) 的路侧基础设施支持下不断运动，理论上可用于提供多种功能，从紧急碰撞通知到互连地理上独立的 VANET [2]、[3]。VANET 中的车辆可以通过车辆到车辆 (V2V) 通信相互通信，并通过车辆到基础设施 (V2I) 通信与 RSU 通信。研究人员认为，借助 VANET 技术，我们可以克服很多问题，包括但不限于碰撞预防和安全 [4]、驾驶员辅助和高速公路管理。例如，在发生事故的情况下，车辆可以将信息广播给可能计划使用相同路线的远处车辆。道路安全也日益受到关注。据全球卫生观察站 (GHO) 数据显示，全球道路交通死亡人数约为 125 万 [5]。VANET 被认为是一种有效的道路安全解决方案，也有可能为城市场景中的高效交通管理做出贡献。此外，随着物联网在 VANET 中的采用，一种称为车联网 (IoV) 的新范式正在被讨论为未来的车辆网络。然而，在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也存在不利之处 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。据全球卫生观察站 (GHO) 数据显示，全球道路交通死亡人数约为 125 万 [5]。VANET 被认为是一种有效的道路安全解决方案，也有可能为城市场景中的高效交通管理做出贡献。此外，随着物联网在 VANET 中的采用，一种称为车联网 (IoV) 的新范式正在被讨论为未来的车辆网络。然而，在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也存在不利之处 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。据全球卫生观察站 (GHO) 数据显示，全球道路交通死亡人数约为 125 万 [5]。VANET 被认为是一种有效的道路安全解决方案，也有可能为城市场景中的高效交通管理做出贡献。此外，随着物联网在 VANET 中的采用，一种称为车联网 (IoV) 的新范式正在被讨论为未来的车辆网络。然而，在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也存在不利之处 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。也有可能为城市场景中的有效交通管理做出贡献。此外，随着物联网在 VANET 中的采用，一种称为车联网 (IoV) 的新范式正在被讨论为未来的车辆网络。然而，在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也存在不利之处 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。也有可能为城市场景中的有效交通管理做出贡献。此外，随着物联网在 VANET 中的采用，一种称为车联网 (IoV) 的新范式正在被讨论为未来的车辆网络。然而，在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也存在不利之处 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也有一个缺点 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。在网络安全方面，作为 VANET 和 IoV 范式的一部分，越来越多的 V2V 和 V2I 通信链路也有一个缺点 [6]、[7]。在这方面，已经提出了几篇研究文章来解决车载网络中的安全问题[8]。

A. 相关调查

我们首先讨论现有的关于车载网络中区块链的调查，并将它们与目前的调查进行对比。巴尔迪尼*等人*。简要回顾了分布式账本技术在道路交通发展中的应用 [9]。[10] 中作者的另一项工作调查了区块链在能源领域的应用，其中

一个应用领域是电动汽车。*谢等人*的广泛调查。[11]关于区块链在智慧城市中的应用讨论了智慧城市的几个方面，智能交通是智慧城市考虑的主要领域之一。莫拉*等人*。[12] 最近提出了对 IoV 网络中区块链应用的综合调查。[13] 中的作者对社交车联网网络中基于区块链的隐私管理技术进行了回顾。其中许多调查更多地关注应用领域和框架，并提到了基于区块链的框架隐含的安全功能。然而，从更严格的面向需求的角度分析安全性的研究，讨论区块链如何精确地满足这些要求，将是及时的。提供了其他观点，例如应用程序和区块链平台如何使用的概述，以使本研究

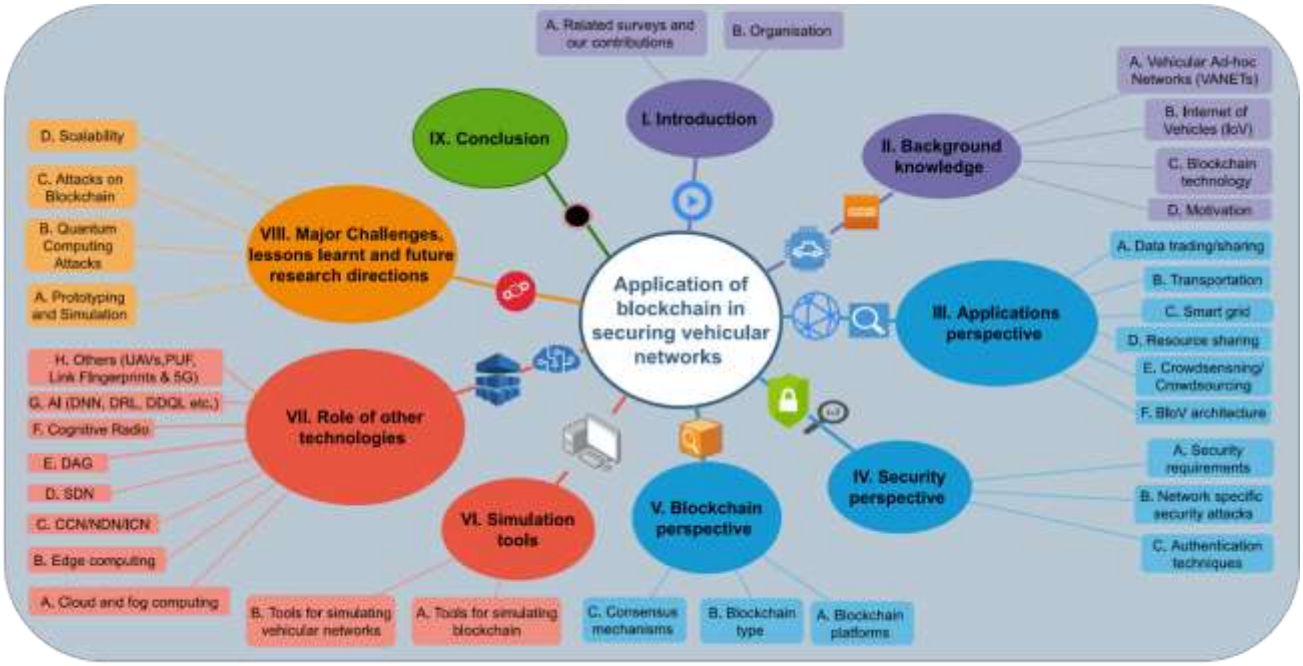


Fig. 1. Overview of this survey.

对读者来说是独立的。总之，本文旨在帮助读者了解车载网络中的安全挑战和要求，以及为缓解这些挑战而开发的区块链技术。表一列出了过去几年（如上所述）对车载网络中区块链应用所做的主要调查和审查工作清单。

B. 动机

网络中的车辆与其他车辆 (V2V)、人类 (V2H)、传感器 (V2S)、基础设施 (V2I) 或任何其他 (V2X) 共享和访问数据，以提供各种服务，例如交通管理、能源交换、避免事故，改善驾驶体验。区块链技术有两个方面使其对车载网络应用特别有用。一是区块链的结构方面——技术本身旨在以不依赖于第三方可信度的方式提供安全服务和数据完整性。另一方面是智能合约的功能，它提供了一种机制来执行复杂的任务，并允许大量节点或车辆进行智能交互。

数据共享是 IoV 的一个关键特性——在任何时候，都有大量数据在网络中生成和分发。车辆访问该数据以做出决策或将其上传以访问云服务。随着数据而来的是相关的安全问题。安全问题将在本文接下来的部分中深入讨论。智能合约已经将区块链的功能扩展到了简单的分布式账本机制之外。

当区块链用于智能电网应用 [14]、[15] 时，它们可以促进电动汽车之间的能源共享，优化 IoV 应用 [16]-[19] 的数据交易（或计算资源共享）的需求和供应，以及任务调度 [20]。当只需要授权一定数量的节点进行交易时，它们也可以用于安全目的 [16]、[21]。由于车辆频繁进出的底层动态拓扑，身份验证在车辆网络中起着重要作用。一些研究工作 [21]-[24] 为 VANET 中的身份验证提供了框架。流量控制机制也是车联网可以有效使用区块链的领域。程*等人*。给出使用基于属性的区块链的数据访问控制模型，其中只有符合某些属性（道路、行进方向等）的车辆才能访问某些信息 [25]。编队是一种模型，其中不同的车辆组成组进行导航和在这些组中行驶，以缓解交通拥堵，并在车辆之间提供更易于管理的协调[26]。

在这项调查中，每项研究工作都根据其解决的问题进行了分析。从该分析中得出了研究界目前正在研究的一些广泛的研究重点领域。基于这一趋势，该领域的未来研究将与这些推力领域中的一个或多个密切相关。表三说明了主要研究领域，其中一些工作包含该研究方向所解决的问题和建议的解决方案。

这项工作的主要贡献如下：

i. 该研究从应用角度分析了基于区块链的车辆网络领域的最新研究，其中研究根据所考虑的应用领域进行分类。
ii. 该研究还从安全角度分析了研究，其中研究根据满足的安全要求、保护的安全攻击、使用的身份验证技术和显示的安全证明进行分类。

iii. 最近的进展也从区块链的角度进行了审查，按区块链平台和共识分类。

iv. 该研究讨论了已在基于区块链的车辆网络研究中使用的各种模拟工具。

v. 我们还对其他最先进技术的作用提供了一些见解，包括但不限于云计算、雾计算、边缘计算、软件定义网络 (SDN)、命名数据网络 (NDN)、人工保护基于区块链的车辆网络的智能、5G 等。六。根据调查，我们提出了一些主要挑战
以及该领域未来可能的研究方向。

C. 组织

本文的其余部分安排如下。在第二部分，我们介绍了 VANET、车联网和区块链技术的背景知识。我们在第三节从应用的角度讨论了基于区块链的车载网络安全框架。第四节从安全角度讨论了不同基于区块链的作品的分类。这些工作在第五节从区块链的角度进一步分类。第六节介绍了所使用的不同模拟工具的汇编。我们将在第 VII 节讨论其他最先进技术在保护基于区块链的车辆框架中的作用。第八节描述了使用区块链保护车辆网络的现有挑战/未解决的问题，并提出了一些未来的研究方向。最后，我们得出结论

表 II 调查中使用的 主要 A 缩略语

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

第九节中的论文。本次调查的组织概况也如图 1 所示。

二、B 背景知识_

本节简要介绍了 VANET、车联网和区块链技术的背景。

A. 车载自组织网络

车载网络背后的理念是采用用于联网计算机的无线技术并将其应用于车辆。车载网络的技术术语是车载自组织网络 (VANET)。Ad-hoc 网络没有定义的基础设施，因此网络拓扑必须由网络中的节点通过协作机制来决定[27]。换句话说，没有中央权威，节点本身就像路由器一样负责在网络中传播信息。

B. 车联网

车联网可以看作是 VANET 的扩展，其中车辆联网能力用于连接到互联网或云服务，并基于 IP 连接的基础设施创建智能交通系统 (ITS)。VANET 提供数据连接；IoV 包括大规模处理该数据，以提供基本服务。理想的 IoV 网络将是车辆、环境和道路上的人的无缝集成，这将提高全市或全国范围内的交通安全和效率。大数据、云计算和人工智能是可以与 VANET 结合使用以实现这一目标的技术。*Yang 等人*首先提出了 IoV 网络的抽象架构。[28]。

车联网应用可分为两大类，即安全应用和商业应用。安全应用是必不可少的服务，例如防撞、限速信息和紧急制动信息等。这些应用程序需要网络中的低传输延迟，因为它们通常是时间敏感的。商业应用包括提供天气和交通信息、媒体流、即时消息或任何其他增强驾驶体验的服务。重要的区别是安全应用程序是必不可少的并且是硬实时应用程序；它们不得受到商业应用的干扰。

IoV 应用的一些示例如下所示：Olaverri-Monreal 等。*Lin 等人*提出了一种视频流技术，可以提高驾驶员可见性的可见性，并支持在具有挑战性的场景中超车 [29] 。提出了一种基于 GPS 和 3G [30] 的车载诊断系统，以及 Lee *等人提出的 MobEyes*。是一个智能系统，它利用支持无线的车辆来执行事件感知，通过让移动节点通过从其环境中提取特征并与相邻节点共享来不断生成数据摘要[31]。

C. 区块链技术

区块链是一种新技术，在金融 [32]、无人机 [33]-[36]、物联网 [37]-[40]、智能城市 [41]、[42]、智能电网 [40]、供应链管理 [43]、VANETs [44]、[45] 等等。它最初是由 S. Nakamoto 在他关于比特币的白皮书 [46] 中提出的。区块

链是一种保存数字交易记录的数据结构，正式称为分布式账本。数据库的相同副本存在于多个不同的计算机上，在区块链术语中称为节点，连接在对等网络中。交易是区块链的基本单元，在一个区块中存储一定数量的交易，并不断地依次附加区块，形成一条链。

下面概述了构建区块链的一些核心思想：

表三

研究基于区块链的安全工作的一些常见应用领域的问题和建议的解决方案

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
Transportation	[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)
	[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.	—

1) *数字签名：*公钥密码学是区块链技术的核心概念之一。每个代理都分配有一个私钥和一个公钥。使用私钥加密的任何东西都只能使用公钥解密，反之亦然。公钥作为每个节点的地址，每个数字资产都与其所有者的公钥相关联[47]。使用私钥对需要传输的数据进行签名。这可用于验证信息；如果使用私钥对数据进行加密签名，那么唯一可以解密它的就是同一个用户的公钥。区块链

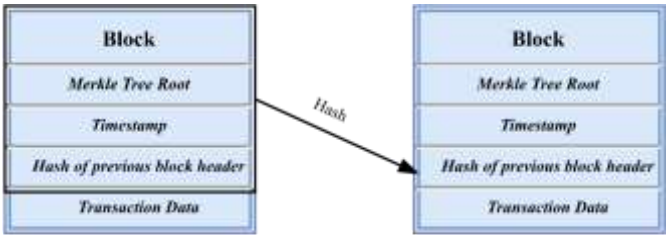


Fig. 2. Blocks in a blockchain.

常用椭圆曲线数字签名算法[48]。

2) *散列：*散列算法可以说是区块链技术的支柱。散列函数是一种加密算法，它接受可变大小的输入并返回固定长度的输出，称为散列。SHA 系列（SHA-1 和 SHA-2）是流行的散列算法。一个好的哈希算法必须遵守两个条件：
   a) 它必须是不可逆的；即，在给定输出的情况下，不可能检索输入。
   b) 两个不同的输入给出相同的输出哈希的机会必须非常小。

   这对安全性有用的原因是一个小的输入更改将完全改变哈希值，这使得篡改变得明显。

3) *块：*区块是区块链的组成元素，通常由区块体和区块头组成。块体包含交易和交易计数器。区块头包含不同的信息，例如默克尔树根、时间戳、区块版本和前一个区块头的哈希值。这些存储的哈希值为事务提供了不变性。如果任何一个区块中的交易被改变，那么它会改变区块头，并且哈希值将与存储在后续块中的哈希值不同，因此篡改是显而易见的。每个块都通过共识算法进行验证，并使用一个必然昂贵或难以执行但易于验证的过程添加 - 不变性来自于恶意实体将无法满足这种难以执行的条件的信念-但易于验证的挖掘过程，因此不能简单地更改块的哈希值来掩盖任何篡改。如果某个区块在创建后被修改并添加到链中，则需要对所有后续区块执行挖掘过程，这实际上是不可能的。区块链是公开的，因此参与节点将能够查看但不能修改内容。一串按顺序附加的块形成区块链。不能简单地更改块的哈希值来掩盖任何篡改。如果某个区块在创建后被修改并添加到链中，则需要对所有后续区块执行挖掘过程，这实际上是不可能的。区块链是公开的，因此参与节点将能够查看但不能修改内容。一串按顺序附加的块形成区块链。

4) *共识算法：*点对点网络中的节点负责验证交易并将其添加到区块链中。这个过程被称为挖矿，是区块链网络最重要的元素之一，因为它负责其去中心化的性质。共识背后的基本思想是节点必须经历一个难以执行但易于验证的过程——阻止恶意实体获取验证无效交易所需的必要条件。

综上所述——假设爱丽丝希望将数字资产发送给鲍勃。然后，Alice 必须使用她的私钥对资产进行签名，并使用该项目和 Bob 的地址广播一个交易请求。矿工在收到交易后，会将该交易与块体中的其他几笔交易捆绑在一起。矿工还将创建区块头，然后将区块头广播到其他区块链节点。这些区块链节点然后执行预先确定的共识算法。如果该块被批准，则将其添加为最新块，并且所有节点都会更新分类帐以反映更改。矿工在这一切中的基本作用是将交易收集、验证和打包成一个块，

区块链有两大类——许可和无许可：

i. 无许可区块链是公开的和开放的访问；任何人都可以加入区块链并参与共识机制。感兴趣的具有 Internet 连接的用户可以加入成为网络的一部分，并且参与者的身份被隐藏，这是一个安全问题。
ii. 许可区块链在读取访问或参与共识过程方面对成员节点施加限制，或两者兼而有之。这通常有助于计算和网络通信开销，这是无许可网络延迟的主要原因。

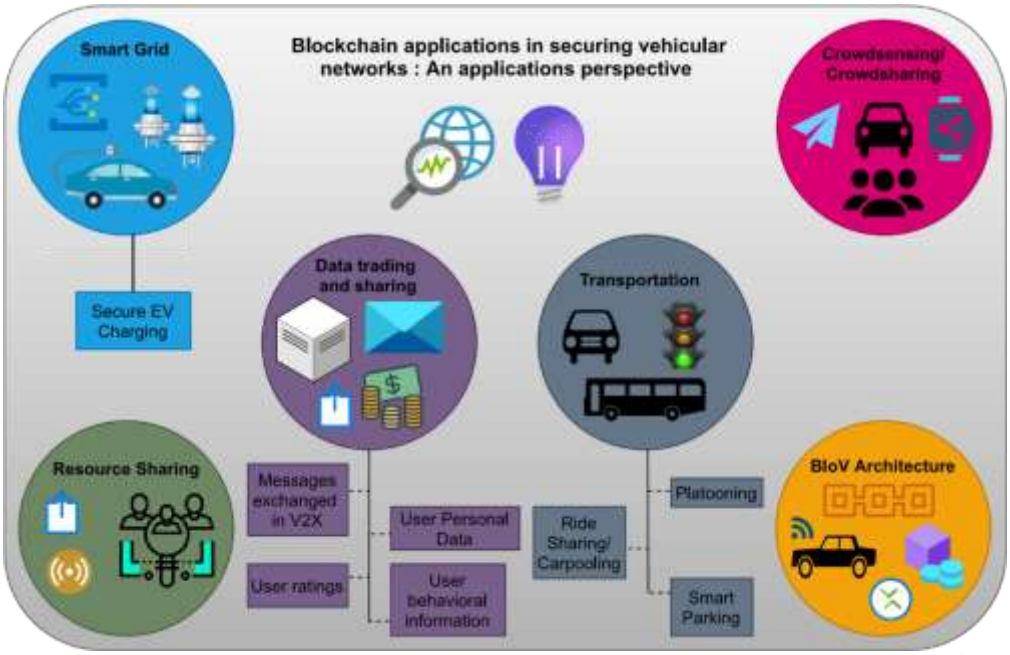
智能合约是可以在区块链上运行以促进和执行协议条款的计算机代码。Szabo [49] 于 1997 年首次提出，智能合约背后的概念是在满足合同/协议的指定条件时自动执行协议的功能/任务。

三、基于应用场景的 C 类 B _

在本节中，我们从应用的角度对不同的基于区块链的安全工作进行分类，即基于所考虑的应用领域。

A. 数据交易与共享

数据交易/共享的概念是将数据视为商品，车辆能够从网络“购买”和“出售”数据。从非常广泛的角度来看，这是所有其他基于区块链的 IoV 框架背后的基本概念；无论是



资源共享的计算信息还是智能电网应用的电池电量信息。必须共享数据以使车辆相互协调。但是，我们将其作为一个单独的重点领域来描述研究，该研究侧重于从获取数据的研究工作中优化数据交易/共享框架

图 3. 应用透视部分概述。

理所当然地分享并专注于网络的其他方面。我们将车载网络中的数据分为四大类：

- *信息交换：*车辆通过交换传感器数据和交通相关信息等信息相互通信。
- *用户个人数据：*用户个人数据是指用户身份、姓名、电子钱包详细信息、图像和视频——可用于识别车辆的任何内容。它还可以包括电动汽车 (EV) 的重要参数，例如电池的充电状态 (SoC)、电池容量和行驶时间表，所有这些都决定了 EV 的类型。
- *用户行为信息：*这包括有关个人在参与交易网络（数据交易、资源交易和能源交易等）时的交易偏好、个人的好恶——任何可用于预测如何进行交易的信息。用户会表现的。
- *用户评级：*各种框架根据车辆以前的历史记录为车辆分配信任评级，其他节点可以使用这些历史记录来评估用户的可信度。这些评级需要防止恶意车辆上传的虚假评级。当车辆离开一个车辆网络并加入另一个网络时，此类数据将被共享。

B. 交通

该应用领域主要处理车辆移动和管理。实时协调车辆可以实现更有效的移动——人们可能会想到即使现在交通信号灯和标志是如何管理和协调交通的，并考虑如何通过极其具体的车辆行驶信息以数字方式扩展这一概念[84]。对于分布式系统以外的任何东西来说，它为过于集中或计算量太大的协作开辟了可能性。其中一些可能性概述如下：

- *拼车/拼车：*减少道路上的车辆数量是改善环境条件和道路安全的必要步骤。区块链的两个方面，即内置加密货币和智能合约使其适合这项任务。
- *编队：*汽车组成一个组并作为一个组导航的概念有几个优点。首先，它减少了交通拥堵，因为协调几组比协调几辆车更容易，其次，它减少了事故的机会。区块链在 [26] 中用作实现此目的的交易框架。
- *智能停车：*许多停车场的使用效率低下，停车模型相当简单，包括固定的小时费率。这些费率在很大程度上取决于当地需求。这种需求可以分散到更大的区域，从而减少未充分利用的停车区的数量。从概念上讲，它只是更有效的资源分配。许多研究都集中在开发智能停车机制 [85]、[86]，例如 Zhang *等人*。提出了一个基于区块链的智能停车框架，将客户与可用停车场联系起来[58]。

C. 智能电网

该应用领域涉及电动汽车[87]。智能电网区别于传统电网的关键特征是大数据分析的适用性。消费者也可以向电网出售能源，这意味着如果现有资源能够满足需求和供应，就不需要产生额外的电力。智能电网需要具有容错能力，能够快速处理任何可能的故障。再次，分布式系统来拯救他们。可扩展性是此类应用程序的主要挑战。因为基础设施和配电的复杂性与地理区域非常不成比例。正在提出更新的区块链架构以提供可扩展性[88]。安全的电动汽车充电是智能电网最常见的应用。随着电动汽车的出现，协调充电计划以保持安全的方式随着时间的推移平衡供需是这类研究工作的主要重点。区块链还提供了一个支付平台，用于奖励与电网共享能源的车辆，例如，如果有人意识到他们在旅行后有多余的电量。

D. 资源共享

云计算是该研究领域的关键驱动技术。范式是相同的——交换计算资源以进行支付，除了车辆网络和边缘计算的复杂性。区块链可用于构建分布式开放市场类型的系统，而不是依赖于单个第三方提供的计算。假设车辆与典型的嵌入式系统不同，可能配备相对更高的处理能力，这使得它们成为计算资源的提供者；他们也可以充当消费者，从 RSU 购买资源。

E. 众筹/众筹

与数据共享类似，众感应用更侧重于优化系统以进行聚合数据收集，而不是点对点数据交易。人群感应允许服务提供商实时收集数据，而区块链允许人们安全地做出贡献（也许是为了支付）。这在地图和基于位置的服务中尤其有用，例如，通知车辆前方发生碰撞或道路封闭。目前已经在实践某种形式的众包，但它缺乏强大的激励机制，这限制了它的有用性。

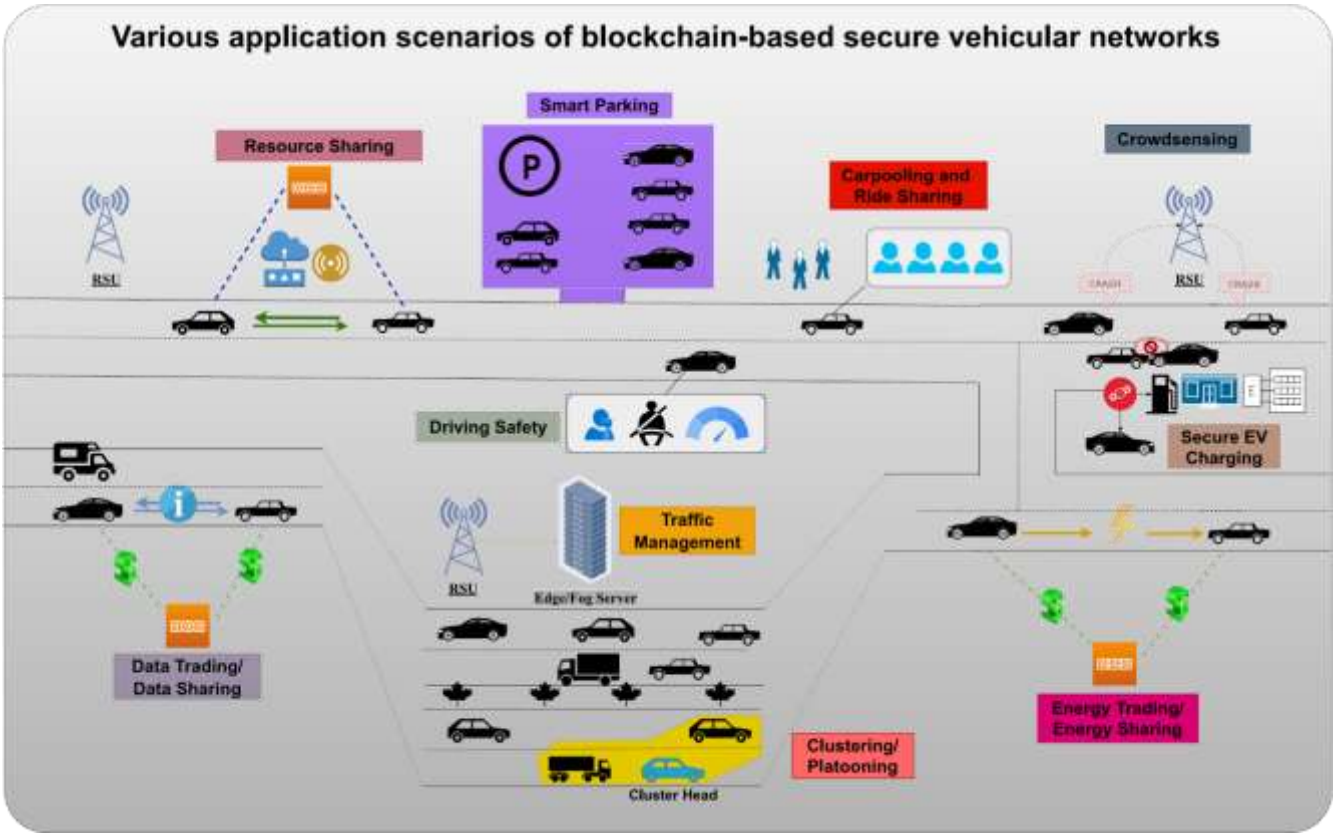


图 4. 区块链用于确保安全的各种应用场景的主题视图。

F. BIOV 架构

迄今为止分析的每个应用领域都是区块链和车联网技术的某种整合。但是这个研究领域值得单独提及，因为它在研究重点方面略有不同。许多研究工作都在优化区块链的核心特性，使其更适应 VANETs。例如，[24] 提出了一种用于车辆网络的自定义共识算法，[80] 引入了一种专门用于支持区块链的车辆网络的节能集群协议。这个研究方向在概念上与其他研究方向不同，因为要解决的主要问题不是通过使用区块链来提供服务，而是通过改变区块链和/或 VANET 的一些核心特征来克服现有的限制。

摘要： 在本节中，针对不同的应用领域对几个基于区块链的 IoV 框架进行了分类。详细讨论了数据交易和共享、交通运输、智能电网、资源共享、众包/众包和 BIOV 架

构等场景，解释了它们的实用性，每个框架都归入其中一组。

四。基于安全功能的 C 分类 _ _

安全视角部分根据以下类别类型对不同的基于区块链的安全工作进行分类。

i. 满足安全要求
ii. 防止网络特定的安全攻击
iii. 认证技术
iv. 安全证明。

每个类别的目的和范围以及其中的字段定义已在后续部分中定义。这将使读者对使用基于区块链的框架在车辆网络安全方面所做的研究有一个整体的看法，从而有助于该领域的进一步研究。

A. 安全要求

安全要求是网络为减轻网络中的攻击和漏洞而应满足的条件。已经有各种研究为车载网络定义了不同的安全要求[101]-[103]。区块链技术由于其去中心化的性质和防篡改的存储机制，隐含地提供了其中一些安全要求。因此，任何基于区块链的安全框架都将默认满足以下安全要求。

1) *化：*区块链通过启用 P2P 网络消除了任何第三方的参与，其中一些区块链节点验证交易。这通过消除与第三方共享其详细信息的需要来保护车辆的隐私[17]。该属性在车辆网络中具有多种应用，例如分散式通信 [89]、数据共享 [90] 和身份管理 [91] 等。
2) *防篡改：*记录在区块链中的数据很难被篡改，因为它是以哈希链[93]等特殊结构的形式组织的，每个区块都包含前一个区块的哈希值。这确保了不可逆性和不变性，因为篡改任何块中的数据都会改变其哈希值并将其与区块链断开连接。此外，区块链的分布式特性确保了数据在任何中间阶段都不会因为第三方的消除而被篡改，即去中心化也导致了防篡改[92]。
3) *不可伪造性：*指网络抵抗对手伪造数据或用户数字签名的能力。区块链的去中心化特性与其数字签名交易相结合，保证了这一点，并确保对手无法冒充其他用户 [90]。在[93]中，李等人。使用基于区块链的公平和匿名广告传播方案，使用称为零知识证明的流行身份验证算法确保不可伪造性。
4) *可追溯性（通过密码散列）：*区块链中的每个块都包含前一个块的密码散列，从而确保可追溯性[92]，[93]。每个节点都可以跟踪和验证数据的对应关系。这将有助于追踪任何恶意活动或消息流通，从而避免车辆网络中的混乱和事故。
5) *公共审计：*区块链通过其共识机制帮助实施公共审计。矿工创建的区块必须满足所使用的共识机制的标准，并且还应该由网络中的其他节点独立验证。此功能已在 [94] 中用于车辆到电网能源交易中的身份验证，并在 [17] 中用于公开审计 IoV 环境中的跨国数据交易。

除了上述安全要求外，基于区块链的方案还必须满足其他安全要求以提高其稳健性。在本研究中，以下是考虑的安全要求列表（不包括区块链隐含的要求）：

1) *不可否认性：*确保发送者不能否认消息的传输，并确保在发生事故时易于识别车辆节点。拒绝攻击的缓解属于此安全要求。它可以通过确保以下来满足。
   a) 所有传输的消息都由传输节点通过其匿名公钥签名，以确保该节点不能声称是网络中的某个其他节点（这可能导致伪装攻击）。
   b) 该节点不能声称该消息已被重放，因为该消息已加盖时间戳。对于调查机构来说，在发生事故时找到事件链和消息细节至关重要。
   c) 由于实施了安全定位解决方案，车辆不能伪造其位置信息。
2) *隐私保护：*满足此安全要求的框架可确保参与节点的隐私信息不会泄露给公众或恶意方。此外，应保证司机的隐私不受未经授权的观察者的影响[104]。它主要有两个重要的特点：
   a) *匿名性：*不应透露节点的具体个人详细信息，例如名称和车辆类型。它通过确保对于每个传入交易，所有可能的发送者都是等概率的，即不可追踪性[70]（不要与作为安全要求的可追踪性混淆）来防止恶意方跟踪用户的活动。匿名通常是通过使用假名和密码技术来实现的。它可以减轻跟踪攻击[23]。
   b) *性：*确保攻击者无法链接接收到的来自同一发送者的消息；或者换句话说，对于任何两个传出交易，不可能证明它们是被发送的同一个人[70]。这类似于前向安全[62]。
3) *可追溯性（通过有条件的隐私）：*通过将车辆的假名与其真实身份相关联，政府机构或受信任的第三方必须能够在车辆被发现有恶意时追踪其身份。参考文献 [93] 也将其称为条件可链接性，并满足此安全要求以防止“双重声明”攻击。
4) *钱包安全：*大多数车辆框架都有激励机制，并用加密货币奖励车辆在网络中的正常行为。车辆还相互支付加密货币以换取服务和数据。因此，通常每个车辆用户都有一个与之关联的电子钱包。满足这一安全要求可确保用户的钱包免受恶意攻击。在 [93] 中，每个用户都使用一个提供安全钱包服务的客户

端来管理加密货币代币并连接到区块链网络。参考文献[17]使用加密数字签名保证车辆的账户安全。如果没有相应的密钥和证书，攻击者无法打开车辆用户的钱包。

5) *可扩展性：*可扩展性确保即使网络中有大量参与车辆时框架也是高效的。对于基于区块链的框架，可扩展性的衡量标准是区块链管理大量交易的能力[105]。低计算开销和适应流量的动态共识算法是实现这一目标的一种方法[98]。根据[96]，去中心化也带来了可扩展性。为了评估框架是否可扩展，可以使用各种模拟平台，并将结果与基准区块链框架（如 Hyperledger Caliper [68]）进行比较。

6) *低延迟和高吞吐量：*低延迟是指网络延迟更少，而高吞吐量是指区块链能够在有限的时间内将大量交易添加到链中。这些都是重要的要求，因为较慢的网络给对手更多的时间来执行攻击[91]。这个安全要求是主观的，没有很好的定义，但考虑到网络的安全性，仍然值得讨论。

表 IV 列出了各种安全要求、满足这些要求的框架、它们的相应定义以及它们有助于缓解的攻击。

B. 网络特定的安全攻击

由于在开放和动态的环境中运行，车载网络容易受到多种安全攻击。因此，大多数安全方案确保他们提出的框架能够抵抗众所周知的网络安全攻击。在本节中，我们将讨论在现有的基于区块链的车载网络安全方案中已经解决的常见网络安全攻击。安全攻击列表如下。

1) *重放攻击：*在这种攻击中，恶意实体模仿合法用户并重放之前捕获的网络中传输的数据。进行这种攻击的目的是针对系统的真实性和机密性，并防止在发生事故或事故时跟踪车辆[112]。

2) *中间人（MITM）攻击：*恶意实体拦截并更改网络中合法节点之间交换的消息[113]。

3) *冒充攻击：*恶意实体冒充网络中的另一个实体并代表它发送消息[63]。它也被称为伪装攻击。

4) *特权内部攻击：*对手是网络内的特权用户，可以访问网络中已部署实体的加密信息，例如证书和私钥[63]。

5) *欺骗攻击：*恶意实体在网络中传播虚假数据。它可能会向邻居广播虚假消息，导致交通事故和拥堵[111]。它还包括关于网络传输通道可用性和其他资源的错误报告生成[93]。它也可以是 GPS 欺骗攻击的形式，对手在基于位置的网络中注入错误的位置数据 [57]。

6) *恶意第三方（MTP）或恶意攻击：*大多数基于区块链的车辆网络方案使用信任管理系统，在该系统中，它们根据其他网络车辆对其过去行为的反馈来存储每辆车的可信度等级。恶意车辆可能会产生虚假评级并将其上传到区块链（或其他维护信任记录的存储场所）中，以降低真车的可信度并提高恶意车辆的评级。这称为 MTP，或说坏话攻击 [14]、[111]、[114]。

7) *Ephemeral Secret-Key Leakage (ESL) 或后台分析攻击：*在 ESL 或背景分析攻击中，攻击者通过分析先前使用的泄露会话密钥或用户的假名身份来找出会话密钥或用户的真实身份，从而破坏用户的隐私。如果用户每次都继续使用相同的假名或密钥，攻击者可以轻松找出实际身份/行为或闯入通信会话。此外，在实体之间通过公共会话进行安全通信的情况下，会话特定秘密（临时秘密）的泄露可能会危及网络和进一步通信会话的安全。此类攻击可分为 ESL [63] 或背景分析攻击 [64]。它们可以通过满足隐私保护的安全要求来缓解，特别是不可链接性或前向安全性。安全方案可以使用随机秘密以及特定于会话的秘密来确保每个会话都有不同的会话密钥。公开的一个特定会话的会话密钥不会影响未来的会话。这也被称为“完美的前向和后向保密”[63]。可以允许车辆使用一组随机生成的假名而不是单个假名，以防止恶意车辆通过背景分析将其真实身份与假名联系起来。

8) *Sybil 攻击：*当恶意实体试图通过同时引入大量伪身份或假名来控制网络的很大一部分时，就会发生 Sybil 攻击[115]。它可以利用它们来非法改变其他节点的信誉值（即，Sybil 攻击可能导致恶意攻击）。大多数车载网络都提供匿名转发公告的功能，这使得它们容易受到女巫攻击。王 *等人。*[67] 讨论了 Sybil 攻击如何在能源交易场景中发生。在 [104] 中，作者通过使用基于拉格朗日插值的阈值密码技术来缓解 Sybil 攻击，该技术确保仅使用固定数量的不同私钥来生成签名。

9) *拒绝服务 (DoS) 攻击：*在 DoS 攻击中，对手试图通过向网络充斥非法服务请求 [116] 来使合法用户无法使用网络资源或在线服务。一些例子包括对伊朗网站的 HTTP-DoS 攻击，该攻击导致重要的政府网站 [117] 和对美国医疗保健政府网站的 DoS 攻击 [118]。Li 和 Hu [66]讨论了车载网络电力交易背景下的 DoS 攻击，其中攻击者需要破坏大量区块链节

表四

各种安全要求的总结， 一些满足这些要求 的框架，

他们的定义和有助于缓解的 方法

	Security requirements		Alternate names / Other similar security requirements	References	Definition	Attacks covered
BLOCKCHAIN SPECIFIC	*Decentralization*		Without third party reliance	[17], [89], [90], [91]	Nodes participate in a P2P network eliminating the need of a third party.	SPoF (Single Point of Failure)
	Traceability (Via transparency)		Transparency	[92], [93]	All the events in the network can be sequentially traced.	Repudiation attack
	Tamper proof		Data integrity	[92], [93]	The stored data inside the network cannot be tampered with.	Data tampering/modification attack MITM Block tampering attack
	Unforgeability		-	[90], [93]	Adversaries cannot forge data or user's digital signature.	Forgery Attack
	Consensus mehanism		Public audit	[17], [94]	Data stored in the network is verified by the network nodes.	MITM
NETWORK SPECIFIC	*Non-repudiation*		-	[66], [92], [93], [25], [60]	Ensures that senders cannot deny that they have sent messages or made transactions.	Repudiation attack, Masquerade/impersonation attack, Forgery attack
	Privacy preservation	*Anonymity*	Untraceability	[23], [92], [95], [66], [70]	Ensures that personal details of users are not compromised while still allowing them to participate fully.	Tracking attack
		Unlinkability	Forward and backward security	[70], [94], [95], [25], [69]	Ensuring that attackers cannot use the relation between two messages sent by the same user to violate that user's privacy.	Background analysis attack
			Known key security		Privacy of future sessions is guaranteed even in case the session key is leaked for one of the previous sessions.	Ephemeral Secret Leakage (ESL)
	Traceability (via conditional privacy)		Conditional linkability	[23], [25], [93], [60], [81]	In the event of an attack, the identity of the offending vehicle must be revealed to authorities.	Double claim attack Repudiation attack
	Wallet security		Account security	[90], [93], [96], [72], [97]	The security of the e-wallet used by the vehicles is guaranteed by the network.	-
	Scalability		-	[66], [91], [92], [98], [99]	The network functionality and performance are not affected when the number of participating vehicles become very large.	-
	Low latency and high throughput		Low computational overhead	[100]	There are minimal network delays and the network is capable of adding a high number of transactions to blockchain in a short time span.	All kinds of attacks (as more latency gives more window to adversaries for carrying out attacks)

点并控制它们向目标发送交易，以防止目标节点参与电力交易.

10) *分布式拒绝服务（DDoS）攻击：* DDoS 攻击类似于DoS攻击，但DoS攻击是通过单个节点执行的，而 DDoS 攻击是通过网络中的多个节点进行的。DDoS 攻击通常通过“僵尸网络”进行。首先，通过用恶意软件感染几个节点来控制它们。这些受感染的节点同时被用来攻击特定的目标机器。这种可以相互通信的受感染节点网络称为僵尸网络。李*等人*。[93] 讨论了车载网络中广告传播场景中的 DDoS 攻击。冯*等人*。[99] 提出了一种区块链辅助身份验证机制，用于减轻 DDoS 攻击以及防止其他常见攻击，如重放和模拟攻击。

11) *攻击：* 指拒绝实体参与车载网络中的全部或部分通信。例如，车辆驾驶员可以拒绝进行信用卡购买，或者对手可以滥用匿名身份验证技术来逃避责任[119]。这种攻击场景可以通过满足不可否认性的安全要求来缓解。Li 和 Hu [66] 讨论了在基于联盟区块链的电动汽车充电和放电方案中借助数字签名减轻拒绝攻击。

12) *窃听攻击：窃听*的字典含义是指偷偷听别人说话的行为[120]。在车载网络场景中，攻击者可以窃听车辆、边缘节点、雾计算节点 [69] 和 RSU 等网络实体之间的通信。在 [89] 中，作者提出了一个正式的安全证明，证明他们的框架如何使用 RSA（使用 2028 位加密算法）对系统进行加密以抵抗窃听攻击。诸如 Burrows-Abadi-Needham (BAN) 逻辑之类的正式安全证明也可用于确定一组交换的消息是否可以防止窃听。

13) *共谋攻击：* 这是一种网络节点与对手达成秘密协议的安全攻击。攻击者可以使用受感染的节点进行恶意活动以利用系统，例如收集机密信息、执行复杂的攻击、注入虚假数据等 [121]。它还可能导致各种网络安全攻击，从而对车载网络构成严重威胁。一些基于区块链的安全方案讨论了可能在车辆网络中发生的各种类型的共谋攻击，如下所示。
    a) *矿工投票串通：* 恶意 RSU 与受损利益相关者之间的串通可能导致选举虚假矿工，这些矿工可能会在挖掘算法期间修改或丢弃合法交易数据。
    b) *区块验证合谋：* 在区块验证阶段，矿工合谋也可能造成错误结果，这可能是发动双花攻击的垫脚石[114]。
    c) *串通认证欺诈：* 网络中具有自私意图的多个代理车辆可以通过尝试重组网络秘密[62]来协作执行认证欺诈。可以通过增加代理车辆的数量和存储身份验证交易记录来缓解这种情况。

14) *伪造攻击：* 指攻击者在不知道各自签名者的私钥的情况下试图重新创建消息的数字签名的攻击[122]。它可以通过满足不可否认性的安全要求来缓解。根据 [106] 的作者，伪造攻击在车载网络场景中非常常见。他们使用数字签名，其中密钥由称为受信任机构 (TA) 的完全受信任的机构生成，并存储在物理隔离的防篡改设备 (TPD) 中。在 [17] 中，作者使用加密签名来防止对手伪造车辆的签名以获得对大部分网络资源的控制。Tan 和 Chung [65]，以及 Sutrala *等人*。[107] 使用随机预言模型进行验证，正式证明他们的框架可以抵御伪造攻击。

表 V 列出了各种基于区块链的网络特定攻击、为车载网络提出的安全方案以及在每个方案中缓解的安全攻击。

C. 认证技术

身份验证是任何安全框架的重要组成部分，在缓解大多数安全攻击方面发挥着重要作用 [8]、[123]。我们在下面列出了一些在基于区块链的车辆安全框架中使用的流行身份验证技术。

1) *双向/双向认证：* 在这种类型的认证中，客户端（车辆）和接入点（RSU）都相互认证。客户端验证它正在打开与合法接入点的会话，并且接入点确定它正在与授权客户端打开会话。验证接入点有助于减轻 MITM 攻击，验证客户端有助于减轻重放攻击[124]。万加拉*等人*。[63] 在他们提出的框架的认证阶段讨论了如何在集群头和集群内的车辆（V2CH）之间以及集群头和 RSU（CH2RSU）之间建立相互认证。在[95]中，作者正式证明了他们的安全模型如何实现电动汽车和充电桩之间的相互认证。

2) *匿名认证：* 它是一种在身份验证过程中保护车辆隐私的身份验证方案。它也被称为隐私保护认证[125]。隐私是指用户拥有完全控制其个人信息的权利，并保留选择与他人共享哪些数据的权利。匿名性是指在有限的用户集中无法识别的质量。匿名是通过假名实现的，假名是用作身份验证的唯一标识符的位字符串，没有任何个人身份信息。因此，使用它们有助于在不知道其真实身份的情况下对特定实体进行身份验证，即匿名身份验证。匿名身份验证方案可以大致分为五类[125]。
    i. 基于对称密码学的方案
    ii. 基于公钥基础设施 (PKI) 的方案
    iii. 基于身份的签名方案 iv。基于无证书签名的方案
    v. 基于组签名的方案。

表五

作为网络特定安全攻击和 B LOCKCHAIN - B ASED FRAMEWORKS 解决这些攻击的总结 _ _ _ _ _

Attack Type	Definition	Security Concerns	Frameworks Addressing the Issue
Replay	Imitate a legitimate user and replay already transmitted data	Authenticity, Confidentiality	[23], [25], [61]–[63], [65], [66], [95], [98], [99], [106]–[108]
Man-in-the-middle	Adversary intercepts the communication between two nodes of the network secretly	Confidentiality, Physical security of the IoV network resources	[18], [25], [61]–[64], [66], [91], [95], [96], [107], [109]
Impersonation	Impersonate a legitimate node in the network secretly	Authenticity, Confidentiality	[61], [63], [66], [67], [69], [93], [95], [98], [99], [107]
Privileged Insider	Malicious insider has privilege account credentials/ privilege access in the network	Confidentiality, Data loss, Physical security of the IoV network resources	[63], [109]
Spoofing	Impersonate a user/ node of the network and get unauthorized access	Authenticity, Physical security of the IoV network resources	[57], [81], [91], [98], [110], [111]
Malicious Third Party	Adversary generates false ratings to disturb the trust records	Authenticity, Network stability	[14], [19], [63], [67], [107], [111]
Ephemeral Secret Leakage	Privacy is broken by obtaining user's credentials illegitimately	Authenticity, Confidentiality, Data loss, Physical security of the IoV network resources	[15], [60], [63], [64], [95], [98], [106]
Sybil	Adversary tries to control a significant part of network under false identities	Authenticity, Network Stability, Physical security of the IoV network resources	[25], [54], [67], [69]
Denial of Service	IoV network resources are made unavailable by flooding the node with false requests	Authenticity, Network Stability, Resource depletion	[77], [89], [110]
Distributed Denial of Service	IoV network resources are made unavailable across several nodes by flooding them with false requests	Authenticity, Network Stability, Resource depletion	[61], [66], [93], [99]
Repudiation	An entity of the network falsely denies participation in an activity	Authenticity	[18], [25], [60], [66], [83], [92], [93]
Eavesdropping	Secretly listening in on the communication between nodes	Confidentiality	[69], [83], [89], [98]
Collusion	A member of the IoV network colludes with an adversary to get them access	Authenticity, Confidentiality, Data loss, Physical security of the IoV network resources	[23], [93]
Forgery	Forging the signature of a member of the IoV network	Authenticity, Physical security of the IoV network resources	[17], [64], [65], [106], [107]

匿名身份验证通常用于车载网络中以保护隐私[60]。例如，在 [93] 中，作者使用匿名身份验证在车载网络中进行基于区块链的匿名公平匿名广告传播。姚等人。[60] 提出了一种用于分布式车载雾服务的区块链辅助轻量级匿名身份验证方案。

3) *基于证书的认证：*在基于证书的认证中，第一实体在与第一实体相关联的数字证书的帮助下向第二实体认证自己[126]。数字证书包含对应实体的公钥，证书的所有者可以通过证书中的数字签名来确认。数字签名由证书颁发单元验证，或者更具体地，由车辆网络环境中的证书颁发机构 (CA) 或 TA 验证。在 [63] 中，作者使用支持区块链的基于证书的身份验证方案 (BCAS-VADN) 使车辆能够安全地向集群头报告与事故检测和通知相关的交易和自己或邻近车辆的通知。周 *等人*。在区块链和边缘计算支持的车辆到电网能源交易中使用基于证书的身份验证[94]。*Kang 等人*也使用了它。[90] 在他们的插电式混合动力汽车本地化点对点电力交易模型中。他们聘请 TA（例如政府部门）来实施基于证书的身份验证。

4) *批量验证：*在批量验证中，不是单个消息/实体，而是一批消息/实体一起验证。根据[92]，批量验证可以解释如下：假设在 1 和 ***n***（都包括）之间随机选择一个整数 ***i***，*其中* ***n*** 是一个正整数，接收到的验证参数可以是 $Ver_i(AID_i, S_i, M_i, C_i)$。这里 C_i 是随机化参数，M_i 是消息，S_i 是最终的签名信息和 AID_i 是车辆生成的化名。对网络节点间共享的消息进行批量验证时产生的多个认证参数是协议。证明者必须通过几个交互式回合向某些验证者证明对秘密的了解。每一轮都包括来自验证者的挑战和来自证明如果 ***n*** *个*签名中的每一个都是合法的，则批验证通过 [127]。*如果* ***n*** *个*签名中的任何一个或多个无效，则批量验证失败。批量验证也可以分为三种：

$BatchVer_n((AID_1, S_1, M_1, C_1), ..., (AID_n, S_n, M_n, C_n))$

i. 验证签名者是否签署了不同的消息

ii. 验证不同的签名者是否签署了相同的消息 iii。验证不同的签名者签署不同的消息批量验证可以帮助安全方案应对验证多条消息时的时间延迟。在 [18] 中，作者在基于能源区块链的电动汽车电力交易框架中使用批量验证。林 *等人*。[61] 使用修改后的 ECDSA 加密方案来实现批量验证。此外，在 [65] 中，作者正式解释了如何在基于区块链的 VANET 的拟议安全框架的身份验证阶段实施批量验证。

5）*零知识证明（ZKP）：*当两个实体在不交换秘密信息的情况下进行身份验证时，使用 ZKP 算法[71]。这个概念最初是由 Lee *等人提出的*。[128]，从那时起，它在身份识别和身份验证匿名等方面发现了许多用途。

6)*阈值认证：*在车载网络中证明消息可靠性的标准方法。在这种技术中，接收节点仅在网络中的车辆数量达到阈值时才接受消息[104]。网络中的消息聚合是实现阈值认证和减少网络开销的好方法。李 *等人*。使用[104]中的阈值环签名方案来设计他们的框架 **“CreditCoin”**，这是一个基于隐私保护的区块链激励公告网络，用于智能车辆的通信。*Liu 等人*也使用它。[106] 在他们的基于区块链的 VANET 信任管理公告方案中。

表 VI 列出了各种安全框架以及它们使用的身份验证技术。

*摘要：*在本节中，基于去中心化、可追溯性等安全要求对不同的基于区块链的框架进行了分类，提供了针对 DoS、ing, Sybil 等，以及相互认证技术，spoof- 等多种网络特定安全攻击的保护

我们根据以下类别类型对不同的基于区块链的安全工作进行分类：

i. 区块链平台
ii. 区块链类型
iii. 共识算法。

V. 基于 B 锁链功能的 C 分类 B

了解不同的区块链平台和类型对于了解区块链如何用于车载网络应用程序至关重要。为了清楚起见，在本节中，

A. 区块链平台

自 2009 年比特币作为开源软件发布以来，随着区块链应用场景的扩大，许多其他平台也应运而生。这些平台通常是一种综合服务，附带工具包和生态系统，供开发人员构建他们的区块链应用程序。平台越先进，它提供的选项就越多——例如，Hyperledger 项目提供了几种不同的框架，具有不同的共识机制，并且是为不同的应用程序设计的。以太坊是另一个受欢迎的平台；虽然 Hyperledger 与任何代币没有严格关联，但以太坊（如比特币）与其加密货币（Ether/ETH）相关联，该加密货币与真实货币具有标准转换率。这很有用，例如，当区块链被用作现实世界市场互动的替代品时；在能源交易应用程序的示例中，通过采矿或其他活动获得的 ETH 可直接用于在充电站购买能源。除了加密货币，区块链平台通常不同的参数是可扩展性、吞吐量、共识机制、崩溃容错、拜占庭容错、智能合约支持（以及用于编程它们的语言） - 存在大量变化在许多技术规范中。被调查的研究工作分为以下几类：共识机制、崩溃容错、拜占庭容错、智能合约支持（以及用于编程它们的语言）——许多技术规范都有很大的变化。被调查的研究工作分为以下几类：共识机制、崩溃容错、拜占庭容错、智能合约支持（以及用于编程它们的语言）——许多技术规范都有很大的变化。被调查的研究工作分为以下几类：

表六

B LOCKCHAIN 使用的身份 验证技术调查-基于 S 安全框架的车辆网络_ _ _ _

Ref.	Mutual/Two-way	Anonymous	Certificate based	Batch verifcation	ZKP	Threshold
[63]	✓	✓	✓	_	_	_
[23]	_	✓	_	_	_	_
[92]	✓	✓	_	✓	_	_
[95]	✓	_	_	_	_	_
[66]	✓	✓	_	_	_	_
[93]	_	✓	_	_	_	_
[94]	_	_	✓	_	_	_
[69]	✓	_	_	_	_	_
[98]	✓	_	✓	_	_	_
[60]	_	✓	_	_	_	_
[106]	_	_	_	_	_	✓
[107]	✓	_	_	✓	_	_
[67]	_	_	✓	_	_	_
[65]	✓	_	✓	✓	_	_
[71]	_	_	_	_	✓	_
[83]	_	_	✓	_	_	_
[61]	_	_	✓	✓	_	_
[104]	_	_	_	_	_	✓
[59]	_	_	✓	_	✓	_
[68]	✓	✓	✓	_	_	_
[76]	_	_	✓	_	_	_
[129]	_	_	_	✓	_	_
[58]	_	✓	_	_	_	_
[130]	_	✓	_	_	_	_
[131]	_	_	✓	✓	_	_
[55]	_	_	_	_	✓	_
[73]	_	✓	_	_	_	_
[132]	_	✓	_	_	_	_

1) *Hyperledger Fabric（HLF）：* Hyperledger Fabric，由 Hyperledger 社区维护，是一个开源区块链项目。该项目提供了一些许可的 DLT 平台，专为在企业中使用而设计 [133]。它是第一个支持使用 Java、Go 和 Node.js 等通用编程语言编写的智能合约的 DLT 平台。它也是许可的，即，与公共无许可网络不同，参与者是彼此已知的。在 [81] 中，作者使用 HLF (v1.0.2) 作为他们的区块链平台，在 [22] 中，采用改进的区块链结构的扩展 HLF 架构用于提供隐私保护认证方案，

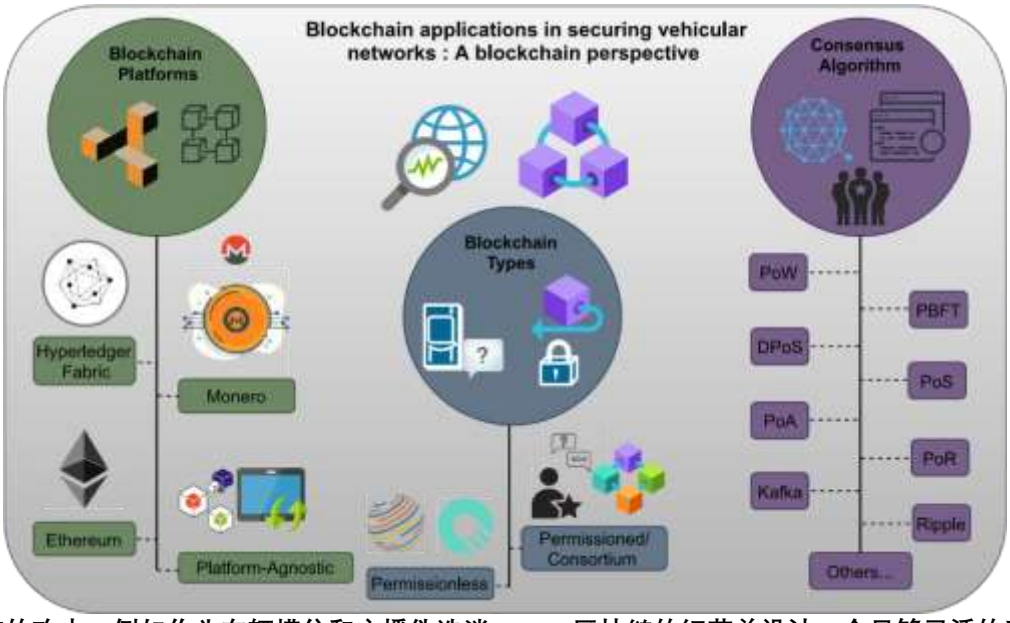


图 5. 区块链透视部分概述。

以抵御潜在的攻击，例如作为车辆模仿和广播伪造消息。

2) *以太坊：*以太坊是一个区块链平台，允许其用户使用图灵完备语言 Solidity 创建智能合约。智能合约拥有的账户功能类似于用户账户，除了它们包含可执行的字节码，它控制着智能合约账户的行为。当用户与智能合约拥有的账户进行交易时，存储的代码会被执行，并且以太坊虚拟机会记录更改。它已在许多框架中使用，例如，在 [129] 中，作者在其自适应流量控制机制中使用了以太坊区块链，而在 [96] 中，以太坊私有链用于 V2G 上 EV 之间的电力共享网络。

3) *门罗币：*门罗币是 2014 年发布的一种加密货币，主要关注隐私，是一种基于 CryptoNote 的开源协议。门罗币中使用的称为混淆公共账本的概念确保任何人都可以广播或发送交易，但外部的观察者无法找到目的地、来源和金额 [134]、[135]。*它用于由 Wang 等人*提出的 V2G 网络的基于区块链的匿名奖励方案 (BBARS) 。在[70]中。车辆可以将储存的能量卖回电网并获利。BBARS 系统模型涉及一个中央聚合器，该聚合器通过一个中间本地聚合器授权和支付车辆，以向电网提供多余的电力，但付款人或收款人都不需要对方的地址或身份来完成交易。椭圆曲线密码学用于确保所有交易的安全性。

4) *平台无关：*许多提出的研究模型仅利用了区块链的基本特征，例如去中心化的点对点共享机制和不变性。这些以及其他一些属性对于每个区块链都是通用的——在某种意义上，它们是属性，没有这些属性，软件首先就不能被称为“区块链”。因此，完全可以抽象出区块链的细节并设计一个足够灵活的系统，可以与任何区块链平台一起使用。已经有模型提出了基于博弈论的安全性[136]、恶意内容检测[109]、交通信号管理[25]、分布式集群节能[80]、GPS 精度增强[16]、队列[26]、数据分享[114]，

B. 区块链类型

主要有两种类型的区块链网络许可和无许可。许可的区块链保留验证和添加块到选定的几个节点的权利，而在无许可的区块链中，任何加入的节点也被允许（或预期）验证和添加块到区块链。这在很大程度上依赖于应用程序。例如，在能源交易的情况下，人们只希望属于注册公司的充电站提供交易平台。因此，添加交易的能力必须仅限于作为充电站的节点，而不是车辆本身。许可的区块链将适用于此。许可区块链也具有更高的吞吐量，因为延迟的很大一部分是由于对等交互 - 如果将其最小化，那么网络可以每秒处理更多事务。必须注意的是，在许可区块链中牺牲了去中心化的某些方面——需要在吞吐量和去中心化水平之间进行权衡。还有一些应用程序，如众包和数据共享，需要无需许可的区块链。已从调查集中选择了一些具有代表性的研究工作，以在下面更详细地说明这些想法。还有一些应用程序，如众包和数据共享，需要无需许可的区块链。已从调查集中选择了一些具有代表性的研究工作，以在下面更详细地说明这些想法。还有一些应用程序，如众包和数据共享，需要无需许可的区块链。已从调查集中选择了一些具有代表性的研究工作，以在下面更详细地说明这些想法。

1) *许可：*郑*等人*。[23] 提出了一种用于 VANET 的区块链系统，提供有条件的隐私——在这里，认证机构是唯一可以验证区块的实体。这是一个身份验证系统，其中合法身份的证明存储在区块链上 - 允许任何车辆向其添加块违背了目的，因此这必须是许可

的区块链。BloCkEd 是另一项提议的研究工作，它可以在车辆网络中实现有效的边缘计算 - 使用使用区块链在边缘设备之间迁移容器的想法，车辆的任务可以轻松地卸载到边缘计算设备，并且无论车辆采用什么路径都会返回结果[71]。该系统只需要边缘计算设备有权验证区块，因为车辆需要在同一个网络上才能与边缘设备交互，但不能参与容器的迁移。苏等。提出了一个能源共享框架[14]，其中只有充电桩有权验证交易。除了提高吞吐量外，这还确保所有交易仅通过受信任的智能电网运营商进行。

2) *许可：* 由于可扩展性问题，这种类型的区块链并不流行。然而，一些人群感知应用程序 [76]-[78] 部署了无需许可的区块链，因为区块链的交易是指示道路状况的信息片段。验证节点必须是也见证相同条件的对等节点，而不是在这种情况下某些受信任的权威 - 就像无许可的区块链如何破坏身份验证的目的，在这种情况下，许可的区块链破坏了众包的目的。Javaid 等人。[98] 提出了一种用于信任管理的无许可区块链 - 可扩展性问题由动态工作证明共识管理，其中难度阈值根据所需的安全保真度、规模和吞吐量不断变化。

C. 共识机制

选择一种共识机制而不是另一种的原因有很多。PoW 是迄今为止最常见的共识算法，但它效率低且浪费能源，更经济的替代方案是 PoS。这些都没有提供拜占庭容错，这是抵抗著名的拜占庭将军问题漏洞的质量。以下是根据所使用的共识机制分类的不同类型的研究工作的说明。

1) *工作量证明 (PoW)：* Zheng 等人。提出了一种车辆之间的匿名消息交换模型。由所有 RSU 组成的区块链采用的共识是 PoW。该算法需要通过反复试验来猜测随机数，耗时且成本高，但易于验证。只要恶意节点的数量不超过所有 RSU 的一半，交易信息就不能被修改，并且区块链越长，其安全性就越好 [23]。基于微区块链的动态入侵检测（MBID）是梁等人*提出的一种机制。*[148]用于入侵检测。微区块链嵌套在宏区块链中，它们共同提供了检测车辆网络入侵的策略。微区块链的主要任务是存储数据和入侵样本，并提供入侵检测策略（如果存在）

表七

C 分类 基于共识车载网络安全文件中使用的算法_ _ _ _ _ _

Consensus	Ref.
Proof of Work (PoW)	[15], [17], [18], [23], [54], [62], [72], [74], [78], [83], [94], [98], [106], [111], [130], [137], [138]
Practical Byzantine Fault Tolerance (PBFT)	[21], [56], [60], [63], [72], [75], [81], [91], [92], [97], [99], [106], [139]
Delegated Proof of Stake (DPoS)	[16], [52], [56], [79], [114], [140]
Proof of Stake (PoS)	[59], [73], [111], [141], [142]
Proof of Activity (PoA)	[61], [93], [96], [143]
Proof of Reputation (PoR)	[19], [62], [67]
KafKa	[66], [68]
Ripple consensus	[21], [104]
Attribute based consensus	[25]
Proof of Online Duration	[69]
Delegated Byzantine Fault Tolerance (DBFT)	[14]
Redundant Byzantine Fault Tolerance (RBFT)	[79]
Zero Knowledge Proof (ZKP)	[71]
Proof of Knowledge (PoK)	[144]
Proof of Utility (PoU)	[131]
DPOSP (PBFT-DPoS hybrid)	[145]
Proof of Elapsed Time (PoET)	[146]
Proof of Event (PoE)	[147]
AlgoRand	[78]

在微区块链中可用。宏区块链存储所有模型和收集的入侵情报，并在适当的微区块链中找不到这些策略时向车辆提供入侵检测策略。网络切片用于在同一区域部署微区块链。PoW 被用作宏区块链的共识算法。

2) *信誉证明 (PoR)：* 提出了一种采用 PoR 的区块链架构，用于 IoV 网络中的资源共享。轻量级区块链处理信任管理和隐私保护。分配信誉值以指示使用其建立共识的工具的信任程度。只有当 RSU 收集了最高的交易信誉总和时，RSU 才能发布区块 [19]。柴等人。[19] 提出了一种使用 PoR 生成块的资源共享区块链模型。信誉是根据历史记录的积累来决定的，信誉有一个饱和上限，以防止任何节点垄断区块链。信誉最高的节点创建固定数量的交易块。声誉较高

的节点更有可能将他们验证的块接受到主区块链中，并为购买计算资源支付更少的成本。

3) *股权证明（PoS）：*在一些工作中，委托权益证明（DPoS）用于实现网络共识。网络中的每个 RSU 根据其权益选择见证人参与区块链系统。票数最高的少数证人 (RSU) 将赢得验证权。The elected witnesses create new blocks in sequence as assigned and get some rewards. 由于减少了验证节点[16]，它加快了区块创建和交易验证的速度。在基于联盟区块链的车辆社交网络 (VSN) 中，车辆身份验证需要一定数量的高于阈值的 RSU 的联盟。如果将权益替换为活动等级（这表明 RSU 在领导者选择过程中的消息中继参与率），则此修改后的 PoS 是高效的 [64]。[114] 中的作者提出了一种增强的 DPoS 共识方案，该方案具有两阶段的安全解决方案，用于在基于区块链的 IoV 中安全地共享车辆数据。第一阶段，采用主观逻辑方法，基于信誉投票选出矿工。第二阶段，激励备用矿工参与区块验证。

4) *拜占庭容错（BFT）：*拜占庭容错只是对拜占庭将军问题的抵抗，即一定数量的对等节点可能无法达成协议，而诚实节点也不清楚哪些节点无法达成协议。即使某些节点出现故障或恶意行为，系统也必须正常运行，而不管其他节点是否知道这些事件。在能源市场中，恶意运营商将严重威胁电动汽车的安全和隐私。提出了一种基于合同的具有许可区块链系统的电动汽车安全充电方案，以满足电动汽车对能源的个性化需求，同时最大限度地提高运营商的效用。基于信誉的委托拜占庭容错（DBFT）共识算法高效达成共识。DBFT 提供 $f = (K-1)/3$ 对包含 K 的共识系统的容错性共识节点[14]。提出了一种方案，其中车辆公钥基础设施 (VPKI) 与许可的区块链和分散的分类账一起使用，为事故调查提供全面的取证服务。为从验证者节点（例如，RSU）中创建的每个块随机选择一个领导者。领导者向网络提出一个区块，验证者运行拜占庭协议（例如，PBFT）以就该区块达成共识。这些协议对领导者和参与者的恶意行为具有弹性[149]。提出了一种基于区块链的安全数据共享系统，由母链和辅助链组成。PBFT等共识机制用于保证消息的一致性。这里，公告消息由见证事件的每辆车签名 - 使用基于多重签名方案的短期密钥。在签名者的特定阈值下，公告消息被认为是可信的 [79]。

5) *其他机制：*开发了一种混合类型的区块链 (PermiDAG)，它由本地有向无环图 (DAG) 和许可区块链组成。它由本地 DAG 组成，并且具有分区容错性，这意味着即使在部分网络的情况下，区块链也可以有效运行。此外，通过将不同的学习参数集成到网络中，可以通过两阶段验证 [52] 进一步验证学习模型的特征。基于属性的区块链可用于改善 IoV 中的交通管理。参考文献[25]提出了一个使用这个概念的模型。基于属性的区块链中的节点通过其匿名身份（化名）和一组模糊身份（位置、行进方向）来区分——这两者都是属性。简单节点可以读取和生成新消息，而共识节点不能直接在区块链中写入/生成消息。但运行共识算法以实现数据一致性的是共识节点。为了改善城市交通状况并减少事故，[26] 提出了一种用于自动驾驶汽车的队列驾驶模型。车辆按排行驶，更有经验和可信的车辆担任排长。信用是一段时间内累积的集体信心指标，用于确定车辆是否值得信赖。在一个排中，声誉值增加了相关车辆成为下一个排长的可能性。这保证了排长的位置不被垄断。但运行共识算法以实现数据一致性的是共识节点。为了改善城市交通状况并减少事故，[26] 提出了一种用于自动驾驶汽车的队列驾驶模型。车辆按排行驶，更有经验和可信的车辆担任排长。信用是一段时间内累积的集体信心指标，用于确定车辆是否值得信赖。在一个排中，声誉值增加了相关车辆成为下一个排长的可能性。这保证了排长的位置不被垄断。但运行共识算法以实现数据一致性的是共识节点。为了改善城市交通状况并减少事故，[26] 提出了一种用于自动驾驶汽车的队列驾驶模型。车辆按排行驶，更有经验和可信的车辆担任排长。信用是一段时间内累积的集体信心指标，用于确定车辆是否值得信赖。在一个排中，声誉值增加了相关车辆成为下一个排长的可能性。这保证了排长的位置不被垄断。以更有经验和可信的车辆作为排长。信用是一段时间内累积的集体信心指标，用于确定车辆是否值得信赖。在一个排中，声誉值增加了相关车辆成为下一个排长的可能性。这保证了排长的位置不被垄断。以更有经验和可信的车辆作为排长。信用是一段时间内累积的集体信心指标，用于确定车辆是否值得信赖。在一个排中，声誉值增加了相关车辆成为下一个排长的可能性。这保证了排长的位置不被垄断。

图 6 展示了一个饼图，显示了被调查作品中各种共识机制的使用情况。

*摘要：*本节从它们提供的区块链功能的角度讨论了一些作品的分类。第一种分类是基于以太坊、HLF 等区块链平台进行的。其次，根据区块链的类型对不同的方法进行分组，即许可和无许可。此外，我们根据其采用的共识机制对用于 IoV 的基于区块链的框架进行分类。

六、RT BI O V F RAMEWORKS 状态下使用的仿真工具的汇编_

在本节中，我们将介绍用于模拟区块链和车辆网络的流行模拟工具的汇编。

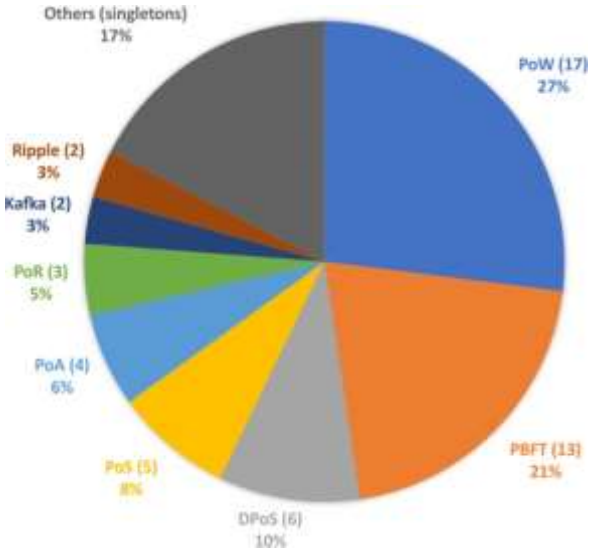


图 6. 饼图显示了被调查作品中各种共识机制的使用情况。

A. 模拟区块链的工具

MIRACL（多精度整数和有理算术密码库）是一种流行的开源 C 库，被广泛认为是椭圆曲线密码学 (ECC) 的黄金标准。区块链使用多种加密原语，包括散列和非对称密钥加密，因此可以使用该库进行编程。[70]、[79] 中的作者使用这个库进行模拟。PBC（基于配对的密码学）是另一个仅模拟基于配对的密码系统的数学运算的库；也就是说，没有认证机构或签名的公钥和私钥系统模拟。其中许多库与 GNU 多精度库 (GMP) 结合使用，允许开发人员对任意精确的数字执行操作，这对于密码学应用和研究很有用。基于以太坊的区块链模拟可以使用 Solidity，这是一种图灵完备（即计算通用）语言，可用于编写几乎可以执行任何应用程序的智能合约。[80]、[150]、[151] 中的作者在他们的区块链模拟中使用 MATLAB。IBM 的 Hyperledger Fabric 是一种开源区块链基础架构，可用于在 Java 和 Go 中构建区块链应用程序。该平台用于模拟许可平台，具有可配置的共识。Hyperledger Fabric 已在 [22] 中用于模拟。Hyperledger Caliper 是一种流行的基准测试工具，用于测量不同区块链解决方案的吞吐量、延迟和资源消耗；它也可以与以太坊平台一起使用。除此之外，Python 也被广泛使用。

B. 模拟车载网络的工具

[152] 中的作者使用 SUMO 和 OMNeT ++库来模拟区块链 IoV 中车辆网络的行为。SUMO 用于模拟流量，OMNeT ++用于模拟网络行为。Veins [153] 是一个模拟工具，它结合了这两种技术，以及模拟物理层属性（如无线电波传播、干扰估计和信号功耗）的 MiXiM 框架。[21] 的作者使用 Veins 来模拟他们模型的网络方面。其他使用 Veins 的出版物可以在 [154] 中找到。Go 是另一种开源编程语言，它是网络的有效选择，在 [23] 中使用。TraNS [155] 是一个流行的开源平台，它结合了 SUMO 模拟器和 NS2。然而，自 2008 年以来，它就不再被积极支持，iTETRIS [156] 是 TraNS 的逻辑扩展，耦合了 SUMO 和 NS3。Node.js 和 web3.js 也可以用来连接和交互系统中的不同节点。

小结： 在本节中，我们讨论了区块链网络的模拟工具，如 MIRACL、PBC 等，以及用于车载网络的模拟工具，如 OMNet ++ 、MiXiM 等。

七。BI O V F 框架中经常使用的重要技术的作用_

在本节中，我们将讨论如何使用各种最先进的技术来保护各种车辆网络，例如 IoV 和 VANET。表 VIII 列出了总结这些技术在调查工作中的作用的表格。

A. 云和雾计算

基于区块链的 IoV 是需要大量计算和硬件资源的系统，而管理这种负载分配的技术（如云计算）最终将发挥核心作用。

云计算是一种概念，即硬件和软件服务可以由那些需要它的人从那些拥有足够未充分利用的基础设施的人那里购买。通过互联网，用户可以购买他们需要的处理量或服务，并将任务卸载到远程计算单元，看似“云服务器”。这种硬件和软件的解耦允许创新者提出应用程序无需担心所需的硬件基础设施。这项技术对车辆特别有用，因为消费者拥有与预算一样多的资源。雾计算是云计算的扩展，云服务更接近传感器和嵌入式系统。在 IoV 的背景下，RSU 可以用作雾单元或到云的本地网关。从广义上讲，

1) 车载云（也称为自主车载云）[164]，其中节点是服务提供者。具有过多计算资源的车辆可以承担其他车辆的计算任务。
2) 使用云服务的 VANET，其中 RSU 充当 Internet 的网关。通过提供雾层，这项技术可以使车辆网络更加有效[165]-[167]。

表八

基于区块链的车辆网络中其他国家的角色_ _ _ _ _ _ _ _ _ _ _

Technology	Ref.	Role of other technology in the network
Cloud Computing	[63]	Cloud server was used as part of the blockchain center for creating, verifying and adding the blocks.

	[21]	Used trusted cloud servers as part of their system architecture to enhance network operations
	[83]	Some of the security managers are cloud based
	[104]	Used a cloud application server to store and exchange some non-cryptographic information in the network
	[59]	Used a cloud server to store the encrypted carpooling data
	[75]	A distributed and large cloud system is used for storing the Personally Identifiable Information (PII) of the vehicles.
Fog computing	[157]	Proposed a pseudonym based privacy preserving scheme for maintaining location privacy specifically in fog computing based IoV networks
	[69]	Used fog computing to overcome drawbacks of a cloud-based centralized management and to provide local computing capabilities with low latency
	[158]	Proposed a route sharing service framework with privacy-preservation where fog nodes pre-process the data and provide anonymous authentication.
	[145]	Proposed a fog computing based V2V energy trading architecture in social hotspots.
	[59]	Proposed a carpooling scheme using vehicular fog computing nodes in a blockchain network that supports conditional privacy, destination matching of users, and auditability of data.
	[81]	Fog computing avoids frequent handovers in the network.
	[60]	Proposed a blockchain-based anonymous lightweight authentication mechanism for distributed Vehicular Fog Services (VFS)
	[146]	Proposed a fog computing based secure framework where RSUs for offload tasks to nearby fog vehicles on the basis of reputation scores which are stored in the blockchain
Edge computing	[57]	Used edge server for running DNN based prediction algorithms for evaluating the positioning error
	[65]	Edge computing infrastructure offers extra computing and storage for vehicles in the network.
	[94]	Developed a task offloading mechanism based on edge computing to increase the success probability of block creation.
	[62]	Proposed a system model based on Dynamic Proxy Edge Computing mode in vehicular networks where the vehicles with edge computing and communication capabilities are the proxy vehicles.
	[72]	Incorporates Mobile Edge Computing (MEC) nodes for providing computing resources and to act as managers of local P2P trading system.
	[63]	Edge servers analyse transactions and contribute to partial block creation
	[131]	Vehicular edge computing network
Named Data Networking (NDN)	[53]	NDN solves issues posed by IP-based networks
	[159]	Amalgamation of blokchain and NDN helps in achieving integrity and accountability in the network.
	[18]	NDN facilitates content centric data sharing for IoV. Bottom layer nodes request for service via announcements in the NDN paradigm
Software Defined Networking (SDN)	[79]	Framework is based on an area control plane, programmable by SDN mechanisms.
	[81]	SDN guarantees that the control processes are adequately accomplished in the vehicular network
Directed Acyclic Graphs (DAG)	[52]	Used for efficient data sharing in IoV and quality verification based on reputation in IoV
	[160]	DAG data structure stores and validates transactions in the network
	[161]	Approach based on DAG improves the security and authenticity of the proposed energy management scheme
	[54]	DAG based blockchains have high throughput
Cognitive Radio Technology	[162]	Use Cognitive Radio technology to solve the problem of spectrum storage in vehicular systems.
	[110]	Framework provides security to IoV during spectrum sensing and data transmission with the help of a Cognitive Radio Network
AI - Deep Neural networks (DNN)	[57]	Used DNN-based prediction algorithm for evaluating the positioning error
	[16]	DNN algorithm used for accurate vehicle positioning
AI - Deep Reinforcement Learning (DRL)	[56]	Used DRL for modelling the lane changing problem of autonomous vehicles.
	[52]	Used an asynchronous federated learning scheme. DRL is used for selection of nodes.
	[19]	Used a DRL based smart contract scheme for pricing based on supply-demand during the resource sharing process.
	[131]	DRL integrated into a permissioned blockchain for secure and intelligent content sharing in the vehicular network.
AI - Dueling Deep Q-Learning (DDQL) approach	[79]	A novel DDQL with prioritized replay approach used to solve optimization problems in vehicular networks (which is modelled as a Markov decision process).
AI - Federated Learning	[56]	Used DRL for modelling the lane changing problem of autonomous vehicles.
	[144]	A multilevel federated learning algorithm is used to satisfy the distributed pattern and privacy requirements of IoVs.
Differential Privacy	[163]	Integrated blockchain with differential privacy to alleviate privacy concerns in intelligent transportation systems.

5G	[81]	Analyzes the SDN based blockchain network for effective operation of the VANET systems, especially in 5G and fog computing paradigms.
UAVs	[140]	UAV assisted aerial to ground framework providing secure and efficient data transmission in areas affected by a natural disaster.
PUF	[98]	PUFs provide a unique fingerprint to identify each vehicle and build a trust management system.
Wireless Link Fingerprints	[108]	Used wireless finger prints for encryption.

B.远距离*边缘计算*。随着海量数据的生成

边缘计算是在 IoV 网络中运行的云计算的扩展，传输大量数据使云服务更接近边缘，传感器远距离处理并返回结果收集数据。这在处理速度方面是有利的，但低延迟也是不可行的。由于不需要传输数据而在区块链上运行的共识算法和去中心化计算量也很大，并且

在其区块链架构中利用边缘计算的解决方案可以减轻 IoV 中车辆的计算负载。在车载网络的情况下，大部分处理工作可以委托给边缘节点或 RSU。移动边缘计算（MEC）架构[168]因此受到了一些关注。由于 RSU 也可以是矿工，因此区块链网络的稳健性也得到了提高。为了确保最佳服务质量 (QoS)，必须在性能和隐私要求之间进行适当的权衡。[157] 的作者提出了一种基于假名的隐私保护方案，用于维护位置隐私，特别是在基于雾计算的 IoV 网络中。路线共享是车联网网络的另一个重要方面——用户可以实时上传他们的路线信息以提供各种服务，包括队列和交通预测。[158] 的作者提出了一种隐私保护路由共享服务模型，其中雾节点对数据进行预处理并提供匿名身份验证。

C. CCN/NDN/ICN

以内容为中心的网络 (CCN)，也称为命名数据网络 (NDN) 或以信息为中心的网络 (ICN)，是一种更强调内容而不是连接的数据通信范式 [169]。它用请求-回复模型 [170]取代了互联网协议的端到端连接模型。与 TCP/IP 不同，数据交换不需要节点的地址。这种方法导致有效的记录广播以及区块链网络中的分类帐同步。没有全节点和轻节点的概念，消除了轻节点完全依赖全节点检索和返回数据的安全漏洞[171]。模拟已经证明，这种范式显着提高了网络性能[172]。于*等人*。[173] 提出了一种基于布隆过滤器的称为布隆过滤器路由的 NDN 路由协议（这些是概率数据结构，可以有效地传达关于查询元素的两件事之一——它可能是集合的一部分，也可能不是）。由于它特别适用于 IoV，因此最近对这项技术产生了很多兴趣。它们已被用于 [18]、[53]、[159] 等研究，以在车辆网络中实现高度的完整性和问责制。

D. 软件定义网络 (SDN)

SDN 是一种相对较新的技术，有助于在通信网络中进行有效的网络管理。传统数据网络由于数据和控制平面耦合在一起的复杂性质，在扩展和更新方面面临许多问题。SDN 是一种可编程网络，通过解耦控制和数据平面来降低网络复杂性。它从节点中移除控制功能并将它们转换为简单的数据包/数据转发节点。这对于像 VANET 这样易变的网络有很多好处。然而，控制平面和数据平面的分离也扩大了攻击面，而区块链是解决该问题的可行解决方案。薛*等人*。[174] 对如何使用区块链解决 SDN 网络的现有问题进行了深入研究。一个称为 SDN 控制器的外部实体负责控制网络事务[81]。很少有研究将 SDN 与区块链一起使用以使其框架更加健壮和高效。例如，在 [79] 中，作者提出了一种新颖的基于区块链的分布式软件定义 VANET 框架（Block-SDV），该框架基于源自 SDN 的可编程区域控制平面。此外，在 [81] 中，Gao *等人*。为雾计算和 5G 网络设计了一个基于区块链、支持 SDN 的 IoV 环境，该环境使用 SDN 来保证控制过程在车载网络中充分完成。查莫拉*等人*。[175]提出了一个使用 SDN 来管理资源共享的小云任务卸载框架。

E. 有向无环图 (DAG)

DAG 是一个图，包括变量（称为节点）和节点之间的箭头（称为有向边）[160]。它们的排列方式是不可能从一个节点开始，沿着箭头方向的有向边，并在一个开始的同一节点上着陆，即它本质上是非循环的[176]。在 [161] 中讨论了基于 DAG 的区块链，如 Nano [177]、Byteball [178] 和 IOTA [179] 能够以并行方式处理事务，这与基于链的区块链中的传统顺序方式不同。这增加了区块链的吞吐量，因为基于链的区块链可以一次按顺序处理一个块，而基于 DAG 的区块链可以同时处理多个块 [54]。许多研究提出了同时使用区块链和 DAG 的安全框架。在 [52] 中，作者开发了一种由许可区块链和本地 DAG 组成的区块链架构，以增强他们提出的在 IoV 环境中安全数据共享框架的安全性和可靠性。在 [160] 中，哈西娅*等*。使用 DAG 数据结构在他们提出的 V2V 通信框架中存储和验证交易。龚*等人*。[161] 使用基于 DAG 的方法来提高他们提出的智能混合微电网能源管理方案的安全性和真实性。杨*等人*。使用基于

DAG 的区块链来确保他们提出的车载社交网络 (VSN) [54] 框架的高吞吐量。

F. 认知无线电

认知无线电网络 (CRN) 是一种环境感知无线通信系统，其运行主要有两个目标：

一世。随时随地确保非常可靠的通信。ii. 有效利用可用的网络频谱。

它已被研究人员主要用于在其框架中实现高效的频谱共享和存储。区块链用于在网络内的记录共享过程中轻松提供安全性和透明度。拉蒂 *等人*。在他们提出的框架中使用 CRN 在频谱感知和信息传输期间为支持区块链的 IoV 网络提供安全性 [110]。在 [162] 中，Nadeem *等人*。使用认知无线电技术解决车载系统中的频谱存储问题。

G. 人工智能 (AI)

人工智能技术已广泛用于许多基于区块链的车辆网络方案，以实现各种数据和计算密集型实用程序。例如，深度神经网络（DNN）已被用于评估 [57] 中的定位误差和 [16] 中的精确车辆定位。深度强化学习 (DRL) 已被用于许多研究，例如自动驾驶汽车的变道问题建模 [56]、节点选择 [52]、资源共享期间的供需匹配 [19]，以及实现智能和安全内容共享机制[131]。Dueling Deep Q-Learning (DDQL) 已在 [79] 中用于解决优化问题，联邦学习已在 [56] 中用于建模车道变换问题，在 [144] 中用于满足 IoV 网络的隐私要求。总之，

H. 差分隐私

在差分隐私中，在查询评估之前向数据中添加了一些噪声[163]。差分隐私的概念已被用于物联网数据等各个领域，因为它确保了个人隐私，并且任何单个记录的添加/删除都不会影响最终输出。[180] 的作者总结了在车载网络中使用差分隐私的几个框架。当区块链和差分隐私这两个概念融合在一起时，即使在公共查询评估中也可以缓解安全问题。[163] 的作者提供了关于将差分隐私与区块链集成以解决安全问题的技术信息，并进一步展示了智能交通系统如何使用这样的框架。

一、其他

很少有框架将其他新兴技术用于其基于区块链的车辆网络，如下所示。

i. 无人机：苏 *等人*。提出了一种无人机辅助的空对地车辆框架，用于在受灾地区进行数据传输[140]。
ii. 物理不可克隆功能 (PUF)：PUF 根据电子设备中存在的过程变化为电子设备分配唯一 ID。该 ID 可用于实现快速和安全的身份验证和识别 [181]。Javaid *等人*。使用 PUFs 在他们提出的基于区块链的车辆网络框架中建立信任 [98]。
iii. 无线链路指纹：已被 Kamal *等人使用*。[108] 其中，正在相互通信的两辆车的信道特性会产生唯一的链路。如果通信车辆的接收功率变化
是相关的，这意味着没有对手影响通信链路。
iv. 5G：5G 可确保车载网络所需的超高速通信。高等 *人*。探索 5G 和雾计算范式中 VANET 系统的区块链和 SDN 组合[81]。

摘要： 本节讨论了最近用于保护车辆网络的一些技术。这里提到的框架使用最先进的技术，如云计算、雾计算、边缘计算、NDN、SDN、DAG、DNN、DRL、DDQL、认知无线电、联邦学习、差分隐私、5G 等。和 VANET 网络出于安全原因。

八。主要挑战,学习 经验和未来研究 方向_ _ _ _ _

在本节中，我们将讨论在实施基于区块链的应用程序以保护车辆网络时面临的主要挑战以及解决这些问题的潜在未来研究方向。

A. 可扩展性

吞吐量，或每秒验证的交易数量，是区块链系统可扩展性的量化指标。比特币的吞吐量为每秒 7 笔交易——相比之下，VISA 的交易吞吐量为每秒 2,000 笔交易[182]。通常，通过对算法本身进行适当的修改，可以在更高的规模上提高较低的吞吐量，例如在 [98] 中。车载网络将产生大量数据，并且由于对延迟至关重要的环境，区块链必须扩展到非常高的标准。许多现有的标准和协议是为加密货币应用程序开发的，它们对时间不敏感。通过选择适当的共识算法和区块链平台可以提高性能。例如，与 PoS 和 PBFT 相比，DPoS 和 DBFT 分别显着提高了交易吞吐量。已经有一些专门整合车联网和区块链共识的研究。在 [114] 中，作者为基于区块链的 IoV 应用程序提出了增强的 DPoS 共识。胡 *等*。[24] 提出了一种特定于 IoV 的拜占庭共识算法进行身份验证。联盟和私有区块链也比无许可区块链更有效，因为验证节点的数量更少。在这种情况下，必须仔细考虑去中心化和吞吐量之间的权衡，因为联盟和私有区块链比无许可区块链更集中。与可扩展性相关的另一个问题是多个传感器和设备的无缝集成。随着 IoV 网络变得越来越大，将使用不同的传感器和平台。确保它们无缝协作将是一项挑战。

B. 隐私

当车载节点用于边缘计算时，诸如行驶路线、卡片信息等敏感信息会被卸载用于各种任务[183]。为了防止不受欢迎的人访问此类信息，可以对信息进行加密。但是，密文

使分析过程非常耗时。保护隐私的区块链框架需要加速边缘计算中的查询过程。

由于数据的敏感性，需要确保用户隐私，同时还允许透明度以符合通用数据保护条例 (GDPR) [9] 等法律要求。分布式账本需要加密和免费访问控制技术来平衡隐私和透明度。

C. 量子计算攻击

量子计算是一个研究领域，将在未来几年具有广泛的适用性[184]。区块链严重依赖其加密散列技术的单向属性。随着量子计算的出现，这些技术可能不像现在那样安全。量子计算机提供了截然不同的计算能力。一些量子计算机可以轻松克服整个普通区块链节点网络的计算能力[185]。哈利法*等人*。[186] 说明了量子计算机如何使用 Grover 算法和 Shor 算法攻击权益证明区块链，并推荐量子弹性签名方案来缓解它们。车联网网络需要抗量子，否则，它们容易受到 51% 的影响和拜占庭式攻击[187]。为了使用量子计算机攻击 IoV 网络，其目的是影响网络的一部分，而不仅仅是单个节点。这可能会导致对区块链网络失去信任。量子攻击是一个活跃的研究领域，并且提出了许多其他解决方案[188]，[189]，但是，必须结合这些技术来制造商业上可行的系统。

D. 原型设计和仿真

被设计为去中心化系统的区块链对原型设计和模拟提出了自然挑战。几个大型效果无法在原型上充分建模。现有的研究工作以小规模模型模拟细节的形式展示了他们的发现，其中许多使用了现有的最佳技术，但是，它们并不能准确地反映几个不可预见的挑战。例如，即使使用随机机制，也很难准确地模拟车辆网络拓扑中固有的随机性。因此，研究界将通过开发更好的模拟工具和原型测试框架得到很好的帮助[33]。

E. 对区块链的攻击

区块链系统的独特性使其容易遭受传统集中式系统中不涉及的几种攻击——包括但不限于 51% 攻击、自私挖矿、日蚀攻击、DNS 攻击和加密劫持 [190]。尽管支持区块链的车辆边缘计算提供了去中心化和透明度等好处，但它容易受到多种攻击[183]。如果网络中大量成员遭到破坏，网络可能会被劫持，交易可能会被伪造。攻击的发生是由于许可区块链网络中使用的轻量级共识协议。因此，在车载边缘计算网络中部署不同类型的链需要一个可扩展且有弹性的共识协议。

九。结论_

在本次调查中，我们深入分析了几个基于区块链的车载网络安全框架，并从三个不同的角度对它们进行了分类，即应用视角、安全视角和区块链视角。从应用角度，我们根据数据交易/共享、资源共享、停车、交通管理等不同的应用场景对框架进行分类。从安全角度，我们根据它们所防御的安全攻击，他们满足的网络安全要求、他们使用的身份验证技术以及他们使用的安全证明。从区块链的角度来看，我们根据他们使用的区块链类型、他们使用的区块链平台的类型对不同的框架进行分类，以及他们方案中使用的共识算法。我们还讨论了用于模拟和测试这些基于区块链的框架的各种模拟工具/平台。此外，大多数基于区块链的安全框架与区块链一起在其方案中采用其他新兴技术来满足低延迟、低计算、数据存储等要求。因此，分析这些框架并讨论这些其他最先进技术在保护这些网络中的作用非常重要。最后，基于调查，我们列出了该领域的主要挑战和未来的研究方向。该调查将作为研究人员和专业人士的指南，这些研究人员和专业人士冒险研究和开发基于区块链的安全解决方案，用于车联网和 VANET 等车辆网络。

参考文献

[1] PK 萨胡，EH-K。Wu、J. Sahoo 和 M. Gerla，“BAHG：VANET 城市环境的骨干辅助跳跃贪婪路由”，*IEEE Trans。英特尔。反式。系统。*，卷。14，没有。1，第 199-213 页，2013 年 3 月。

[2] A.-SK Pathan，*自组织网络的安全性：MANET、WSN、WMN、VANET*。美国佛罗里达州博卡拉顿：CRC Press，2016 年 4 月。

[3] MA Elsadig 和 YA Fadlalla，“VANETs 安全问题和挑战：一项调查”，*Indian J. Sci。技术。*，卷。9，没有。28，第 1-8 页，2016 年 7 月。

[4] A. Mehra、M. Mandal、P. Narang 和 V. Chamola，“ReViewNet：一种快速且资源优化的网络，用于在朦胧天气条件下实现安全自动驾驶”，*IEEE Trans。英特尔。反式。系统。*，卷。22，没有。7，第 4256-4266 页，2021 年 7 月。

[5] “全球卫生观察站 (GHO) 数据”。2020. [在线]。可用：https://www.who.int/gho/road_safety/mortality/en/（访问时间：2020 年 3 月 14 日）。

[6] T. Alladi、V. Chamola、B. Sikdar 和 K.-KR Choo，“消费者物联网：安全漏洞案例研究和解决方案”，*IEEE Consum。电子。麦格。*，卷。9，没有。2，页。3 月 17 日至 25 日，2020 年。

[7] T. Alladi、V. Chamola 和 S. Zeadally，“工业控制系统：网络攻击趋势和对策”，*计算机。交流。*，卷。155，第 1-8 页，2020 年 4 月。

[8] T. Alladi、S. Chakravarty、V. Chamola 和 M. Guizani，“车联网场景中运输车辆的轻量级身份验证和证明方案”，*IEEE Trans。车。技术。*，卷。69，没有。12，第 14188-14197 页，2020 年 12 月。

[9] G. Baldini、JL Hernandez-Ramos、G. Steri、R. Neisse 和 IN Fovino，“分布式账本在公路运输发展中的应用综述”，*IEEE 互联网计算。*，卷。24，没有。6，第 27-36 页，11 月/12 月。2020 年。

[10] J. Bao、D. He、M. Luo 和 K.-KR Choo，“能源领域区块链应用调查”，*IEEE Syst。J.*，卷。15，没有。3，第 3370-3381 页，2021 年 9 月。

[11] J.谢*等人*。，“应用于智慧城市的区块链技术调查：研究问题和挑战”，*IEEE Commun。调查图。*，卷。21，没有。3，第 2794-2830 页，2019 年第 3 季度。

[12] MB Mollah *等人*。，“面向智能交通系统的车联网区块链：一项调查”，2020 年 10 月，*arXiv:2007.06022*。

[13] TA Butt、R. Iqbal、K. Salah、M. Aloqaily 和 Y. Jararweh，“社交车联网中的隐私管理：回顾、挑战和基于区块链的解决方案”，*IEEE Access*，第一卷。7，第 79694-79713 页，2019 年。

[14] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian 和 N. Zhang，“能源区块链智能社区电动汽车的安全充电方案”，*IEEE Internet Things J.*，第一卷。6，没有。3，第 4601-4613 页，2019 年 6 月。

[15] Z. Zhou、B. Wang、Y. Guo 和 Y. Zhang，“区块链和计算智能激发了电动汽车互联网中激励兼容的需求响应”，*IEEE Trans。出现。主题计算。英特尔。*，卷。3，没有。3，第 205-216 页，2019 年 6 月。

[16] Y. Song, Y. Fu, FR Yu, and L. Zhou，“协同定位的区块链车联网：一种深度神经网络方法”，*IEEE Internet Things J.*，第一卷。7，没有。4，第 3485-3498 页，2020 年 4 月。

[17] K. Liu、W. Chen、Z. Zheng、Z. Li 和 W. Liang，“车联网中基于区块链的数据交易的新型债务信用机制”，*IEEE Internet Things J.*，卷。6，没有。5，第 9098-9111 页，2019 年 10 月。

[18] C. Chen、J. Wu、H. Lin、W. Chen 和 Z. Zheng，“一种安全高效的基于区块链的车联网数据交易方法”，*IEEE Trans。车。技术。*，卷。68，没有。9，第 9110-9121 页，2019 年 9 月。

[19] H. Chai、S. Leng、K. Zhang 和 S. Mao，“基于信誉证明的联盟区块链用于车联网中的信任资源共享”，*IEEE Access*，第一卷。7，第 175744-175757 页，2019 年。

[20] J. Fan, R. Li, and S. Li，“任务调度策略研究：基于车载云计算环境中的智能合约”，*Proc. 第一届 IEEE 诠释。会议。热信息。中心网络 (HotICN)*，2018 年 8 月，第 248-249 页。

[21] X. Wang、P. Zeng、N. Patterson、F. Jiang 和 R. Doss，“基于区块链技术的车联网改进认证方案”，*IEEE Access*，第一卷。7，第 45061-45072 页，2019 年。

[22] Z. Lu、Q. Wang、G. Qu、H. Zhang 和 Z. Liu，“用于 VANETs 的基于区块链的隐私保护认证方案”，*IEEE Trans。超大规模积分。(VLSI) 系统。*，卷。27，没有。12，第 2792-2801 页，2019 年 12 月。

[23] D. Zheng、C. Jing、R. Guo、S. Gao 和 L. Wang，“基于区块链的可追溯访问认证系统，在 VANETs 中具有隐私保护”，*IEEE Access*，第一卷。7，第 117716-117726 页，2019 年。

[24] W. Hu, Y. Hu, W. Yao, and H. Li，“基于区块链的车联网信息认证拜占庭共识算法”，*IEEE Access*，第一卷。7，第 139703-139711 页，2019 年。

[25] L. Cheng *等人。*，“Sctsc：车联网中基于属性的区块链的半集中式交通信号控制模式”，*IEEE Trans。计算。社会党。系统。*，卷。6，没有。6，第 1373-1385 页，2019 年 12 月。

[26] C. Chen、T. Xiao、T. Qiu、N. Lv 和 Q. Pei，“区块链城市车联网中基于智能合约的经济队列”，*IEEE Trans. 工业信息。*，卷。16，没有。6，第 4122-4133 页，2010 年 6 月。

[27] MM Zanjireh 和 H. Larijani，“关于 WSN 的集中式和分布式集群路由算法的调查”，*Proc。IEEE 81 号车辆。技术。会议。(VTC Spring)*，2015 年 5 月，第 1-6 页。

[28] F. Yang、S. Wang、J. Li、Z. Liu 和 Q. Sun，“车联网概述”，*中国通讯。*，卷。11，没有。10，第 1-15 页，2014 年 10 月。

[29] C. Olaverri-Monreal、P. Gomes、R. Fernandes、F. Vieira 和 M. Ferreira，“透视系统：支持 VANET 的超车操作助手”，*Proc。IEEE 英特尔。车。症状。*，2010 年 6 月，第 123-128 页。

[30] J. Lin, S.-C. 陈，Y.-T。施和 S.-H。陈，“融合 OBD、GPS、3G 技术的车辆远程在线诊断系统研究”，*World Acad。科学。英。技术。*，卷。56，第 435-441 页，2009 年 8 月。

[31] U. Lee、B. Zhou、M. Gerla、E. Magistretti、P. Bellavista 和 A. Corradi，“Mobeyes：使用车载传感器网络进行城市监控的智能暴民”，*IEEE 无线通信。*，卷。13，没有。5，第 52-57 页，2006 年 10 月。

[32] A. Tapscott 和 D. Tapscott，“区块链如何改变金融”，*哈佛巴士。牧师*，卷。1，没有。9，第 2-5 页，2017 年 3 月。

[33] T. Alladi、V. Chamola、N. Sahu 和 M. Guizani，“区块链在无人机中的应用：综述”，*Veh。交流。*，卷。2020 年 6 月 23 日，艺术。不。100249。

[34] TM Fernandez-Caramés、O. Blanco-Novoa、M. Suárez-Albela 和 P. Fraga-Lamas，“用于工业 4.0 库存和可追溯性应用的基于无人机和区块链的系统”，*Multidiscipl。数字。出版。研究所。过程。*，卷。4，没有。1，第 26，

[35] A. Kapitonov、S. Lonshakov、A. Krupenkin 和 I. Berman，“由无人机组成的多智能体系统的基于区块链的自主业务活动协议”，*Proc。车间水库。教育。开发。无人机系统 (RED-UAS)*，2017 年 10 月，第 84-89 页。

[36] K. Lei、Q. Zhang、J. Lou、B. Bai 和 K. Xu，“使用区块链保护基于 ICN 的无人机自组织网络”，*IEEE Commun。麦格。*，卷。57，没有。6，第 26-32 页，2019 年 6 月。

[37] A. Dorri、SS Kanhere 和 R. Jurdak，“迈向物联网优化区块链”，*Proc。IEEE/ACM 2nd Int。会议。互联网事物设计 实施。(IoTDI)*，2017 年 4 月，第 173-178 页。

[38] O. Novo，“区块链遇到物联网：物联网中可扩展访问管理的架构”，*IEEE Internet Things J.*，第一卷。5，没有。2，第 1184-1195 页，2018 年 4 月。

[39] A. Panarello、N. Tapas、G. Merlino、F. Longo 和 A. Puliafito，“区块链和物联网集成：系统调查”，*传感器*，卷。18，没有。第 8 页 2575 年 8 月 2018 年。

[40] T. Alladi、V. Chamola、JJPC Rodrigues 和 SA Kozlov，“智能电网中的区块链：不同用例的回顾”，*传感器*，卷。19，没有。第 22 页，第 4862，2019 年 11 月。

[41] K. Biswas 和 V. Muthukkumarasamy，“使用区块链技术保护智能城市”，*Proc。IEEE 第 18 届国际会议。会议。高性能。计算。交流。IEEE 第 14 届国际会议。会议。智能城市 IEEE 2nd Int。会议。数据科学。系统。(HPCC/SmartCity/DSS)*，2016 年 12 月，第 1392–1393 页。

[42] J. Sun、J. Yan 和 KZK Zhang，“基于区块链的共享服务：区块链技术可以为智慧城市做出哪些贡献”，*Financ。创新。*，卷。2，没有。1，第 1-9 页，2016 年 12 月。

[43] Y. Tribis、A. El Bouchti 和 H. Bouayad，“基于区块链的供应链管理：系统映射研究”，*Proc。MATEC 网络会议* , 卷。200, 2018, p. 20.

[44] B. Leiding、P. Memarmoshrefi 和 D. Hogrefe，“自我管理和基于区块链的车辆自组织网络”，*Proc。ACM 诠释 联合会议 普适计算。附件*，2016 年 9 月，第 137-140 页。

[45] Z. Lu、Q. Wang、G. Qu 和 Z. Liu，“BARS：基于区块链的匿名信誉系统，用于 VANET 中的信任管理”，*Proc。第 17 届 IEEE 诠释。会议。信任安全隐私计算。Commun./12th IEEE Int. 会议。大数据科学。英。(TrustCom/BigDataSE)*，2018 年 8 月，第 98-103 页。

[46] S. Nakamoto，“比特币：点对点电子现金系统”，*分散式总线。牧师*，2008 年，艺术。不。21260。

[47] M. Pilkington，“区块链技术：原理和应用”，*数字化转型研究手册*。英国切尔滕纳姆：Edward Elgar 出版社，2016 年 9 月。

[48] D. Johnson、A. Menezes 和 S. Vanstone，“椭圆曲线数字签名算法 (ECDSA)”，*诠释。J.Inf。安全*，第一卷。1，没有。1，第 36-63 页，2001 年 8 月。

[49] N.萨博。“智能合约的理念。”1997. [在线]。可用：https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contract_idea.html

[50] B. Chen、D. He、N. Kumar、H. Wang 和 K.-KR Choo，“用于车辆通信系统的基于区块链的代理重新加密和相等性测试”，*IEEE Trans。网络。科学。英。*，卷。8，没有。3，第 2048-2059 页，7 月至 9 月。2021 年。

[51] B. Chen、L. Wu、H. Wang、L. Zhou 和 D. He，“一种基于区块链的可搜索公钥加密，用于云辅助车辆社交网络的前向和后向隐

私，" *IEEE Trans。车。技术。*, 卷。69，没有。6，第 5813-5825 页，2020 年 6 月。

[52] Y. Lu、X. Huang、K. Zhang、S. Maharjan 和 Y. Zhang，"区块链赋能异步联邦学习以实现车联网中的安全数据共享"，*IEEE Trans。车。技术。*, 卷。69，没有。4，第 4298-4311 页，2020 年 4 月。

[53] F. Ahmad、CA Kerrache、F. Kurugollu 和 R. Hussain，"在基于命名数据网络的车联网中实现区块链"，*IT 教授*，第一卷。21，没有。4，第 41-47 页，7 月/8 月。2019 年。

[54] W. Yang、X. Dai、J. Xiao 和 H. Jin，"LDV：用于车辆社交网络的基于 DAG 的轻量级区块链"，*IEEE Trans。车。技术。*, 卷。69，没有。6，第 5749-5759 页，2020 年 6 月。

[55] M. Baza、N. Lasla、MMEA Mahmoud、G. Srivastava 和 M. Abdallah，"B-ride：在公共区块链上实现隐私保护、信任和公平支付的乘车共享"，*IEEE Trans。网络。科学。英。*, 卷。8，没有。2，第 1214-1229 页，4 月至 6 月。2021 年。

[56] Y. Fu, C. Li, FR Yu, TH Luan, and Y. Zhang，"车载区块链辅助知识积累和转移的自主换道系统"，*IEEE Internet Things J.*, vol. 7，没有。11，第 11123-11136 页，2020 年 11 月。

[57] C. Li、Y. Fu、FR Yu、TH Luan 和 Y. Zhang，"车辆位置校正：基于车辆区块链网络的 GPS 错误共享框架"，*IEEE Trans。英特尔。反式。系统。*, 卷。22，没有。2，第 898-912 页，2021 年 2 月。

[58] C.张*等人*。, "BSFP：具有公平性、可靠性和隐私保护的区块链智能停车"，*IEEE Trans. 车。技术。*, 卷。69，没有。6，第 6578-6591 页，2020 年 6 月。

[59] M. Li、L. Zhu 和 X. Lin，"使用区块链辅助车辆雾计算实现高效且保护隐私的拼车"，*IEEE Internet Things J.*，卷。6，没有。3，第 4573-4584 页，2019 年 6 月。

[60] Y. Yao、X. Chang、J. Mišic、VB Miši′ c 和 L. Li，"BLA：区块链-′辅助分布式车载雾服务的轻量级匿名身份验证"，*IEEE Internet Things J.*，第一卷。6，没有。2，第 3775-3784 页，2019 年 4 月。

[61] C. Lin、D. He、X. Huang、N. Kumar 和 K.-KR Choo，"BCPPA：一种基于区块链的有条件保护隐私的车载网络认证协议"，*IEEE Trans。英特尔。反式。系统。*, 卷。22，没有。12，第 7408-7420 页，2021 年 12 月。

[62] H. Liu、P. Zhang、G. Pu、T. Yang、S. Maharjan 和 Y. Zhang，"区块链在车辆边缘计算中赋予协作身份验证和数据可追溯性，" *IEEE Trans。车。技术。*, 卷。69，没有。4，第 4221-4232 页，2020 年 4 月。

[63] A. Vangala、B. Bera、S. Saha、AK Das、N. Kumar 和 YH Park，"基于区块链的证书认证，用于智能交通系统中的车辆事故检测和通知，" *IEEE Sensors J.*，第一卷。21，没有。14，第 15824-15838 页，2021 年 7 月。

[64] H. Shen、J. Zhou、Z. Cao、X. Dong 和 K.-KR Choo，"基于区块链的轻量级证书颁发机构，用于车载社交网络中基于位置的高效隐私保护服务"，*IEEE Internet Things J* . , 卷。7，没有。7，第 6610-6622 页，2020 年 7 月。

[65] H. Tan 和 I. Chung，"VANET 中区块链的安全认证和密钥管理"，*IEEE Access*，第一卷。8，第 2482-2498 页，2019 年。

[66] Y. Li 和 B. Hu，"使用联盟区块链的电动汽车迭代两层优化充放电交易方案"，*IEEE Trans。智能电网*，第一卷。11，没有。3，第 2627-2637 页，2020 年 5 月。

[67] Y. Wang、Z. Su 和 N. Zhang，"BSIS：基于区块链的车载能源网络能源输送安全激励方案"，*IEEE Trans。工业信息。*, 卷。15，没有。6，第 3620-3631 页，2019 年 6 月。

[68] Y. Li 和 B. Hu，"联盟区块链支持的安全和隐私保护的电动汽车优化充电和放电交易方案"，*IEEE Trans。工业信息。*, 卷。17，没有。3，第 1968-1977 页，2021 年 3 月。

[69] H. Li、D. Han 和 M. Tang，"使用区块链和雾计算的电动汽车隐私保护充电方案"，*IEEE Syst。J.*，卷。15，没有。3，第 3189-3200 页，2021 年 9 月。

[70] H. Wang、Q. Wang、D. He、Q. Li 和 Z. Liu，"Bbars：基于区块链的 V2G 网络匿名奖励方案"，*IEEE Internet Things J.*，卷。6，没有。2，第 3676-3687 页，2019 年 4 月。

[71] GS Aujia、A. Singh、M. Singh、S. Sharma、N. Kumar 和 K.-KR Choo，"阻塞：边缘设想的 V2X 环境中基于区块链的安全数据处理框架"，*IEEE Trans。车。技术。*, 卷。69，没有。6，第 5850-5863 页，2020 年 6 月。

[72] X. Lin、J. Wu、S. Mumtaz、S. Garg、J. Li 和 M. Guizani，"车联网辅助智慧城市中基于区块链的按需计算资源交易"，*IEEE Trans。出现。主题计算。*, 卷。9，没有。3，第 1373-1385 页，7 月至 9 月。2021 年。

[73] S. Wang、D. Ye、X. Huang、R. Yu、Y. Wang 和 Y. Zhang，"用于车辆边缘计算中安全资源共享的联盟区块链：基于合同的方法"，*IEEE Trans。网络。科学。英。*, 卷。8，没有。2，第 1189-1201 页，4 月至 6 月。2021 年。

[74] X. Huang、D. Ye、R. Yu 和 L. Shu，"使用区块链和最优智能合约设计保护停放车辆辅助雾计算"，*IEEE/CAA J. Autom。中文*, 第一卷。7，没有。2，第 426-441 页，2020 年 3 月。

[75] Y. Yao、X. Chang、J. Mišic 和 VB Miši′ c，"车辆云计算中的轻量级和隐私保护 ID 即服务配置"，*IEEE Trans。车。技术。*, 卷。69，没有。2，第 2185-2194 页，2020 年 2 月。

[76] J. Wang, X. Feng, T. Xu, H. Ning, and T. Qiu，"基于区块链的车辆团队合作非确定性人群感知策略模型"，*IEEE Internet Things J.*，第一卷。7，没有。9，第 8090-8098 页，2020 年 9 月。

[77] C. Lai、M. Zhang、J. Cao 和 D. Zheng，"SPIR：用于可靠实时地图更新的安全和隐私保护激励方案"，*IEEE Internet Things J.*，第一卷。7，没有。1，第 416-428 页，2020 年 1 月。

[78] J. Zhang、F. Yang、Z. Ma、Z. Wang、X. Liu 和 J. Ma，"车联网的分散位置隐私保护空间众包"，*IEEE Trans。英特尔。反式。系统。*, 卷。22，没有。4，第 2299-2313 页，2021 年 4 月。

[79] L.张*等人*。, "基于区块链的车联网安全数据共享系统：立场文件"，*Veh。交流。*, 卷。16，第 85-93 页，2019 年 4 月。

[80] V. Sharma，"支持区块链的车联网 (IoV) 的节能交易模型"，*IEEE Commun。莱特。*, 卷。23，没有。2，第 246-249 页，2019 年 2 月。

[81] J.高等*人*。，"用于雾计算和 5G 网络的基于区块链 SDN 的车联网环境"，*IEEE Internet Things J.*，第一卷。7，没有。5，第 4278-4291 页，2020 年 5 月。

[82] F. Jameel、MA Javed、S. Zeadally 和 R. Jäntti，"基于区块链的蜂窝 V2X 通信的高效挖掘集群选择"，*IEEE Trans。英特尔。反式。系统。*, 卷。22，没有。7，第 4064-4072 页，2021 年 7 月。

[83] A. Lei、H. Cruickshank、Y. Cao、P. Asuquo、CPA Ogah 和 Z. Sun，"异构智能交通系统的基于区块链的动态密钥管理"，*IEEE Internet Things J.*，第一卷。4，没有。6，第 1832-1843 页，2017 年 12 月。

[84] V. Hassija、V. Gupta、S. Garg 和 V. Chamola，"基于区块链和深度神经网络的交通拥堵概率估计"，*IEEE Trans。英特尔。反式。系统。*, 卷。22，没有。7，第 3919-3928 页，2021 年 7 月。

[85] V. Chamola、A. Sancheti、S. Chakravarty、N. Kumar 和 M. Guizani，"基于物联网和边缘计算的 V2G 系统充电调度和电动汽车选择框架"，*IEEE Trans。车。技术。*, 卷。69，没有。10，第 10569-10580 页，2020 年 10 月。

[86] V. Hassija、V. Saxena、V. Chamola 和 FR Yu，"基于虚拟投票和自适应定价算法的停车位分配框架"，*IEEE Trans。车。技术。*, 卷。69，没有。6，第 5945-5957 页，2020 年 6 月。

[87] A. Miglani、N. Kumar、V. Chamola 和 S. Zeadally，"能源管理互联网区块链：回顾、解决方案和挑战"，*Comput。交流。*, 卷。151，第 395-418 页，2020 年 2 月。

[88] V. Hassija、V. Chamola、S. Garg、DNG Krishna、G. Kaddoum 和 DNK Jayakody，"基于区块链的 V2G 网络中轻量级数据共享和能源交易框架"，*IEEE Trans。车。技术。*, 卷。69，没有。6，第 5799-5812 页，2020 年 6 月。

[89] L. Shi、Y. Li、T. Liu、J. Liu、B. Shan 和 H. Chen，“基于区块链的动态分布式蜜罐”，*IEEE Access*，第一卷。7，第 72234-72246 页，2019 年。

[90] J. Kang、R. Yu、X. Huang、S. Maharjan、Y. Zhang 和 E. Hossain，“使用联盟区块链实现插电式混合动力电动汽车之间的本地化点对点电力交易”，*IEEE Trans。工业信息。*，卷。13，没有。6，第 3154-3164 页，2017 年 12 月。

[91] A. Sheikh、V. Kamuni、A. Urooj、S. Wagh、N. Singh 和 D. Patel，“使用基于拜占庭的区块链共识的安全能源交易”，*IEEE Access*，第一卷。8，第 8554-8571 页，2019 年。

[92] X. Zhang 和 X. Chen，“车载自组织网络中基于联盟区块链的数据安全共享和存储”，*IEEE Access*，第一卷。7，第 58241-58254 页，2019 年。

[93] M. Li, J. Weng, A. Yang, J.-N. Liu 和 X. Lin，“在车载网络中实现基于区块链的公平和匿名广告传播”，*IEEE Trans。车。技术。*，卷。68，没有。11，第 11248-11259 页，2019 年 11 月。

[94] Z. Zhou、B. Wang、M. Dong 和 K. Ota，“网络物理系统中安全高效的车辆到电网能源交易：区块链和边缘计算的集成”，*IEEE Trans。Syst., Man, Cybern., Syst.*，卷。50，没有。1，第 43-57 页，2020 年 1 月。

[95] X. Huang, C. Xu, P. Wang, and H. Liu，“LNSC：基于区块链生态系统的电动汽车和充电桩管理安全模型”，*IEEE Access*，第一卷。6，第 13565-13574 页，2018 年。

[96] H. Liu, Y. Zhang, S. Zheng, and Y. Li，“V2G 网络中基于区块链和智能合约的电动汽车电量交易机制”，*IEEE Access* , vol. 7，第 160546-160558 页，2019 年。

[97] W. Chen、Y. Chen、X. Chen 和 Z. Zheng，“实现 IoV 的安全数据共享：具有链上和链下保证的质量驱动的激励机制”，*IEEE Internet Things J.*，卷。7，没有。3，第 1625-1640 页，2020 年 3 月。

[98] U. Javaid、MN Aman 和 B. Sikdar，“使用区块链驱动车联网信任管理的可扩展协议”，*IEEE Internet Things J.*，第一卷。7，没有。12，第 11815-11829 页，2020 年 12 月。

[99] Q. Feng、D. He、S. Zeadally 和 K. Liang，“BPAS：用于车载自组织网络的区块链辅助隐私保护认证系统”，*IEEE Trans。工业信息。*，卷。16，没有。6，第 4146-4155 页，2020 年 6 月。

[100] MA Ferrag 和 L. Maglaras，“DeepCoin：一种新颖的深度学习和基于区块链的智能电网能源交换框架”，*IEEE Trans。英。管理。*，卷。67，没有。4，第 1285-1297 页，2020 年 11 月。

[101] SS Manvi 和 S. Tangade，“关于 VANET 中用于安全通信的身份验证方案的调查”，*Veh。交流。*，卷。9，第 19-30 页，2017 年 7 月。

[102] M. Raya 和 J.-P。Hubaux，“车载自组织网络的安全性”，在 *Proc。第三届 ACM 研讨会安全 Ad Hoc Sens. Netw。*，2005 年 11 月，第 11-21 页。

[103] M. Raya 和 J.-P。Hubaux，“保护车载自组织网络”，*J. Comput。安全*，第一卷。15，没有。1，第 39-68 页，2007 年 1 月。

[104] L.李*等人*。，“CreditCoin：基于隐私保护的区块链激励公告网络，用于智能车辆通信，”*IEEE Trans. 英特尔。反式。系统。*，卷。19，没有。7，第 2204-2220 页，2018 年 7 月。

[105] K. 张和 H.-A。Jacobsen，“走向可靠、可扩展和普遍使用区块链的分布式账本”，*Proc。ICDCS*，2018 年，第 1337-1346 页。

[106] X. Liu, H. Huang, F. Xiao, and Z. Ma，“一种基于区块链的信任管理与 VANETs 有条件的隐私保护公告方案”，*IEEE Internet Things J.*，第一卷。7，没有。5，第 4101-4112 页，2020 年 5 月。

[107] AK Sutrala、P. Bagga、AK Das、N. Kumar、JJPC Rodrigues 和 P. Lorenz，“关于车联网部署的基于条件隐私保护批量验证的身份验证方案的设计”，*IEEE Trans。车。技术。*，卷。69，没有。5，第 5535-5548 页，2020 年 5 月。

[108] M. Kamal、G. Srivastava 和 M. Tariq，“车联网中基于区块链的轻量级和安全 V2V 通信”，*IEEE Trans。英特尔。反式。系统。*，卷。22，没有。7，第 3997-4004 页，2021 年 7 月。

[109] F. Ahmad、F. Kurugollu、A. Adnane、R. Hussain 和 F. Hussain，“MARINE：互联车辆中的抗中间人攻击信任模型”，*IEEE Internet Things J.*，第一卷. 7，没有。4，第 3310-3322 页，2020 年 4 月。

[110] G. Rathee、F. Ahmad、F. Kurugollu、MA Azad、R. Iqbal 和 M. Imran，“CRT-bIoV：一种用于支持区块链的车联网的认知无线电技术”，*IEEE Trans。英特尔。反式。系统。*，卷。22，没有。7，页。4005–4015，七月。2021 年。

[111] Z. Yang、K. Yang、L. Lei、K. Zheng 和 VCM Leung，“车载网络中基于区块链的去中心化信任管理”，*IEEE Internet Things J.*，第一卷。6，没有。2，第 1495-1505 页，2018 年 4 月。

[112] R. Mishra、A. Singh 和 R. Kumar，“VANET 安全：问题、挑战和解决方案”，*Proc。诠释。会议。电。电子。优化。技术。(ICEEOT)*，2016 年 3 月，第 1050-1055 页。

[113] F. Ahmad、A. Adnane、VNL Franqueira、F. Kurugollu 和 L. Liu，“车载自组织网络中的中间人攻击：评估攻击者策略的影响”，*传感器*，卷。18，没有。第 11 页 4040，2018 年 11 月。

[114] J. Kang、Z. Xiong、D. Niyato、D. Ye、DI Kim 和 J. Zhao，“走向安全的基于区块链的车联网：使用声誉和合同理论优化共识管理”，*IEEE Trans。车。技术。*，卷。68，没有。3，第 2906-2920 页，2019 年 3 月。

[115] JR Douceur，“女巫攻击”，*Proc。诠释。车间点对点系统。*，2002 年 3 月，第 251-260 页。

[116] G. Carl、G. Kesidis、RR Brooks 和 S. Rai，“拒绝服务攻击检测技术”，*IEEE Internet Comput。*，卷。10，没有。1，第 82-89 页，1 月/2 月。2006 年。

[117] A. Chonka、Y. Xiang、W. Zhou 和 A. Bonti，“保护云计算免受 HTTP-DoS 和 XML-DoS 攻击的云安全防御”，*J. Netw。计算。应用程序。*，卷。34，没有。4，第 1097-1107 页，2011 年 7 月。

[118] BB Gupta 和 OP Badve，“云计算环境中 DoS 和 DDoS 攻击的分类和理想的防御机制”，*神经计算。应用程序。*，卷。28，没有。12，第 3655-3682 页，2017 年 12 月。

[119] J. Li、H. Lu 和 M. Guizani，“ACPN：一种新颖的身份验证框架，具有条件隐私保护和 VANET 不可否认性”，*IEEE Trans。并行分布。系统。*，卷。26，没有。4，第 938-948 页，2015 年 4 月。

[120] L. Bighash、KS Alexander、CS Hagen 和 AB Hollingshead，“通信网络中社会窃听的模型”，*诠释。J. 通讯。*，卷。第 14 页 2020 年 6 月 23 日。

[121] MZA Bhuiyan 和 J. Wu，“网络系统中的共谋攻击检测”，*Proc。IEEE 第 14 届国际会议。会议。依靠。自动。安全计算。第十四诠释。会议。无处不在的情报。计算。第二诠释。会议。大数据英特尔。计算。网络科学。技术。大会。(DASC/PiCom/DataCom/CyberSciTech)*，2016 年 8 月，第 286-293 页。

[122] G. Bleumer，“Forgery”，*加密和安全百科全书*，HCA van Tilborg，Ed。美国马萨诸塞州波士顿：Springer，2005 年，第 237–238 页，[在线]。可用：https://doi.org/10.1007/0-387-234837_172，doi：10.1007/0-387-23483-7_172。

[123] T. Alladi、V. Chamola 和 Naren，“HARCI：用于三个实体医疗保健物联网网络的双向身份验证协议”，*IEEE J. Sel。地区交流。*，卷。39，没有。2，第 361-369 页，2021 年 2 月。

[124] D. Welch 和 S. Lathrop，“无线安全威胁分类法”，*Proc。IEEE 系统。人赛博恩。社会信息。保证。研讨会*，2003 年 6 月，第 76-83 页。

[125] Z. Lu、G. Qu 和 Z. Liu，“关于车载网络安全、信任和隐私方面最新进展的调查”，*IEEE Trans。英特尔。反式。系统。*，卷。20，没有。2，第 760-776 页，2019 年 2 月。

[126] R. Falk 和 S. Fries，“基于证书的身份验证方法”，美国专利 9432198，2016 年 8 月 30 日。

[127] J. Camenisch、S. Hohenberger 和 M. Ø。Pedersen，“短签名的批量验证”，*Proc。安努。诠释。会议。理论应用 密码学。技术。*，2007 年 5 月，第 246-263 页。

[128] PPC Lee、JCS Lui 和 DKY Yau，“动态对等组的分布式协作密钥协议和身份验证协议”，*IEEE/ACM Trans。网络。*，卷。14，没有。2，第 263-276 页，2006 年 4 月。

[129] X. Zhang 和 D. Wang，“基于联盟区块链的智能交通自适应交通信号控制机制”，*IEEE Access*，第一卷。7，第 97281-97295 页，2019 年。

[130] Z. Lu、W. Liu、Q. Wang、G. Qu 和 Z. Liu，“基于区块链的 VANET 隐私保护信任模型”，*IEEE Access*，卷。6，第 45655-45664 页，2018 年。

[131] Y. Dai、D. Xu、K. Zhang、S. Maharjan 和 Y. Zhang，“用于车辆边缘计算和网络中内容缓存的深度强化学习和许可区块链”，*IEEE Trans。车。技术。*，卷。69，没有。4，第 4312-4324 页，2020 年 4 月。

[132] L. Wang、X. Lin、E. Zima 和 C. Ma，“基于区块链的类似 airbnb 的隐私增强型私人停车位共享”，*IEEE Trans。车。技术。*，卷。69，没有。3，第 2411-2423 页，2020 年 3 月。

[133] “Hyperledger 架构，第 I 卷（白皮书）”，Hyperledger Found.，美国加利福尼亚州旧金山，白皮书，2021 年。[在线]。可用： https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[134] N. Van Saberhagen，“Cryptonote v 2.0”，字节币，白皮书，2013 年。[在线]。可用：https://www.bytecoin.org/old/whitepaper.pdf

[135] A. 默恩。 “错过了 比特币 热潮？ 五更莫名其妙 _ 加密货币让你的储蓄大增。” 2016. [在线]。可用：https://www.theguardian.com/technology/shortcuts/2017/dec/11/missedbitcoin-boom-five-more-baffling-cryptocurrencies-to-blow-yoursavings-on

[136] S.-K。Kim，“使用区块链治理游戏增强车联网安全网络”，2019 年 1 月，*arXiv:1904.11340*。

[137] R. Shrestha 和 SY Nam，“用于防止 51% 攻击的车辆网络区域区块链”，*IEEE Access*，第一卷。7，第 95021-95033 页，2019 年。

[138] H. Liao、Y. Mu、Z. Zhou、M. Sun、Z. Wang 和 C. Pan，“用于车载雾计算的基于区块链和学习的安全智能任务卸载”，*IEEE Trans。英特尔。反式。系统。*，卷。22，没有。7，第 4051-4063 页，2021 年 7 月。

[139] B. Luo、X. Li、J. Weng、J. Guo 和 J. Ma，“区块链在 VANET 中启用了基于信任的位置隐私保护方案”，*IEEE Trans。车。技术。*，卷。69，没有。2，第 2034-2048 页，2020 年 2 月。

[140] Z. Su、Y. Wang、Q. Xu 和 N. Zhang，“LVBS：用于灾害救援中安全数据共享的轻量级车载区块链”，*IEEE Trans。可靠的安全计算。*，卷。19，没有。1，第 19-32 页，1 月/2 月。2022 年。

[141] X. Deng 和 T. Gao，“VANETs 中基于区块链的电子支付方案”，*IEEE Access*，第一卷。8，第 38296-38303 页，2020 年。

[142] J.康*等人。*，“用于车辆边缘计算和网络中安全高效数据共享的区块链”，*IEEE Internet Things J.*，第一卷。6，没有。3，第 4660-4670 页，2019 年 6 月。

[143] S. Xia、F. Lin、Z. Chen、C. Tang、Y. Ma 和 X. Yu，“基于贝叶斯博弈的区块链车联网车对车电力交易方案”，*IEEE Trans . 车。技术。*，卷。69，没有。7，第 6856-6868 页，2020 年 7 月。

[144] H. Chai、S. Leng、Y. Chen 和 K. Zhang，“用于车联网知识共享的分层区块链联合学习算法”，*IEEE Trans。英特尔。反式。系统。*，卷。22，没有。7，第 3975-3986 页，2021 年 7 月。

[145] G. Sun, M. Dai, F. Zhang, H. Yu, X. Du, and M. Guizani, “Blockchainenhanced high-confidence energy sharing in Electric Vehicles Internet,” *IEEE Internet Things J.* , vol. 7，没有。9，第 7868-7882 页，2020 年 9 月。

[146] S. Iqbal、AW Malik、AU Rahman 和 RM Noor，“基于区块链的微级别车载雾网络中任务卸载的声誉管理”，*IEEE Access*，第一卷。8，第 52968-52980 页，2020 年。

[147] Y.-T。杨，L.-D。周，C.-W。曾，F.-H. 曾和 C.-C。刘，“基于区块链的 VANET 交通事件验证和信任验证”，*IEEE Access*，第一卷。7，第 30868-30877 页，2019 年。

[148] H. Liang、J. Wu、S. Mumtaz、J. Li、X. Lin 和 M. Wen，“MBID：基于微区块链的 V2X 地理动态入侵检测”，*IEEE Commun。麦格。*，卷。57，没有。10，第 101-1 页 10 月 77–83 日 2019 年。

[149] M. Cebe、 E . Erdin 、 K. Akkaya、 H. Aksu 和 S. Uluagac，“Block4Forensic：用于联网车辆取证应用的集成轻量级区块链框架，” *IEEE Commun。麦格。*，卷。56，没有。10，第 50-57 页，2018 年 10 月。

[150] T. Jiang、H. Fang 和 H. Wang，“基于区块链的车联网：分布式网络架构和性能分析”，*IEEE Internet Things J.*，第一卷。6，没有。3，第 4640-4649 页，2019 年 6 月。

[151] B. Yin、Y. Wu、T. Hu、J. Dong 和 Z. Jiang，“基于区块链安全信息交换的车联网 (IoV) 高效协作和激励机制”，*IEEE Internet Things J.*，卷。7，没有。3，第 1582-1593 页，2020 年 3 月。

[152] M. Labrador 和 W. Hou，“在车联网 (IoV) 中实施区块链技术”，*Proc。诠释。会议。英特尔。计算。出现。应用程序。(ICEA)*，2019 年，第 5-10 页。

[153] C. Sommer、R. German 和 F. Dressler，“用于改进 IVC 分析的双向耦合网络和道路交通仿真”，*IEEE Trans。移动计算。*，卷。10，没有。1，第 3-15 页，2011 年 1 月。

[154] MJ Haidari 和 Z. Yetgin，“基于静脉的车载自组织网络研究”，*Proc。诠释。神器。英特尔。数据处理。症状。(IDAP)*，2019 年 9 月，第 1-7 页。

[155] M. Piórkowski、M. Stripe、AL Lugo、P. Papadimitros、M. Grossglauser 和 J.-P。Hubaux，“TraNS：用于 VANETs 的现实联合交通和网络模拟器”，*ACM SIGMOBILE 移动计算。交流。神父牧师。*，卷。12，没有。1，页。1 月 31 日至 33 日，2008 年。

[156] 诉库马尔*等人。*，“iTETRIS：ITS 技术在大规模集成仿真中的应用”，*Proc。IEEE 第 71 辆汽车。技术。会议。*，2010 年 6 月，第 1-5 页。

[157] J. Kang、R. Yu、X. Huang 和 Y. Zhang，“雾计算支持的车联网的隐私保护假名方案”，*IEEE Trans。英特尔。反式。系统。*，卷。19，没有。8，第 2627-2637 页，2018 年 8 月。

[158] M. Li、L. Zhu、Z. Zhang、X. Du 和 M. Guizani，“PROS：通过车载雾计算保护隐私的路线共享服务”，*IEEE Access*，卷。6，第 66188-66197 页，2018 年。

[159] DB Rawat、R. Doku、A. Adebayo、C. Bajracharya 和 C. Kamhoua，“区块链启用命名数据网络以实现安全的车与一切通信”，*IEEE 网络。*，卷。34，没有。5，第 185–189 页，9 月/10 月。2020 年。

[160] V. Hassija、V. Chamola、G. Han、JJPC Rodrigues 和 M. Guizani，“DAGIoV：使用有向无环图和博弈论的车对车通信框架”，*IEEE Trans。车。技术。*，卷。69，没有。4，第 4182-4191 页，2020 年 4 月。

[161] X. Gong、F. Dong、MA Mohamed、OM Abdalla 和 ZM Ali，“考虑 PEM 燃料电池和电动汽车的智能混合微电网的安全能源管理架构”，*IEEE Access*，第一卷。8，第 47807-47823 页，2020 年。

[162] S. Nadeem、M. Rizwan、F. Ahmad 和 J. Manzoor，“使用基于雾节点的分布式区块链云架构保护认知无线电车载自组网络”，*诠释。J.Adv。计算。科学。应用程序。*，卷。10，没有。1，第 288-295 页，2019 年 1 月。

[163] MU Hassan、MH Rehmani 和 J. Chen，“区块链技术中的差异隐私：一种未来方法”，*J. Parallel Distrib。计算。*，卷。145，第 50-74 页，2020 年 11 月。

[164] M. Eltoweissy、S. Olariu 和 M. Younis，“走向自主车辆云”，*Proc。诠释。会议。特设网络。*，2010 年 8 月，第 1-16 页。

[165] C. Yu、B. Lin、P. Guo、W. Zhang、S. Li 和 R. He，“用于自动驾驶的基于雾计算的车联网基础设施的部署和尺寸确定”，*IEEE Internet Things J .*，卷。6，没有。1，第 149-160 页，2019 年 2 月。

[166] H. Lu、Q. Liu、D. Tian、Y. Li、H. Kim 和 S. Serikawa，“自动驾驶汽车的认知互联网”，*IEEE 网络。*，卷。33，没有。3，第 65-73 页，5 月/6 月。2019 年。

[167] H. Wang、B. Kim、J. Xie 和 Z. Han，“电动汽车：具有边缘辅助自动驾驶功能的联网车辆的通信方案”，*Proc。IEEE 国际。会议。交流。(ICC)*，2019 年 5 月，第 1-6 页。

[168] P. Mach 和 Z. Becvar，“移动边缘计算：关于架构和计算卸载的调查”，*IEEE Commun。调查图。*，卷。19，没有。3，第 1628-1656 页，第 3 季度，2017 年。

[169] V. Jacobson、DK Smetters、JD Thornton、MF Plass、NH Briggs 和 RL Braynard，“网络命名内容”，*Proc。第五诠释。会议。出现。网络。经验。技术。*，2009 年 12 月，第 1-12 页。

[170] L. Wang、R. Wakikawa、R. Kuntz、R. Vuyyuru 和 L. Zhang，“车对车通信中的数据命名”，*Proc。IEEE INFOCOM 研讨会*，2012 年 3 月，第 328–333 页。

[171] K. Asaf、RA Rehman 和 B.-S。Kim，“命名数据网络中的区块链技术：详细调查”，*J. Netw。计算。应用程序。*，卷。171，2020 年 12 月，艺术。不。102840。

[172] DO Mau、Y. Zhang、T. Taleb 和 M. Chen，“通过命名数据的车辆互联互通——一项 OPNET 模拟研究”，*Proc。诠释。会议。试验台水库。基础设施。*，2014 年 5 月，第 116-125 页。

[173] Y.-T。https://doi.org/10.1103/PhysRevLett.198.110001，Google Scholar Crossref，CAS 20。Yu、T. Punihaole、M. Gerla 和 MY Sanadidi，“车辆云中的内容路由”，*Proc。IEEE 军 交流。会议。(MILCOM)* 11 月 2012 年，第 101-1 页 1–6

[174] C. Xue, N. Xu, and Y. Bo，“基于区块链的软件定义网络关键技术研究”，*Proc. IEEE 国际。会议。服务。东方。系统。英。(SOSE)*，2019 年，第 239-2394 页。

[175] SSC G，V. 查莫拉，C.-K。Tham、S. Gurunarayanan 和 N. Ansari，“无线 SDN 网络边缘小云的最佳延迟感知任务分配方案”，*Future Gener。计算。系统。*，卷。102，第 862–875 页，2020 年 1 月。[在线]。可用：https://doi.org/10.1016/j.future.2019.09.003

[176] TJ VanderWeele 和 JM Robins，“四种效应修正：基于有向无环图的分类”，*流行病学*，卷。18，没有。5，第 561-568 页，2007 年 9 月。

[177] C. LeMahieu，“Nano：无感觉的分布式加密货币网络”，Nano Found.，伦敦，英国，白皮书，2018 年 4 月。访问：2018 年 3 月 24 日。[在线]。可用：https://content.nano.org/whitepaper/ Nano_Whitepaper_en.pdf

[178] A.丘留莫夫。“Byteball：用于存储和转移价值的去中心化系统。”2016. [在线]。可用：https://byteball.org/Byteball.pdf

[179] S. Popov，“The tangle，1.4.2 版”，IOTA Found.，柏林，德国，白皮书，第一卷。1，第 2018 年 3 月。[在线]。可用的：https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[180] MU Hassan、MH Rehmani 和 J. Chen，“网络物理系统的差分隐私技术：一项调查”，*IEEE Commun。调查图。*，卷。22，没有。1，第 746–789 页，2019 年第一季度。

[181] G. Bansal、N. Naren、V. Chamola、B. Sikdar、N. Kumar 和 M. Guizani，“使用物理不可克隆功能的 V2G 轻量级相互认证协议”，*IEEE Trans。车。技术。*，卷。69，没有。7，第 7234-7246 页，2020 年 7 月。

[182] K.克罗曼*等人。*，“关于扩展去中心化区块链”，*Proc。诠释。会议。金融。加密货币。数据安全*，2016 年 2 月，第 106-125 页。

[183] S. Islam、S. Badsha、S. Sengupta、H. La、I. Khalil 和 M. Atiquzzaman，“支持区块链的智能车辆边缘计算”，*IEEE Netw。*，卷。35，没有。3，第 125–131 页，5 月/6 月。2021 年。

[184] V. Hassija、V. Chamola、A. Goyal、SS Kanhere 和 N. Guizani，“即将到来的量子计算应用：展望未来”，*IET Quantum Commun。*，卷。1，没有。2，第 35-41 页，2020 年 12 月。

[185] AK Fedorov、EO Kiktenko 和 AI Lvovsky，“量子计算机将区块链安全置于风险之中”，《*自然*》，待出版。

[186] AM Khalifa、AM Bahaa-Eldin 和 MA Sobh，“用于权益证明的量子攻击和防御”，*Proc。第十四诠释。会议。计算。英。系统。(ICCES)*，2019 年 12 月，第 112-117 页。

[187] SS Vattaparambil、R. Koduri、S. Nandyala 和 M. Manalikandy，“用于安全车对车通信的可扩展分散式解决方案”，SAE Techn。论文，美国宾夕法尼亚州沃伦代尔，众议员 2020-010724，2020 年 4 月。

[188] EO Kiktenko *等人。*，“量子安全区块链”，*量子科学。技术。*，卷。3，没有。3，2018 年 5 月，艺术。不。35004. [在线]。可用的：http://dx.doi.org/10.1088/2058-9565/aabc6b

[189] X. Sun、M. Sopek、Q. Wang 和 P. Kulicki，“迈向量子安全许可区块链：签名、共识和逻辑”，*熵*，卷。21，没有。第 9 页 887，2019 年 9 月。

[190] M.萨德*等人。*，“探索区块链的攻击面：综合调查”，*IEEE Commun。调查图。*，卷。22，没有。3，第 1977-2008 页，2020 年第 3 季度。

Tejasvi Alladi（IEEE 高级成员）于 2010 年在印度皮拉尼的 Birla Institute of Technology and Science (BITS-Pilani) 获得学士学位，在美国北卡罗来纳州罗利市的北卡罗来纳州立大学获得硕士学位，2015 年获得博士学位。2021 年获得 BITS-Pilani 学位。2021 年 1 月至 2021 年 12 月，他在加拿大安大略省渥太华的卡尔顿大学系统与计算机工程系担任博士后研究员。他目前是助理计算机科学系教授和信息系统，BITS-Pilani。他还在半导体跨国公司（例如高通技术和三星电子）的嵌入式系统方面拥有大约六年的行业经验。他的研究兴趣包括使用密码学、深度学习和区块链技术开发物联网安全解决方案。

Vinay Chamola（IEEE 高级成员）分别于 2010 年和 2013 年在印度皮拉尼的 Birla Institute of Technology and Science (BITS-Pilani) 获得电气和电子工程学士学位和通信工程硕士学位，和博士学位。2016 年获得新加坡国立大学电气和计算机工程学士学位。2015 年，他是美国加利福尼亚州洛杉矶市南加州大学自治网络研究组的访问研究员。他还曾在新加坡国立大学担任博士后研究员。他目前是 BITS-Pilani 电气和电子工程系的助理教授，领导物联网研究小组/实验室。他在高级别 SCI 期刊上发表了 90 多篇论文，其中包括 60 多篇 IEEE Transactions、期刊和杂志文章。他的研究兴趣包括物联网安全、区块链、无人机、VANET、5G 和医疗保健。他担任 *AdHoc Networks* (Elsevier) 和 *IEEE Internet of Things Magazine 的区域编辑*. 他担任多个知名研讨会的联合主席，例如 IEEE Globecom Workshop 2021、IEEE INFOCOM Workshop 2022、IEEE ANTS 2021 和 IEEE ICIAfS 2021。他是一家医疗保健初创公司 Medsupervision Pvt 的联合创始人和总裁。他还担任 IEEE NETWORKING LETTERS、*IET Quantum Communications* 和 *IET Networks* 的副主编。他是 *Computer Communication* (Elsevier) 和 *IET Intelligent Transportation Systems* 的客座编辑。

Nishad Sahu 于 2020 年在皮拉尼的 Birla Institute of Technology and Science (BITS-Pilani) 获得电气和电子学学士学位，目前他正在该学院的电气和电子系攻读嵌入式系统的 ME 学位。他在 IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS 、IEEE SENSORS 和 *Vehicular Communications* 等 SCI 索引的国际期刊上与人合着了 8 篇期刊论文，并在国际会议上发表了 2 篇论文。他与两个人实习过
印度著名的政府研究实验室；DRDO，防御实验室，焦特布尔和 CSIR-CEERI，皮拉尼。他的研究兴趣包括为人工智能算法设计硬件加速器、车辆网络、自动驾驶汽车、物联网安全、区块链、FPGA、无人机、物联网应用的智能传感器开发和系统工程。他还获得了许多奖项，如 Wiley 颁发的 2018-2019 年最佳下载论文证书、皮拉尼校区 BITSPilani 2020 年毕业班的 VS Rao 教授最佳全能奖、Center for the Center for the Innovator of the Year Award 2019-2020 创业领导力，以及 2017 年 BITS Pilani 和艾利丹尼森发明精神奖学金。他的硕士论文获得了 35 万印度卢比的学生创新资助，来自印度科学研究所班加罗尔的人工智能和技术园 (ARTPARK)。

Vishnu Venkatesh 于 2021 年在皮拉尼的 Birla Institude of Technology and Science 获得电气和电子工程学士学位。他目前在 WCB Robotics Pvt 担任副设计工程师。Ltd. 他的主要专业兴趣是嵌入式系统开发，尤其是硬件和固件设计。在本科期间，他还参与了密码学、光子学、物联网安全、车载网络和区块链领域的研究项目和合着论文。

Adit Goyal 目前正在追求 B.Tech。拥有诺伊达 Jaypee 信息技术学院计算机科学系的学位。他目前正在印度皮拉尼的 BITS-Pilani 进行研究实习，师从 V. Chamola 博士。他在数据科学、机器学习和大数据领域完成了一些项目。他的研究兴趣包括机器学习、数据科学和量子计算。

Mohsen Guizani（IEEE 研究员）获得了 BS（以优异成绩）、MS 和博士学位。分别于 1985 年、1987 年和 1990 年在美国纽约州雪城大学雪城大学获得电气和计算机工程学位。他目前是 Mohamed Bin Zayed 大学的机器学习教授和副教务长
人工智能 (MBZUAI)，阿联酋阿布扎比。此前，他曾在美国的不同机构工作。他撰写了十本书和 800 多篇出版物。他的研究兴趣包括
应用机器学习和人工智能、物联网、智能系统、智慧城市和网络安全。他在 2019 年、2020 年和 2021 年被列为 Clarivate Analytics 计算机科学高被引科学家。他获得了多项研究奖项，包括 2015 年 IEEE 通信学会最佳调查论文奖、2021 年最佳 ComSoc 期刊论文奖等作为 ICC 和 Globecom 会议的五项最佳论文奖。他还是 2017 年 IEEE 通信学会无线技术委员会认可奖、2018 年 AdHoc 技术委员会认可奖和 2019 年 IEEE 通信和信息安全技术认可奖的获得者。他曾担任 IEEE NETWORK 的主编目前在许多 IEEE TRANSACTIONS 和杂志的编委任职。他曾任 IEEE 通信协会无线技术委员会主席和 TAOS 技术委员会主席。他曾担任 IEEE 计算机学会杰出演讲者，目前是 IEEE ComSoc 杰出讲师。