中国科学: 信息科学 2023 年 第 53 卷 第 5 期: 841–877
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
评述

基于区块链的车联网安全综述

刘媛妮[1], 李奕[1], 陈山枝[2*]

1. 重庆邮电大学网络空间安全与信息法学院, 重庆 400065
2. 无线移动通信全国重点实验室 (中国信息通信科技集团有限公司), 北京 100191
* 通信作者. E-mail: chensz@cict.com

收稿日期: 2022–01–13; 修回日期: 2022–04–05; 接受日期: 2022–05–24; 网络出版日期: 2023–05–06

国家自然科学基金 (批准号: 61731017, 61931005)、四川省重点研发计划项目 (批准号: 2022YFG0022)、重庆市自然科学基金面上项目 (批准号: cstc2020jcyj-msxmX1021) 和重庆市教委科学技术研究项目 (批准号: KJZD-K202000602) 资助

摘要 随着车联网 (Internet of vehicles, IoV 或 vehicle to everything, V2X) 技术推动汽车行业和交通行业的智能化、网联化进程加快, 车联网安全问题日益严峻. 区块链 (Blockchain, BC) 作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用, 为车联网安全提供新的解决思路. 本文对基于区块链的车联网安全研究展开综述, 首先汇总了现有的车联网安全威胁和防护手段; 其次梳理了区块链和车联网结合的研究价值; 然后分析了当前基于区块链的车联网安全关键技术; 接着从通信安全、数据安全、应用安全 3 个角度重点阐述了现有基于区块链的车联网安全防护手段和方法, 并总结了现有的基于区块链的新型车联网安全体系架构; 最后展望了基于区块链的车联网安全的未来发展方向和研究重点.

关键词 车联网安全, 区块链, 通信安全, 数据安全, 应用安全

1 引言

车联网指借助新一代信息通信技术, 实现车内、车与人 (vehicle to pedestrians, V2P)、车与车 (vehicle to vehicle, V2V)、车与路 (vehicle to infrastructure, V2I)、车与平台 (vehicle to network, V2N) 的全方位网络连接, 提升汽车智能化水平和自动驾驶能力, 降低事故率, 从而提高交通效率, 改善汽车驾乘体验, 构建汽车和交通服务新业态, 为用户提供智能、舒适、安全、节能、高效的综合服务 [1]. 狭义的车联网专指 V2X (vehicle to everything), 实现从远程信息处理 (telematics) 到车与车、车与路的实时协同、从单车智能到网联智能, 基于 V2V, V2I, V2P, V2N 等提供的环境感知、信息交互与协同控制能力支撑交通安全类、交通效率类、自动驾驶类、信息娱乐类丰富的应用类型. 广义的车联网指车内网 (in vehicle network, IVN)、车际网 (inter-vehicle communication, ICV)、车云网三者的结合, 是车

引用格式: 刘媛妮, 李奕, 陈山枝. 基于区块链的车联网安全综述. 中国科学: 信息科学, 2023, 53: 841–877, doi: 10.1360/SSI-2022-0019
Liu Y N, Li Y, Chen S Z. A survey of Internet of vehicles/vehicle to everything security based on Blockchain (in Chinese). Sci Sin Inform, 2023, 53: 841–877, doi: 10.1360/SSI-2022-0019

辆、道路、环境、云 (平台) 间进行数据和信息交换的通信技术, 是实现智能交通和无人驾驶的关键使能技术 [2].

车联网网络的开放性、网络拓扑的不稳定性、数据的混杂性、设备的异构性等特征使系统的安全性受到严重威胁. 首先, 攻击者通过散布虚假信息影响交通秩序, 甚至引发交通事故 [3]; 其次, 攻击者可以跟踪用户轨迹, 窥探并侵犯用户的隐私; 再者, 攻击者也可篡改车辆自身信息规避事故责任. 传统车联网安全技术, 例如: 加密、认证、访问控制等, 在一定程度上能够满足车联网的安全需求. 然而, 车联网增强应用, 如高级驾驶、远程驾驶、车辆编队行驶等, 正朝着低时延、高可靠的方向快速演进, 亟须引进一种具有高安全性、隐蔽性和抗毁性的范式来满足新型车联网应用的安全需求.

作为一种全新的去中心化基础架构和分布式计算范式, 区块链 (Blockchain, BC) 将哈希函数、Merkle 树、共识算法等成熟技术进行重组, 结合公钥加密、数字签名、零知识证明等密码学技术, 能够构建具有良好抗毁性、容错性和扩展性的分布式对等网络. 在该分布式网络结构下, 部分节点被破坏后, 系统仍可以保证数据的存储和网络的计算能力, 并通过共识机制维持网络的正常运转. 目前, 区块链技术已被用于多个场景, 如金融、产品溯源、政务民生、电子存证、数字身份、供应链协同等. 在此背景下, 将区块链引入到车联网环境中, 对于实现车联网系统协作与同步、安全与信任、数据共享等方面具有重要的理论研究意义.

目前, 区块链的相关理论研究与车联网产业实践均处于快速发展阶段, 针对区块链使能车联网安全的研究仍处于探索阶段, 相关问题尚未形成统一的认识. 本文将主要围绕基于区块链的车联网安全关键技术, 对区块链在应对车联网面临的安全威胁问题的研究以及未来挑战进行综述, 具体贡献如下.

(1) 全面概括了车联网安全技术. 针对车联网架构中设备、通信、云平台、应用服务的安全威胁, 梳理了现有的安全防护手段; 在分析基于区块链的车联网安全现状的基础上, 归纳了区块链和车联网结合的研究价值.

(2) 全面总结了基于区块链的车联网安全研究工作. 从信息安全的角度, 梳理了现有基于区块链的车联网安全关键技术; 并从通信安全、数据安全、应用安全 3 个角度介绍了现有基于区块链的安全防护方法; 概括了区块链和边缘计算/网络功能虚拟化/软件定义网络融合的新型车联网安全体系架构.

(3) 全面探讨了基于区块链的车联网安全技术目前的机遇与挑战, 并在此基础上提出了区块链技术应用于车联网安全领域的未来研究方向.

2 基于区块链的车联网安全

2.1 车联网体系架构及面临的安全威胁

车联网通信技术主要包括: 蜂窝网络通信技术 (如 3/4/5G)、车内通信技术 (如 CAN 总线、LIN、车内以太网、Flexray、MOST)、V2X 通信技术 (C-V2X [4,5]: LTE-V2X 和 NR-V2X、DSRC)、WiFi 通信技术、无线个域通信技术 (Bluetooth, RFID, Zigbee, NFC). 其中, 蜂窝网络通信技术多用于 V2N 场景, 车内通信技术仅用于 IVN 场景, V2X 通信技术多用于 V2V, V2I, V2P 场景, WiFi 通信和无线个域通信技术多用于 IVN, V2P 场景.

车联网较长的产业链涵盖了元器件供应商、设备生产商、软硬件技术提供商等制造商, 文献 [2] 对车联网涉及的关键技术进行了梳理, 提出了车路协同视角下的感知层、通信层、平台层、应用层的 4 层架构, 并将其映射到通信和应用视角下的 “端 – 边 – 管 – 云” 车联网系统架构 (如图 1 所示). 与传统的网络相比, 车联网具有新的系统组成和应用场景, 其安全威胁涉及到体系架构中的各个层面, 主

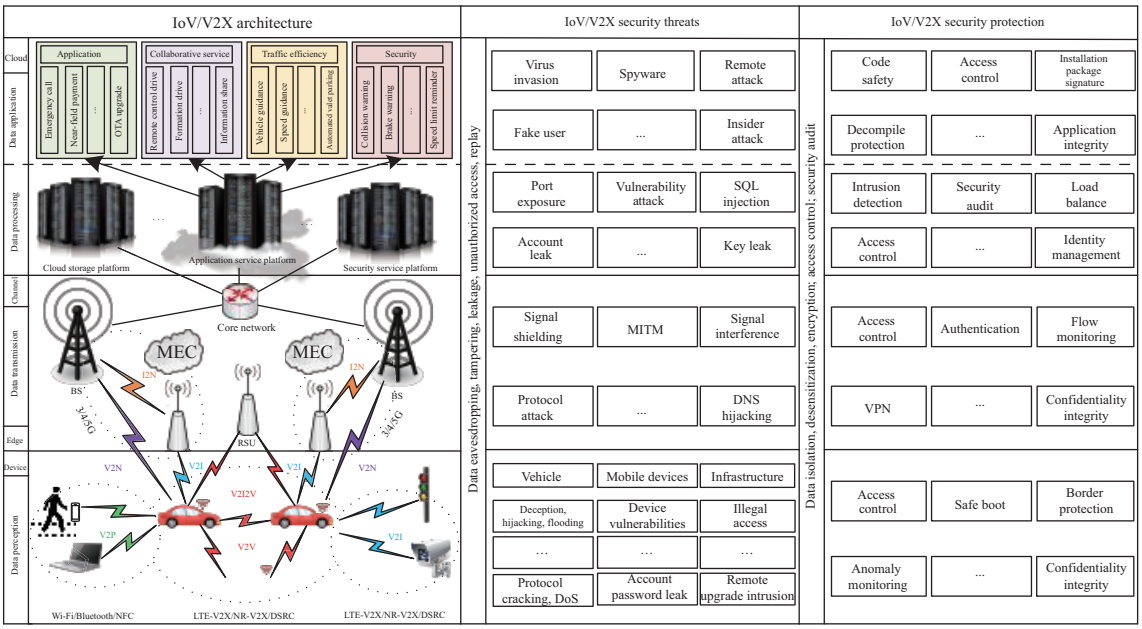

图 1 车联网体系架构、安全威胁、安全防护

Figure 1 IoV (Internet of vehicles)/V2X system architecture, security threats, security protection

要表现在设备安全、V2X 通信安全、平台安全、应用安全等方面.

车联网设备主要包括通信车辆、移动设备 (手机、平板等) 和基础设施 (路侧设备、摄像头、红绿灯等) 等. 通信车辆的安全威胁来自于车载设备, 其中, 车载网关和电子控制单元 (electronic control unit, ECU) 易遭受欺骗、劫持、泛洪等攻击; 远程信息处理器 (telematics box, T-BOX) 易遭受信息泄露、协议破解、DoS 等攻击; 车载信息娱乐系统 (in-vehicle infotainment, IVI) 易遭受漏洞利用、数据窃取等攻击; 车载诊断接口 (on-board diagnostic, OBD) 易遭受篡改、提取等攻击. 移动设备主要面临账户密码泄露、设备漏洞等安全威胁. 基础设施主要面临非法接入、远程升级入侵等安全威胁.

V2X 通信网络主要包括 V2P, V2I, V2V, V2N 等. V2X 多采用无线链路, 与有线链路相比, 无线链路更容易遭受攻击者的数据拦截, 导致消息的篡改/重放、敏感数据泄漏等. 攻击者也可通过信号屏蔽、信号篡改、信号干扰等方式阻断无线网络通信. 此外, 协议伪装、DNS (domain name system) 劫持、中间人攻击、GPS (global positioning system) 欺骗也会影响 V2X 通信安全.

车联网云平台负责数据的汇聚、计算、监控和管理. 云平台的开放性使得攻击者和用户具有相同的权限访问云服务, 比传统云计算平台更易遭受跨站脚本攻击、SQL 注入、逻辑漏洞、暴力破解、文件上传、信息泄露、拒绝服务等安全威胁.

车联网应用服务根据服务对象的不同, 可分为应用类、协同服务类、交通效率类、安全类. 其安全威胁主要来自应用程序, 包括病毒入侵破坏程序的正常运行; 广告软件、间谍软件泄露隐私信息; DNS 投毒、TCP (transmission control protocol) 去同步化实施远程攻击. 同时, 弱身份认证使得应用程序数据易遭受伪造/篡改/窃听以及用户隐私泄露等安全威胁.

此外, 车联网数据的窃听、泄露、篡改、非授权访问、重放以及隐私泄露等安全威胁问题贯穿于车联网体系架构的各个环节.

2.2 现有的车联网安全防护措施

针对车联网系统面临的上述安全威胁, 现有的研究 [2] 提出了相关的安全防护措施.

设备安全的防护包括安全启动、边界防护、异常监测、机密性完整性保护等. 在车载设备上, 通过完备的接入控制机制保证合法用户接入, 同时加强安全防护, 例如: 在硬件方面, 增加硬件安全模块, 将加密算法、访问控制、完整性检查等功能嵌入到 ECU 控制系统; 在软件方面, 保护 ECU 软件的完整性. 在移动设备上设置系统安全启动措施避免恶意攻击. 在基础设施上设置边界防护系统, 防止攻击者非法入侵, 保证路侧基础设施安全.

通信安全的防护包括利用身份认证机制, 保证身份的合法性, 避免恶意攻击者对信号的屏蔽/篡改/干扰; 利用加密技术实现对网络协议、网络接口的加密; 利用流量监测机制防止恶意流量对网络的阻塞, 保证网络高效稳定运行.

平台安全的防护包括访问控制、负载均衡、身份管理等. 配备防火墙设备, 阻止不明身份的访问, 防止内部信息泄露; 配备负载均衡设备, 统一接受全部请求, 再按规则进行分配, 分解单个服务器压力, 从而保证用户功能的实时性; 设置身份管理模块, 对接入平台的用户进行鉴别、授权、记账等; 设置信任管理模块, 评估接入节点的可信程度, 防止恶意入侵.

应用安全的防护主要是针对应用程序进行安全防护, 包括代码安全检测、安装包签名、反编译保护、应用完整性保护等, 确保应用程序不受侵害.

此外, 访问控制、数据隔离、数据脱敏、数据加密、安全审计、隐私保护等防护措施贯穿于车联网体系架构的各个层面, 是车联网安全防护研究的重要内容.

总的来看, 现有车联网安全防护措施多利用信息安全的方法和手段保证车联网的安全. 全生命周期的 “汽车即服务” 渐成趋势以及个性化定制、生产设计协同、OTA (over-the-air) 技术软件升级等业务的推陈出新使得车联网需要精准、实时的数据交换与共享, 然而车辆的高移动性、无线网络的复杂性、组件的异构性使得传统基于云的数据存储手段和管理模式面临巨大的困难 [6], 迫切需要一种新的范式来构建去中心化、扩展性强、高安全性的车联网系统.

2.3 区块链使能的车联网安全

区块链利用加密链式结构来验证与存储数据, 利用分布式节点共识算法来生成和更新数据, 利用自动化脚本代码 (智能合约) 来编程和操作数据 [7], 其具有的去中心化、时序数据、集体维护、可编程和安全可信的特点可为车联网安全提供新的解决方案. 针对区块链在车联网领域的应用, 目前已有综述性文献进行了总结. 文献 [8] 梳理了在 V2X 中实施区块链的十大挑战: 账本的可伸缩性差、区块处理算法能力和时间一致性问题、数据交互的管理问题、不同 V2X 系统的互操作问题、设备资源的异构性、攻击面较多、主账本存储量大、缺乏可用的共识机制、相关法律的修订和更新问题、敏感数据的保密问题, 对区块链成功部署在 V2X 中具有重要的借鉴意义. 文献 [9] 从 IoV 的安全问题出发, 提出将区块链结合到 IoV 中面临的挑战和机会, 对区块链和 IoV 的结合具有指导意义. 文献 [10] 针对当前 IoV 架构未考虑的安全性、隐私性、信任和共享等问题, 论述了当前基于区块链的 IoV 的 4 种应用研究: 安全 (透明性、不变性)、信任 (交易自动化)、激励 (加密货币)、隐私保护 (匿名), 对构建安全的基于区块链的车联网架构具有借鉴作用. 文献 [11] 将区块链技术分为基于安全、隐私、声誉、分布式、去中心化、数据共享、身份认证、信任的方法, 全面调查现有基于区块链的 IoV 保护方案, 并指出现有研究的局限性.

综上所述, 本文认为将区块链引入到车联网中具有重要的研究意义, 现详细阐述如下:

(1) 构建去中心化的车联网. 区块链能够创建去中心化的车联网, 包含更多的分布式实体, 如基站、RSUs (road side units)、车辆等. 这些分布式实体能够独立管理自己的操作, 并利用分布式共识机制来验证和更新数据. 当前基于中心决策的车联网工作模式将被迁移到分布式体系架构中, 不再需要实体与网络中的第三方机构通信, 减少应用程序和服务的延迟, 增强用户体验. 此外, 由于分布式和中心化存储技术的结合, 基于区块链的数据存储及交易代价将会大大降低.

(2) 构建高抗毁性的车联网. 区块链依靠现代加密技术, 能够为车联网提供更好的安全性和隐私性. 在基于区块链的车联网中, 每个用户可以管理自己的密钥, 并且每个区块节点只需存储用户数据加密后的分片. 同时, 所有对等节点之间具有同步和复制的特点, 即使一个或多个节点受损, 服务也能平稳运行, 使得车联网具有更强的抗毁性.

(3) 基于智能合约的自动化及智能化事务管控. 智能合约旨在以代码的方式验证或强制执行预定义的协议规则, 从而允许匿名用户间可信的交易. 车联网借助智能合约可以部署和实施任何预定义的规则或脚本, 从而实现基于 Uu 接口的云平台业务应用和基于 PC5 接口的直连通信业务应用. 进一步地, 结合智能合约, 车联网系统可在去中心化事务交互时实现各种流程的自动化及智能化管控.

(4) 为车联网数据提供更高的安全性. 区块链作为不可篡改的分布式账本, 其特有的时序性、不变性、不可伪造性、透明性、可审计性可以自动记录带时间戳的车辆信息, 并通过区块哈希相互连接, 潜在地避免数据被篡改, 可在分布式账本下实现交易的追溯, 有助于精准审计.

(5) 连接互不信任的异构实体. 借助新的共识机制, 区块链可在不受信任实体间建立强大的信任. 此外, 还可以通过智能合约对事先约定的内容作出信任决策, 无需依赖受信任的实体.

本文后续章节在梳理基于区块链的车联网安全关键技术的基础上, 对基于区块链的车联网通信安全、数据安全、应用安全、新型安全体系架构的研究现状和存在的问题进行详细总结. 综合全篇内容, 本文提出了基于区块链的车联网安全研究框架与技术路线, 如图 2 所示, 以期待能够为后续的创新发展提供有价值的参考. 可以看出, 密钥管理、认证机制、访问控制、信任管理、隐私保护属于保障车联网安全的共性关键技术, 支撑车联网通信安全、数据安全、应用安全、新型体系架构安全的发展和演化. 基于人工智能/软件定义网络/有向无环图等技术优化的高性能区块链网络是支撑车联网高效、安全通信的重要基石, 为车联网数据交易和共享提供可靠性保障. 同时, 基于区块链的车联网数据安全是上层应用安全的基础支撑. 最后, 车联网应用安全对通信时延、通信范围、传输效率等多样化需求将进一步推动新型车联网体系架构安全的创新发展.

3 基于区块链的车联网安全关键技术

由于车联网环境本身的特殊性, 传统的安全解决方案无法很好地适应动态、自组织、多跳的车联网生态系统 [12]. 当前, 基于区块链的车联网安全技术已成为学术界研究的重点, 这些技术借助区块链实现车联网的去中心化、分布式、匿名化、轻量级、高效率、可审计追踪等目标. 本节主要从基于区块链的车联网密钥管理、认证机制、访问控制、信任管理和隐私保护等关键技术展开论述. 其中, 密钥管理主要对密钥产生、分发、运算, 以及销毁等行为进行管理, 保证用户密钥安全. 认证通过判断通信方身份的合法性以及验证消息完整性避免非法用户恶意传播消息; 访问控制在认证的基础上对合法实体的资源访问权限实施策略控制, 防止资源的未授权访问; 信任管理通过构建信任模型计算节点的信任值, 识别恶意节点, 防止恶意攻击. 隐私保护通过匿名、加解密等手段保证车辆身份和位置信息, 防止敏感信息泄露.

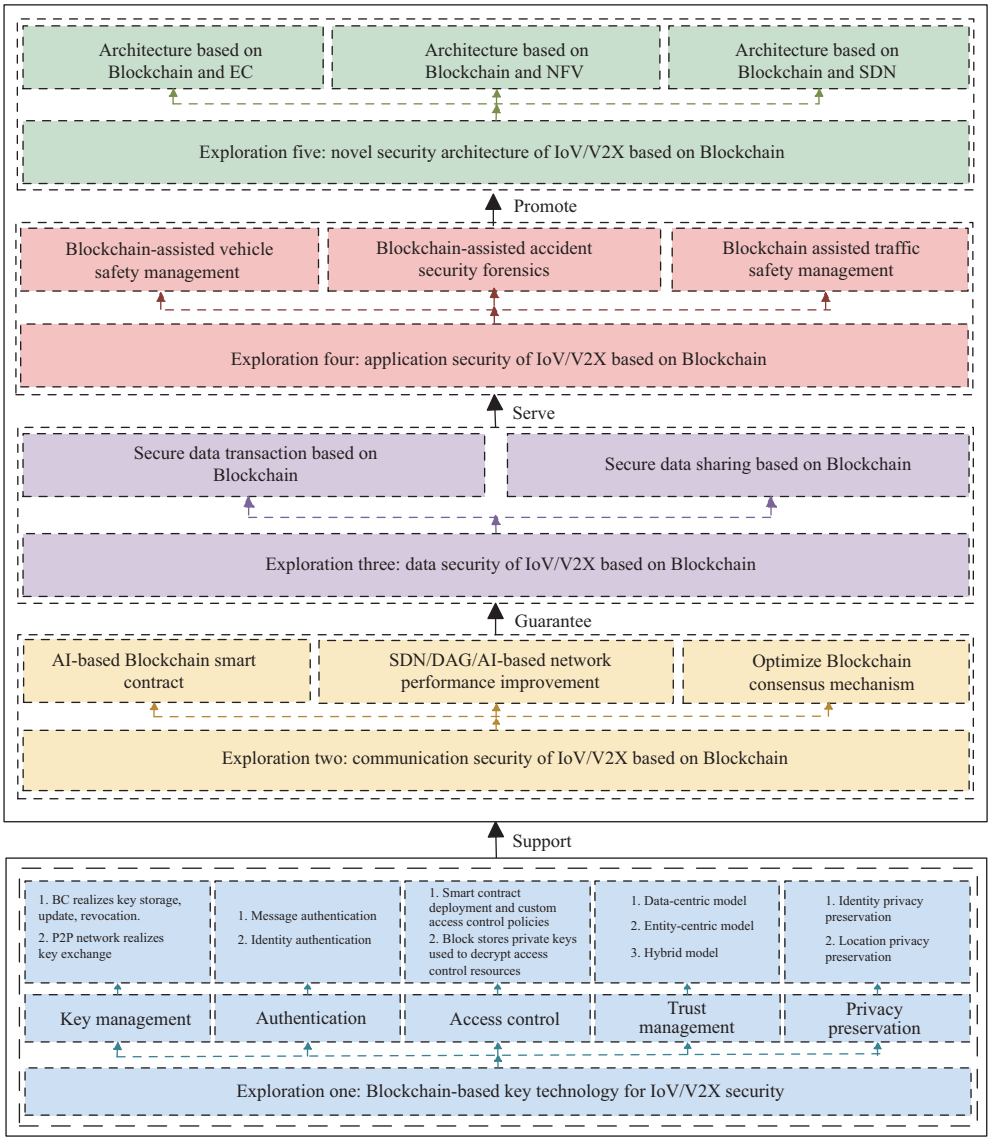

图 2　基于区块链的车联网安全研究框架与技术路线

Figure 2　IoV/V2X security research framework and technical route based on Blockchain

3.1　基于区块链的车联网密钥管理

密钥管理作为机密性、实体认证、数据完整性和数字签名等技术的基础, 在车联网身份标识、车间通信、数据安全等方面起着至关重要的作用. 当前, 基于区块链的车联网密钥管理的研究主要分为以下两个方面 [13]: 利用区块链存储密钥, 并通过智能合约实现密钥自动更新、撤销; 将密钥的信息封装在区块交易中, 通过 P2P 网络实现密钥交换. 相关文献对比表格如表 1 [14~17] 所示.

针对传统基于公钥基础设施 (public key infrastructure, PKI) 的密钥管理存在的单点故障问题, 文献 [14] 面向车载自组织网络 (vehicular ad-hoc network, VANET) 提出由权威中心 (trusted authority, TA) 和 RSUs 共同维护联盟链, 并使用联盟链分布式存储群组内车辆用于身份认证的公钥, 而公钥的更新/撤销均在区块链上动态、独立地执行, 有效避免单点故障. 文献 [15] 提议车辆在区块链上注册获

表 1 基于区块链的车联网密钥管理对比

Table 1 Comparison of IoV/V2X key management based on Blockchain

Problem	Proposal	Description	Method	BC techno.	BC nodes	Security properties
The single point of failure	[14]	Blockchain-based group key agreement protocol	BC stores short-term public keys	Consortium BC	TA, RSUs	Anonymity, traceability, non-linkability, forward and backward security
The single point of failure	[15]	Decentralized key management mechanism	Automatic registration, update and revocation of public key on the BC	Own	RSUs, Service provider	Resisting internal and external attacks
MITM, packet-dropping, decryption failure attacks	[16]	Key negotiations via BC	Key is embedded in the transaction currency value	Bitcoin	–	Traceable, authenticity
Heterogeneous VCS domains	[17]	Blockchain-based dynamic key management	Key transfer processes are verified and authenticated by the SM network	Own	Security managers	Integrity, traceability, authenticity

得公私钥, 并基于智能合约实现公钥的更新和撤销, 摆脱对中心化机构的依赖; 同时, 利用基于双变量多项式的轻量级认证和密钥协商协议, 防止注销用户和恶意用户的非法访问.

针对 Diffie-Hellman 密钥协商遭受的中间人 (man-in-the-middle, MITM)、丢弃报文和解密失败攻击, 文献 [16] 认为将密钥信息嵌入到比特币的价值信息中, 使用交易价值渠道、静态脚本和动态脚本进行密钥交换并保存带时间戳的记录, 可以保证密钥交换的追溯性和认证性. 类似地, 为简化异构车辆通信系统 (vehicular communication systems, VCS) 的密钥传输时间, 文献 [17] 认为将密钥信息封装到区块交易头上, 通过安全管理器 (security manager, SM) 的挖掘和广播完成交易的认证, 可保证密钥传输的完整性和不可否认性; 进一步地, 基于控制变量的方法根据最小密钥传输时间优化交易收集时间, 有效减少密钥传输的时间.

综上所述, 目前基于区块链的车联网密钥管理方案集中于利用区块链的防篡改特性构建公钥的信任链、利用智能合约自动化管理密钥以及利用区块链 P2P 网络实现的密钥交换. 本文认为, 车联网中基于区块链的密钥分发还存在丢包的风险, 可以考虑文献 [14] 提出的基于广播消息的自愈机制和基于相邻节点的互愈机制来减轻上述风险, 进而构建更健壮的密钥协商方案.

3.2 基于区块链的车联网认证机制

认证 (authentication) 在车辆身份核实、消息完整性验证上起到至关重要的作用 [18]. 基于区块链的认证机制通过对区块交易过程中的用户身份合法性、签名完整性和数据安全性等信息进行认证, 保证系统内部工作节点和外部注册用户身份的可验证性和可监管性 [19]. 本小节将从消息认证和身份认证两方面总结现有的基于区块链的车联网认证机制研究现状, 相关文献的对比表格如表 2 [20~33] 所示.

3.2.1 基于区块链的车联网消息认证

在基于区块链的消息认证的研究中, 文献 [20] 提出基于区块链的车辆身份识别和交易认证方法, 本地服务器存储和控制注册车辆 ID 并将区块链加密所需的公私钥发布给车辆, 由车辆和 RSUs 构成的区块链网络基于 SHA256 和公钥体制实现车辆交易数据的认证. 文献 [21] 在基于区块链的 IoV 数据安全共享系统中, 提出当区域内实体完成数据共享时, 利用辅助区块链存储共享数据, 否则将共享信息

表 2 基于区块链的车联网认证机制对比 [a)]

Table 2 Comparison of IoV/V2X authentication mechanism based on Blockchain[a)]

Proposal	Description	Method	BC techno.	BC nodes	Security properties
[20]	BC-based vehicle identification and data authentication	Data authentication based on hash and public key system	Own	Vehicles, RSUs	Confidentiality, privacy, authenticity
[21]	BC-based IoV data security sharing	Posterior countermeasures based on multi-signature	Own	Vehicles, RSUs, TMA, LED, issuers, tracers	Authenticity, privacy, non-repudiation
[22]	BC-based secure V2V communication	Data authentication based on link fingerprints	Own	Vehicles, cloud server	Authenticity, reliability
[23]	Information authentication based on improved Byzantine consensus	Consensus authentication based on time sequence and gossip protocol	Own	Vehicles, RSUs	Authenticity
[24]	Improved authentication based on BC	Identity authentication based on BC and public key	Own	Vehicles, RSUs, trusted cloud service providers	Authenticity
[25]	An efficient authentication scheme over BC	Mutual authentication between vehicle and BM based on ECC	Consortium Blockchain	BM, AM	CIA, privacy, anonymity, non-repudiation
[26]	Identity authentication and expeditious revocation based on BC	Mutual authentication between vehicle and RSU based on IBE	Own	RSUs, CA, RA	Integrity
[27]	BC-based lightweight authentication	Mutual authentication between vehicle and SM based on ECC	Consortium Blockchain	SM, witness peer	Confidentiality, privacy, anonymity
[28]	Lightweight BC-based authentication	Public key-based identity authentication	Own	Vehicles, RSUs, CA	Integrity, validity
[29]	BC-based and RSU-assisted authentication and key agreement	Mutual authentication between vehicle and TA based on block identifier	Own	TA	Forward and backward secrecy, anonymity
[30]	BC-based privacy preserving authentication	BC stores registration information	Ethereum	Local authentication centers	Confidentiality, non-repudiation, integrity, privacy
[31]	BC-based authentication and secure data transfer	BC stores pseudo identity	Own	–	Privacy
[32]	BC-based V2X remote attestation	BC stores identity key and integrity certification	Own	Gateway	Traceability, anonymity, non-repudiation, privacy
[33]	BC-based identity and trust management	Mutual authentication based on DIDs	Hyperledger Indy	–	Confidentiality, integrity, privacy
Rowan	V2V secure communication based on BC and side channel	Identity authentication based on certificate checks and visual identity	Public Blockchain	–	Practical forward secrecy

a) TMA: traffic management authority; LED: law enforcement department; AM: authentication manager; CIA: confidentiality, integrity, authenticity.

存储在父区块链中; 同时, 父区块链部署智能合约, 以确保数据的一致性; 此外, 系统利用基于阈值的先验对策判定车辆共享消息是否可信, 并基于多重签名的后验对策实现消息认证, 防止恶意车辆的消息传播. 上述认证方案均依赖于公钥密码, 在一定程度上存在计算复杂度高和时延长的问题, 文献 [22] 提议车辆将十进制的通信信道特性 (信号强度指示) 转化为二进制的链路指纹并和前一个 SHA-1 值生成新哈希, 再存储到分类账后发送到云端. 公开的分类账通过验证哈希值保证数据的可靠传输, 实现

轻量级的 V2V 通信.

3.2.2 基于区块链的车联网身份认证

在 “人 – 车 – 路 – 云” 一体化的车联网环境下, 根据认证对象、认证方法和认证行为的不同, 可将基于区块链的身份认证分为两大类: 节点认证和用户身份认证 [19].

节点认证是指对 P2P 网络节点的安全性进行认证, 过滤恶意节点, 建立安全的网络环境. 文献 [23] 通过 Gossip 协议的 Push-Pull 模式和时间序列改进拜占庭共识算法, 保证两个节点在一个周期内拥有相同的信息, 通过多次通信达成共识后, 实现对车辆节点的全局认证.

用户身份认证是对区块链用户身份合法性进行鉴别, 包括用户身份注册、身份信息存储、更新和撤销等. 目前, 基于区块链的用户身份认证机制主要分为基于密码体制、基于信息区块、基于数字代币、基于生物特征等 4 个方面.

(1) 基于密码体制的车辆身份认证. 文献 [24] 提出基于密码累加器的 PKI 密钥分发机制, 区块链和公钥机制相结合的方法判断车辆的访问资格, 设计基于 Rayleigh 共识的智能合约, 根据从数据库检索出的车辆节点的信用记录和信用等级来判断该节点是否为信任节点, 阻止恶意节点加入区块链网络. 文献 [25] 面向支持雾计算的 IoV 提出基于区块链的高效认证方案, 车辆在 TA 注册后获得身份令牌, 并基于椭圆曲线加密 (elliptic curve cryptography, ECC)、哈希函数、XOR 运算生成身份认证令牌实现与区块链管理器 (Blockchain manager, BM) 的双向认证, 同时在基于实用拜占庭容错 (practical Byzantine fault tolerance, PBFT) 共识后存储在区块链中, 保证认证的可追溯性. 文献 [26] 面向 VANET 提出基于区块链的分布式身份认证和快速撤销方案, 私有区块链存储车辆从认证权威机构 (certification authority, CA) 注册后获取的带有数字签名的伪 ID 和基于 ECC 的公私钥对, 保证验证的可靠性; 并基于身份的加密 (identity-based encryption, IBE) 实现 RSUs 和车辆双向认证和撤销, 在保证匿名性的基础上有效地提高认证和撤销效率. 文献 [27] 提出基于区块链和 ECC 的跨数据中心的车辆身份认证, 车辆通过 RSUs 基于 ECC 实现车辆和服务管理器间的相互认证, 并基于 PBFT 共识将认证结果存入区块链, 避免跨数据中心的多次认证. 文献 [28] 面向协作式智能交通系统提出基于区块链的车辆身份认证方案, 由车辆、RSUs、CA 构成的区块链存储车辆有效或撤销的证书 (包括车辆公钥和有效期), 避免单点故障; 车辆仅需检查用于消息签名的公钥是否保存在区块链中就可验证身份的合法性, 减少通信和计算开销.

(2) 基于信息区块的车辆身份认证. 文献 [29] 提出基于区块链和 RSUs 辅助的身份认证和密钥协商协议, 数据中心用于存储所有车辆的注册信息, 由 TA 组成的区块链存储认证参数, 便于实现 RSUs 辅助的基于哈希运算、异或运算和伪随机数的 TA 和车辆间的相互认证, 提高跨 TA 的认证效率. 文献 [30] 提出基于区块链的隐私保护车辆身份认证方案, 将本地注册中心视为区块链节点, 并以分布式方式管理和存储车联网身份认证信息. 车辆通过私钥向注册中心发送认证请求, 区块链基于公钥回复车辆身份的真实性, 防止恶意节点参与通信. 文献 [31] 提出基于区块链的身份认证和数据安全传输机制, 利用区块链存储注册中心分配给车联网节点签名后的伪身份标识, 并基于伪身份标识和 Diffie-Hellman 密钥协商协议生成公私钥对, 用于车联网节点的分布式身份认证和数据安全传输. 文献 [32] 提出基于隐私保护区块链的 V2X 远程认证模型, 传统网关构成的区块链存储车辆身份密钥和完整性证书, 并基于服务器生成的访问策略过程实现车联网节点的远程认证.

(3) 基于数字代币/生物特征的车辆身份认证. 文献 [33] 面向 IoV 生态系统提出基于区块链的身份和信任管理框架. 该框架包括身份标识和注册以及相互认证两个阶段. 在标识和注册阶段, 分布式标识符 (decentralised identifier, DIDs) 作为身份凭证被从欧盟的标准注册范式中获取, 并将获取的角

表 3 基于区块链的车联网访问控制对比

Table 3 Comparison of IoV/V2X access control based on Blockchain

Proposal	Description	Method	BC techno.	BC nodes	Security properties
[39]	Access control strategy based on smart contract	Smart contract deployment ABAC	Own	RSUs	Security policy
[40]	Intelligent edge-chain-enabled access control	Smart contract deployment access control based on risk prediction	Own	Vehicles, RSUs	Confidentiality, integrity, availability
[41]	Access control strategy based on smart contract	Smart contract deployment vehicle access rules	Own	BS	Reliability, credibility, immutable
[42]	Fine-grained access control scheme	Identity chain stores the private key of identity, data chain stores the decryption key of data	Own	RSUs	Reliability, availability
[43]	Location-based data access control	Deploy access control policy based on vehicle attributes and location	Public Blockchain	–	Confidentiality

色映射到 Hyperledger Indy 权限角色; 在相互认证阶段, 持有成对 DIDs 和签名密钥的车辆之间可以彼此认证. Rowan 等 [34] 提出通过可见光和超声波编码建立 V2V 通信的侧信道, 实现安全的基于区块链 PKI 的密钥交换; 包含 PKI 的 Blockstack 节点存储对称加密密钥、车辆身份哈希值和身份证书, 车辆可以通过下载副本数据并基于证书检查和视觉识别 (图像处理) 手段验证通信车辆的身份.

综上所述, 基于区块链的消息认证和身份认证取得了一定成果, 然而认证方式未考虑条件隐私性、条件可追溯性、不可链接性 [35] 等问题, 仍然需进一步的研究.

3.3 基于区块链的车联网访问控制

访问控制机制为合法主体在特定访问环境下授予相应的访问权限, 是保障数据安全的主要手段 [36]. 传统静态的访问控制模型, 如自主访问控制 (discretionary access control, DAC)、强制访问控制 (mandatory access control, MAC)、基于角色的访问控制 (role based access control, RBAC)、基于对象的访问控制 (object based access control, OBAC)、基于属性的访问控制 (attribute based access control, ABAC)、基于任务的访问控制 (task based access control, TBAC) 等难以适应车联网通信网络拓扑的高动态性, 导致当前车联网的访问控制方案灵活性不高、安全性较差. 动态授权 [37] 和风险预测 [38] 等方案未考量车联网场景的多域性, 导致不同区域的访问控制方案 “各自为政”. 区块链能够为车辆提供更多实时、安全、可扩展的资源服务, 基于区块链的访问控制策略主要包括两方面: 通过智能合约部署和订制访问控制策略, 实现对资源的可编程访问; 利用区块节点存储私钥, 保证资源的安全性. 相关文献对比表格如表 3 [39~43] 所示.

在利用智能合约构建可编程资源访问的相关研究中, 文献 [39] 提出基于智能合约和 ABAC 模型的分布式车辆访问控制模型, RSUs 组成的区块链在执行智能合约交易时将访问控制策略自动添加到资源车辆的策略列表中, 防止其他非授权车辆的资源访问. 文献 [40] 提出基于智能边缘链的 IoV 访问控制机制, 设计基于风险预测的访问控制模型, 并对区块链存储的车辆网络行为数据进行分析, 预测车辆的风险等级作为节点权限的判断标准, 从而生成相应的访问控制策略; 同时利用智能合约强制执行控制策略, 自动触发边缘 RSUs 为车辆提供动态的访问控制服务, 避免恶意车辆破坏信息共享的安全. 为增强访问控制策略的自主性, 文献 [41] 提出车辆根据租赁规则订制智能合约, 并将合约发布到由基

站构成的区块链网络上; 智能合约被节点验证后保存在区块链上并成为后台可自动运行的服务, 从而实现车辆在多个机构之间可信的权限交易.

在利用区块节点存储私钥的相关研究中, 文献 [42] 提出基于密文策略属性加密 (ciphertext policy attribute based encryption, CP-ABE) 的细粒度访问控制方案, 利用身份链存储合法用户的私钥、数据链存储数据的解密密钥, 构建具备数据安全、隐私保护特性的数据共享平台. 文献 [43] 面向基于位置的服务提出基于属性的数据访问控制方案, 支持数据所有者将加密数据提交到云服务器, 并利用区块链为满足权限要求和位置属性的车辆分发私钥. 当车辆到达指定位置并满足访问控制策略时才能获得相应的信息资源, 实现可靠、安全的信息数据访问.

综上所述, 目前基于区块链的车联网访问控制研究正处于初级阶段, 探索更多面向车联网访问控制方案, 对于车辆资源的安全合规性访问具有重要意义. 本文认为, 将传统访问控制模型中用户、角色、属性、资源、动作、权限、环境等概念 [44] 与车联网中的节点融合并关联区块链中的交易、账户、验证、合约等相关概念可衍生出更多基于区块链交易的车联网资源访问控制方案.

3.4 基于区块链的车联网信任管理

在开放、高移动性、拓扑结构动态变化的车联网中, 基于认证和访问控制的安全机制无法抵御已认证和授权的内部节点的攻击 [45]. 信任管理机制通过建立、维护、验证节点间的信任关系, 可以减少节点交互的风险, 提高系统安全性、健壮性. 现有的信任管理方法大致分为两类: 集中式的中心可信实体/服务器管理信任值 [46] 和车辆/基站分布式维护信任数据 [47]. 然而, 现有集中式信任管理方案存在可扩展性差、单点故障、验证和撤销难等问题, 分布式管理方案存在处理稀疏性、信任一致性、隐私性等问题 [48]. 区块链的高安全性、去中心化、一致性和可靠性等显著特点使其成为建立车联网实体间信任模型的最佳解决方案. 当前, 学术界针对车联网中基于区块链的信任管理研究主要集中于 3 个方面: 以数据为中心的信任管理、以实体为中心的信任管理, 以及基于混合模型的信任管理. 相关文献对比表格如表 4 [48~55] 所示.

3.4.1 以数据为中心的信任管理

以数据为中心的信任模型专注于数据信任计算, 计算数据在真实性、正确性和准确性方面的可信度. 使用以数据为中心的信任模型通常基于事件的上下文, 并考虑位置和时间的邻近度、相同事件的记录和类型. 传统以数据为中心的信任模型可分为 5 类 [48]: 基于信任报告、基于加权投票、基于多数投票、基于贝叶斯推理、基于 Dempster-Shafer 理论.

在以数据为中心的基于区块链的信任管理的研究中, Mohmand 等[1)] 提出通过基于区块链的信任管理来保护车辆间的通信, 车辆和行人基于贝叶斯推理检查消息是否可信并将结果发送到 RSUs 区块链, 区块链基于 PoW (proof of work) 和 PoS (proof of stake) 共识来判断消息的真实性并更新信任值, 实现基于信任等级的安全通信. 文献 [49] 使用区块链构建去中心化的信任管理方案, 车辆基于贝叶斯推理生成消息评级, RSUs 基于车辆节点的消息可信度评估信任偏移量, 并将信任偏移量存储到区块链上防止被篡改. 同时, 采用基于 PoW 和 PoS 的共识激励更多 RSUs 参与信任更新, 保证信任的一致性. 文献 [50] 面向基于命名数据网络 (named data networking, NDN) 的 IoV 提议使用信誉区块链来保护车辆数据转发和内容缓存, 由车辆和 RSUs 构成的区块链网络为新加入的车辆指定节点和缓存内容两个信誉值, 而数据转发车辆根据车辆兴趣包的有效性和缓存内容的可信度调整信誉值并存储在区

1) Mohmand I U R, Javaid N. Blockchain based mobile nodes in vehicular network. 2019. https://www.researchgate.net/publication/334696838.

表 4 基于区块链的车联网信任管理对比

Table 4 Comparison of IoV/V2X trust management based on Blockchain

Class	Proposal	Description	Method	BC techno.	BC nodes	Security properties
Data-centric	Mohmand	Trust management of mobile nodes based on BC	BC verifies the authenticity of the message to update the trust value	Own	RSUs	Reliability
Data-centric	[49]	BC-based decentralized trust management	After Bayesian inference generates a message rating, RSUs calculate the trust value offsets	Own	RSUs	Availability, reliability
Data-centric	[50]	Data forwarding and content caching based on BC and NDN	Reputation value based on the validity of Interest and the credibility of content	Own	Vehicles, RSUs	Privacy
Entity-centric	[51]	Intelligent vehicle commination based on BC and rewards	Authorize TrustBit based on historical information	Own	Vehicles, RSUs	Confidentiality, integrity, privacy
Entity-centric	[48]	Adaptive trust management based on smart contract	Trust value based on the validity of the message	LocalBC, GlobalBC	LocalBC: RSUs; GlobalBC: TA, CA, RA	Integrity, authenticity, availability
Entity-centric	[52]	Trust management based on consortium Blockchain	RSU calculates the trust degree based on the rating value of the evaluator	Consortium Blockchain	Vehicles, RSUs	Confidentiality, privacy
Hybrid	[53]	BC-based VANET anonymous reputation system	Vehicle reputation score evaluates message trust	Own	CA, law enforcement authority, RSUs	Privacy
Hybrid	Abbasi	Intelligent vehicle secure communication based on multilevel BC	The authenticity of the message changes the trust value	Own	Vehicles, RSUs	Reliability, availability
Hybrid	[54]	BC-based trust management	Rating summation based on weighted aggregation of the reputation value ratings	Own	RSUs	Confidentiality, integrity, traceability
Hybrid	[55]	BC-based secure message exchange	Local BC updates vehicle trust by verifying event message	Public BC, local BC	Public BC: vehicles; local BC: RSUs	Confidentiality, integrity
Hybrid	Arshad	BC-based scalable access management and trust development	Calculate trust value based on message and PoC consensus	Own	Vehicles, manager nodes	Authenticity
Hybrid	Ijaz	Decentralized BC-based reward and penalty mechanism	Trust based on message-based trust rating	Own	Vehicles, RSUs	Authenticity
Hybrid	Yousuf	BC-based decentralized incentive in trust management	Trust based on message-based trust rating	Own	–	Authenticity

块链中, 避免信誉值被篡改. 同时, 车载 NDN 通过验证车辆请求的内容名称可防止恶意车辆的内容中毒 (content poisoning)、兴趣泛滥 (interest flooding)、缓存中毒 (cache poisoning) 等攻击, 保证车载网络内容转发的安全性.

3.4.2 以实体为中心的信任管理

以实体为中心的信任模型专注于车辆的可信度计算, 车辆的可信度是车联网安全路由和可靠数据传输的基础. 常见的可信度评估方法有 4 种: 基于多属性的方法、基于基础设施评估 (RSU 推荐) 的方法、面向集群的方法、基于权重的动态实体中心信任 [48].

在以车辆为中心的基于区块链的信任管理的研究中, 文献 [51] 提出由车辆销售商/授权经销商基于车辆的事故和犯罪历史信息发行加密 ID —— TrustBit (类似于比特币) 代表车辆信任值, 并存储在由车辆和 RSUs 组成的区块链网络上, 而通信车辆则通过提供信任位来建立对通信网络的信任. 文献 [48] 提出基于区块链智能合约的自适应信任管理. 当车辆发送事件交易时, 交通管理局给车辆分配假名并通过 CA 颁发证书和初始信任值, 本地区块链验证交易的有效性后修改信任值并存储在区块节点中, 保证信任值的可靠性和一致性; 全局区块链根据车辆检测真实事件中的贡献度和准确度分配奖励, 鼓励车辆更多的良好表现. 文献 [52] 提出基于区块链的隐私保护信任管理系统, 在系统初始化阶段, 车辆在执法机构上注册验证后获得假名、初始信任值并生成 RSU 可信环境 (trusted execution environment, TEE) 的公私钥对. 在信任更新阶段, 评估器基于消息计算车辆评级值, 并使用公钥加密作为评估结果的一部分; Non-TEE 将评估结果和车辆身份排序后完成加法同态加密; TEE 使用私钥解密后得到最终信任值. 当车辆意识到身份暴露时, 可向 RSUs 区块链发送假名更新请求, TEE 广播该请求并在验证通过后将更新的假名存入区块链, 有效地保护了车辆的身份隐私.

3.4.3 基于混合模型的信任管理

混合信任模型利用车辆的可信度来评估数据的信任值或利用数据的可信度来评估车辆的信任值, 即信任评估是根据车辆和数据的可信度交换进行的.

在利用车辆的可信度来评估消息的信任值的研究中, 文献 [53] 面向 VANET 提出基于区块链的信任管理匿名信誉系统, 依靠车辆的信誉评分来确定广播消息的信任级别, 减少虚假消息的传播. 同时构建 MesBC (Blockchain for messages) 区块链用于保存所有广播消息作为车辆信誉的持久性证据, 避免发布恶意车辆信息时发生争议; 构建 CerBC (Blockchain for certificates) 和 RevBC (Blockchain for revoked public keys) 两个区块链, 分别为发行证书提供存在证明和已撤销的公钥提供缺席证明, 确保车辆匿名身份认证的真实性.

在利用消息的可信度来评估车辆的信任值的研究中, Abbasi 等[2)] 采用分配通信车辆 ID 和初始信任值, 并基于车辆间共享消息的真实性更改信任值的方式, 实现可靠的车辆通信网络; 并采用本地动态区块链存储所有信任值和消息, 主区块链存储更新信任值的方式极大地减少时延, 提高了系统的整体性能. 文献 [54] 提出基于区块链的 IoV 信任管理方案. 车辆基于消息可信度和贝叶斯推理计算其他车辆的消息评级, 并采用椭圆曲线数字签名算法 (elliptic curve digital signature algorithm, ECDSA) 加密后转发给 RSU. RSUs 区块链根据基于评级的加权聚合声誉算法计算信誉更新值, 并通过基于 PoW 和 PoS 共识机制存储信誉变化大的车辆信誉值, 有效地检测和识别恶意车辆, 同时采用降低信誉值的方法削弱恶意车辆对系统的影响. 文献 [55] 面向 VANET 提出基于区块链的消息安全交换方案, 公有链存储所有节点信任值和消息的可信度, 本地链存储车辆完整信任信息和事件消息的历史记录. 当车辆广播事件消息时, 本地链基于位置证明证书验证事件消息是否真实, 并聚合真实性数据更新车辆的信任值, 保证安全可靠的事件消息交换.

此外, 为激励更多车辆加入信任管理系统中, Arshad 等[3)] 在基于区块链的可扩展智能交通系统 (intelligent transport system, ITS) 中的车辆访问过程中, 提议响应车辆基于协助证明共识机制判断请求消息的正确性, 并将结果转发给管理器节点来判断车辆信任值的增减, 以激励更多的车辆加入信任

2) Abbasi S N, Javaid N. Multilevel Blockchain technology in intelligent vehicle. 2019. https://www.researchgate.net/publication/334697995.

3) Arshad M U, Javaid N. Blockchain-based scalable access management and trust development for ITS in smart city. 2019. https://www.researchgate.net/publication/334696671.

消息的提供. Ijaz 等[4] 提出基于分布式区块链的车辆奖惩机制, RSUs 区块链网络在基于消息可信度生成的信任评级的帮助下生成车辆的信任值, 并根据信任值的正负奖励或惩罚车辆, 激励更多车辆发送真实信息, 提高通信网络的安全性. 类似地, Yousuf 等[5] 在车辆信任管理中使用区块链实现分布式激励机制, RSUs 充当本地存储系统存储评级 "+1" 的车辆信息, 区块链存储评级持续 "−1" 的车辆信息, 并惩罚车辆共享信息无效, 激励更多的车辆分享真实信息.

综上所述, 区块链通过分布式地维护/更新车辆/消息信任值的方式保证车联网信任管理的可靠性、可用性和一致性. 当前的研究虽取得一定进展, 然而在共识资源消耗大、信任模型对经验数据依赖性强且兼容性差的车联网中, 仍需进一步探索具备通信时延低、计算开销低、可扩展性高等特性的信任管理方案.

3.5 基于区块链的车联网隐私保护

车联网隐私保护可以防止车辆/用户的敏感信息 (驾驶者的姓名、车辆牌照、行驶速度、车辆当前位置、车辆行驶路径等) 被泄露. 这些敏感信息泄露的缘由主要来自两个方面 [56]: 车辆广播的 Beacon 消息包含大量的隐私信息; 车辆运动轨迹具有可预测性. 目前, 车联网身份隐私保护多采用匿名认证的方案, 位置隐私保护多采用基于模糊、混合区域、k 匿名的方案 [56]. 然而, 上述方案未解决单点故障、服务不稳定的问题, 区块链以分布式、透明、不可篡改的方式记录各方的交易 (例如, 交通控制 [57]、停车服务 [58]、拼车服务 [59]、vehicle-to-grid 支付 [60]), 为车联网隐私保护提供新的解决方案. 现有基于区块链的车联网隐私保护研究主要包含身份隐私保护和位置隐私保护.

3.5.1 基于区块链的车辆身份隐私保护

在高移动性、多节点的车联网环境下, 基于区块链的车辆身份隐私保护的研究主要分为基于匿名认证和基于假名两类, 相关文献对比表格如表 5 [61~70] 所示.

(1) 基于匿名 (anonymous) 认证的车辆身份隐私保护. 现有基于匿名认证的车辆身份隐私方案多采用加密、加噪、混合等方式处理身份标识, 使得恶意节点无法获得车辆真实身份. 然而, 集中式匿名认证方案易遭受中心实体性能瓶颈和单点故障问题; 同时, 匿名认证的车辆广播网络存在缺乏回复消息热情的问题, 区块链去中心的特性和经济激励机制为上述问题提供了解决思路.

针对集中式认证出现的单点故障问题, 文献 [61] 面向 VANET 提议驾驶员基于车辆信息在根信任机构注册后得到公私钥、系统密钥, 并将指纹等生物特征存储在根区块链中, 有效地保护车辆的真实身份. 同时, 车辆在本地信任机构管理的区域中使用生物特征来认证身份的真实性, 在认证成功后生成消息哈希值并和前一个块的哈希值连接起来, 并使用私钥和系统密钥先后加密消息哈希后广播到网络中, 本地区块链节点使用公钥解密并判断前一个区块的哈希值是否相等可实现消息认证. 文献 [62] 面向车辆雾服务提出基于区块链和雾计算的轻量级匿名认证方案, 车辆在审计部门基于椭圆曲线加性循环群的系统参数中随机选择整数作为私钥的一部分, 并使用私钥加密身份信息发送给审计部门, 审计部门使用自身公钥加密身份信息, 保证车辆真实身份的隐私性. 当服务管理器在审计部门注册后获得审计部门的公钥并实现对车辆的身份认证, 认证结果在见证节点的基于 PBFT 共识后存入区块链, 保证真实身份的可追溯性和不可否认性. 文献 [63] 面向乘车协作服务提出基于区块链和车辆雾计算的隐私保护方案, CA 为服务提供商们提供系统组公私钥, RSUs 雾节点在本地实时收集乘车请求和响

4) Ijaz A, Javaid N. Reward and penalty based mechanism in vehicular network using decentralized Blockchain technology. 2019. https://www.researchgate.net/publication/334644810.

5) Yousuf A, Javaid N. Decentralized incentive based trust management in vehicles using Blockchain technology. 2019. https://www.researchgate.net/publication/334696097.

表 5 基于区块链的车联网身份隐私保护对比

Table 5 Comparison of IoV/V2X identity privacy preservation based on Blockchain

Class	Proposal	Description	Method	BC techno.	BC nodes	Security properties
Anonymous	[61]	BC-based distributed message authentication	Biometric-based authentication	Private Blockchain	Vehicle, RSUs, root and local TA	Integrity, non-repudiation, traceability
Anonymous	[62]	BC-assisted anonymous authentication	AD re-encrypts vehicle's private key encrypted identity	Consortium Blockchain	Service managers, witness peer	Confidentiality, integrity, traceability, non-repudiation
Anonymous	[63]	Anonymously identity authentication based on BC and vehicular fog computing	RSU authenticates the identity of service provider group public key encryption	Consortium Blockchain	Service providers	CIA, unlinkability, traceability, auditability
Anonymous	[64]	BC-based incentive announcement system	Use the address of Ethereum as an identity	Ethereum	–	Reliability
Anonymous	[65]	Privacy-preserving BC-based incentive announcement network	Threshold ring signature guarantees the identity of witness vehicle	Own	RSUs	Unlinkability, traceability, reliability
Anonymous	[66]	BC-based anonymous Ad dissemination	Anonymous credential based on ZKPoK	Own	RSUs	Anonymity, conditional linkability
Pseudonym	[67]	Privacy-preserving authentication based on EC and BC	One-time pseudonyms based on elliptic curve	Consortium Blockchain	–	Integrity, non-repudiation, traceability, forward and backward security
Pseudonym	[68]	BC-based authentication and privacy preservation	BC stores pseudonym ID for authentication	Ethereum	–	Confidentiality, integrity, traceability
Pseudonym	[69]	BC-based privacy preservation multimedia sharing	BC stores pseudonym and signature information	Ethereum	–	Confidentiality, integrity, traceability, reliability
Pseudonym	[70]	BC-based privacy authentication and message dissemination	Private BC stores pseudo-identity	Private BC, public BC	Private BC: TA; public BC: RSUs	Traceability, revocability, non-repudiation

应, 并验证由所有服务提供商公钥加密的车辆身份真实性以及数据完整性, 再将加密的协作服务数据上传到服务提供商; 服务提供商构建联盟区块链并基于智能合约匹配乘客和司机, 保存交易和协作服务数据的哈希值, 实现服务数据的可追溯性.

针对车辆广播网络中节点回复消息不积极的问题, 文献 [64] 提议请求车辆使用以太坊地址 (公钥) 作为匿名身份来发送广播请求, 防止身份信息泄露, 并将报酬存放在区块链上; 区块链 Bloom 过滤器对基于签名的见证消息进行认证, 并通过智能合约支付报酬给见证车辆、支付服务费给 RSUs 的激励方式鼓励更多见证车辆加入公告网络. 文献 [65] 面向车载广播网络提出基于区块链的隐私保护激励公告系统 —— CreditCoin, 设计 Echo-Announcement 公告协议, 当车辆见证事件后可发见证请求包, 见证车辆发送基于部分环签名的回复包同意加入, 并将基于门限环签名的公告聚合数据广播到网络中以验证事件的真实性; 同时设计基于区块链的激励机制, 通过消费一定硬币的方式鼓励更多的车辆参与真实公告的转发. 针对车载网络广告传播面临的 "搭便车" 攻击 (车辆串通欺骗广告商), 文献 [66] 提出基于区块链的匿名广告传播方案, 车辆和广告商在注册机构注册获得各自的密钥和证书; 广告商

表 6　基于区块链的车联网位置隐私保护对比

Table 6　Comparison of IoV/V2X location privacy preservation based on Blockchain

Class	Proposal	Description	Method	BC techno.	BC nodes	Security properties
Encryption	[71]	BC-based location privacy-preserving spatial crowdsourcing	OPE-based location encryption	Own	RSUs	Confidentiality
K-anonymous	[72]	BC-based LBS privacy preserving trust model	Construct cloaking region to protect vehicle's position	CerBC, ReqBC	RSUs	Conditional anonymity
K-anonymous	[73]	BC-enabled trust-based location privacy preservation	Construct cloaking region to protect vehicle's position	Consortium Blockchain	RSUs	Authenticity

收到有效证书后选定 RSU 将广告摘要信息发布到名为 "Ad dissemination" 的智能合约中; 车辆 A 使用基于非交互式 ZKPoK (zero-knowledge proof of knowledge) 的身份匿名凭证传播广告, 车辆 B 使用 ZKPoK 响应并将传播证明上传到区块链, 保证广告传播的匿名性和条件链接性; 而由 RSUs 组成的区块链基于哈希树和智能合约实现 "广告接收证明" (proof of Ad receiving, PoAR) 的特性, 保证广告传播的正确性; 同时使用智能合约支付预定义的奖励, 保证奖励支付的公平性.

(2) 基于假名 (pseudonym) 的车辆身份隐私保护. 假名机制是匿名机制上的一种演变, 其通过可信中心/权威机构为车辆颁发假名身份来代替真实身份, 使其他节点无法获取其真实身份, 并兼顾假名和真实身份间的不可关联性, 可有效保护车辆的身份隐私. 基于区块链和假名认证的车辆身份隐私保护方案利用不可伪造的区块结构存储和分发车辆的伪标识, 确保认证的可靠性和隐私性.

在基于假名机制的车辆身份隐私保护的研究上, 文献 [67] 面向车辆通信提议信任机构基于椭圆曲线参数为其随机生成一次性假名隐藏身份识别码, 实现车辆身份的隐私保护; 并使用联盟区块链对边缘通信数据进行审核、验证, 并将验证通过的数据记录在区块链中, 保证数据的可追溯性; 同时采用基于身份的聚合签名实现消息认证, 保证数据的完整性.

在基于区块链和假名认证的车辆身份隐私保护的研究上, 文献 [68] 提议车辆使用原始 ID 在注册服务器上注册得到伪 ID, 并基于与注册服务器的椭圆曲线 Diffie-Hellman 密钥协商得到会话密钥; 注册服务器将交易信息 (交易类型、车辆伪 ID、共享秘密信息、会话详细信息、车辆公钥) 添加到区块链中. 当车辆访问服务时, 先向服务提供商发送服务请求和数字签名, 服务提供商根据区块链中的伪 ID 进行身份认证, 并根据数字签名的真实性授权车辆的访问权限. 文献 [69] 面向车载社交网络提出 TA 使用伪随机函数为用户/车辆/RSU 生成伪标识和公私钥对, 用户/车辆/RSU 将假名和哈希加密的多媒体数据发给 TA, TA 将认证通过的交易 (包括假名、公钥、加密数据、签名信息) 发布到区块链, 有效地保证车辆身份隐私和多媒体共享数据的完整性、可追溯性. 文献 [70] 面向 VANET 提出由 TA 组成的私有链存储真实身份和伪身份标识, 以支持特定区域的身份认证, 保证身份认证的隐私性和可靠性; 同时, 由 RSUs 组成的本地链存储诸如交通拥堵等事件消息, 保证消息传播的安全性.

3.5.2　基于区块链的车辆位置隐私保护

车辆位置隐私泄露使得攻击者很容易跟踪目标车辆, 进而推断出用户的运动轨迹, 严重影响车辆的驾驶安全. 当前, 在基于区块链的车辆位置隐私保护的研究中, 基于加密和基于 k 匿名的方案成为主流研究热点. 相关文献对比表格如表 6 [71~73] 所示.

(1) 基于加密的车辆位置隐私保护. 基于加密的位置隐私保护利用加密算法对车辆的位置信息进行加密, 使得其他节点难以获得车辆的真实位置信息. 文献 [71] 面向基于车辆的空间众包 (spatial

crowdsourcing, SC) 应用提出使用区块链实现分布式的位置隐私保护. 在位置记录阶段, 工作车辆基于保序加密 (order-preserving encryption, OPE) 自身位置并通过 RSU 将包含密文哈希值的位置记录保存在区块链中; 在任务提交阶段, 服务请求者向区块链发送基于加法同态加密 (additively homomorphic encryption, AHE) 的任务请求 (包含任务描述、位置策略、奖励策略). 车辆根据位置策略密文验证并确定是否可参与任务. 在任务解决阶段, 工作车辆将任务数据和基于 OPE 以及非交互式零知识证明生成的位置证明发给区块链, 请求者在验证车辆提交的位置密文和区块链位置密文一致性后, 通过区块链为车辆分发奖励.

(2) 基于 k 匿名的车辆位置隐私保护. 车辆在享受基于位置的服务 (location based services, LBS) 带来便利的同时也要承担位置信息泄露的风险 (服务提供商滥用位置数据), 基于 k 匿名的位置隐私保护使用 k 个参与者的位置构建匿名隐身区域, 使得车辆在匿名隐身区域与至少 "$k-1$" 个参与者联系, 有效地保护车辆的位置隐私. 文献 [72] 在空天地一体化网络的辅助下提出基于区块链的 LBS 隐私保护信任服务方案. 车辆在注册权威 (register authority, RA) 机构注册后获得身份数字证书, RSUs 构成的区块链在验证证书的合法性后存储该证书, 而 RA 存储真实身份, 实现车辆身份的条件匿名性; 当车辆发起服务请求时, RSU 通过基于历史信息的信任评估算法评估车辆行为, 并选择 "$k-1$" 个合格信任值的诚实车辆的虚拟位置构建 k 匿名隐身区域, 然后将服务请求和隐身区域提交给服务提供商, 有效保证车辆的位置隐私. 文献 [73] 提议车辆在 RA 上注册获得假名和初始信任值, 并以交易账单的形式存储在 RSU 区块链上, 以便车辆随时查询信任值. 在构建隐身区域时, 车辆结合基于狄利克雷分布的历史信任记录和当前行为计算合作车辆信任值, 并将车辆到期的假名和新的信任值发送给 RSU, 实现构建可信隐身区域过程中的车辆位置隐私.

区块链分布式存储和管理的特性给车辆隐私保护方法带来新的研究思路. 结合现有文献来看, 基于区块链的车辆隐私保护研究仍处于初级阶段, 缺乏对条件隐私保护方案的探讨. 同时, 结合新兴隐私保护技术 (安全多方计算、机密计算、差分隐私 [74] 等) 可以探索更多基于区块链的车联网隐私保护方案.

总体而言, 在多应用场景接入的 "人 – 车 – 路 – 云" 车联网环境下, 构建安全保障体系对于车联网产业健康发展至关重要. 当前, 基于区块链的车联网安全关键技术的研究正如火如荼地进行, 综合现有文献来看, 密钥管理是车联网安全的基础, 认证机制、访问控制、信任管理、隐私保护共同支撑车联网通信安全、数据安全、应用安全体系建设, 推动新型车联网安全体系架构的演化和发展.

4 基于区块链的车联网通信安全

车联网通信 (车内通信不在本文讨论范围) 安全是数据安全的基础, 其安全风险来源于车联网架构中的云平台、移动终端和路基设施等组成部分以及通信网络协议 [4, 75]. 基于区块链的认证机制和信任管理可以有效识别恶意节点, 避免虚假/恶意消息的传播, 在一定程度上保证了车联网通信安全. 然而, 区块链技术固有的缺陷, 例如: 智能合约漏洞、共识过程的资源消耗等, 给车联网通信安全及性能带来一定的阻碍. 现有研究从减少智能合约漏洞、优化共识机制和提升网络性能等方面提出可行性解决方案.

针对智能合约漏洞 (以太坊的 solidity 语言漏洞、交易顺序依赖、时间戳依赖、可重入性等) 引发的 IoV 恶意攻击的问题, 文献 [76] 提议采用朴素贝叶斯分类器预测车辆节点的请求内容, 并使用自然语言处理 (natural language processing, NLP) 进行智能合约的自动编码, 实现 smart contract 到 intelligent contract 的转变, 确保请求的智能决策, 进而实现高性能、安全的 V2X 网络通信.

在对共识机制改进优化的研究中, 文献 [77] 面向车载社交网络提出基于私有链和公共链的轻量级共识协议. 在私有链上, 本地车辆在可靠/不可靠的两种通信链接下交换投票, 并就车辆传感数据真实性的达成共识/生成投票区块结构, 再随机选择节点将共识结果上传至 RSU 公有链/服务器; 服务器检查投票签名的数量是否超过阈值和签名分组的正确性达成共识结构并上传至 RSU 公有链. 文献 [78] 利用高性能区块链共识算法构建安全的 IoV 通信系统, RSUs 组成的区块链用于存储路由数据和交易数据, 避免窃听、重播和错误数据注入等攻击. 而高性能区块链共识算法主张主区块节点创建新区块, 并基于拜占庭机制将区块生成消息广播到其他区块节点以达成共识, 减少系统的计算资源, 增大区块链网络的吞吐量.

在提升车联网通信网络性能的研究中, 文献 [79] 提议在 IoV 系统中启用支持软件定义网络 (software defined network, SDN) 的 OBUs (on board units)、RSUs、基站, 利用联盟区块链实现车辆分布式注册和验证, 并基于车辆消息的信任权重判断可信度; SDN 控制器用于分配资源、管理资源移动和移动策略, 实现高效的网络控制流程; RSUs 和基站等基础设施形成雾节点在边缘进行数据的处理和存储, 降低数据传输的丢包率和时延. 文献 [80] 提出基于有向无环图 (directed acyclic graph, DAG) 和博弈论的 V2V 通信架构, 利用 IOTA 共识机制达成交易序列, 并采用有向无环图数据结构存储 P2P 网络中的交易, 提高 V2V 信息传输速率; 同时, 利用博弈论映射卸载服务的提供者和使用者, 实现成本最优的服务交易. 文献 [81] 使用深度强化学习选择区块生产者, 并动态调整区块大小和区块生成间隔, 最大化区块交易吞吐量, 满足动态多变的 IoV 应用场景.

总体而言, 区块链固有的技术缺陷给车联网高效安全通信带来一定的阻碍, 新兴 AI 技术、SDN 网络架构, 以及 DAG 技术在区块链网络上的安全性、可扩展性, 以及连通性的研究正处于初级阶段, 给基于区块链的车联网通信安全带来新的研究路线.

5 基于区块链的车联网数据安全

车联网数据主要包括基础属性类数据、车辆工况类数据、环境感知类数据、车控类数据、应用服务类数据、用户个人信息 [82] (本节仅涉及环境感知类数据、应用服务类数据). 当前, 车联网数据安全威胁来源于两个方面 [83]: 具有巨大经济价值的车联网数据交易遭受窃取、滥用; 车辆数据共享打破传统数据管理的边界, 数据所有者难以控制其他实体对数据的访问控制. 区块链由于其分布式存储、不可篡改等特点, 提升了车联网数据的共享安全. 本节从基于区块链的车联网数据交易安全和基于区块链的车联网数据共享安全展开论述.

5.1 基于区块链的车联网数据交易安全

车辆收集的关于其他车辆、道路及周边有价值的数据, 例如, 娱乐视频、道路维护信息、停车场占用情况 [84] 等, 可以在车联网实体间实施交易, 使得多个组织 (买方、卖方和中间人) 受益 [85]. 为解决交易信息透明度低、非法数据篡改和支付纠纷等问题, 现有研究通过引入区块链来实现分布式数据交付和分布式数据存储, 有效地保证交易数据安全. 相关文献对比表格如表 7 [84~91] 所示.

针对利用区块链实现车联网数据分布式交付保证交易安全的研究, 文献 [86] 提出基于区块链的分布式智能车辆生态系统安全架构, 利用区块链簇头 (cluster heads, CHs) 实现交易数据的分布式验证, 提高车辆生态系统的安全性, 而车载存储设备保存隐私敏感数据, 保证用户的隐私性. 文献 [87] 提出基于区块链的消息安全传递架构, 利用区块链在车辆间分发 V2V 警告消息 (紧急电子制动灯警告、前方碰撞警告、交叉路口移动辅助消息、车道变更/盲点警告), 克服集中式通信对中央服务器的依赖. 同

表 7 基于区块链的车联网数据交易安全对比

Table 7 Comparison of IoV/V2X data transaction security based on Blockchain

Proposal	Description	Method	BC techno.	BC nodes	Security properties
[86]	Smart vehicle architecture based on BC	Overlay block manager verifies the public key signature of the transaction	Own	Vehicles, original equipment manufacturers, service providers	Confidentiality, integrity
[87]	Message distribution based on BC	Use BC to rate the credibility of message source	Own	Vehicles	Authenticity
[88]	Vehicle communication system using Ethereum	BC application manages communication	Ethereum	–	Confidentiality, integrity, availability, consistency, immutability
[89]	BC-based smart IoV architecture	P2P network establishes secure and open communication	Own	Vehicle-related authorities	Confidentiality, privacy
[85]	BC-based data trading	RSUs verify transaction information	Consortium Blockchain	RSUs	Integrity, reliability
[90]	A hierarchical BC aided proactive caching	Top-Chain audit, Ground-Chain verification	Consortium Blockchain	Top-Chain: BS; Ground-Chain: RSUs, vehicles	Integrity
[84]	Content caching based on DRL and permissioned BC	DRL approach to learn dynamic network topology and time-varying wireless channel condition	Permissioned Blockchain	Base station	Traceability, privacy
[91]	Zero-knowledge proof and BC-based anonymous data transaction	Anonymous transaction based on zk-SNARK and smart contract	Bitcoin	Vehicles	Anonymity, authenticity

时区块链也为车辆分配信誉值以区分 “正常” 和 “恶意” 车辆, 保证消息传递时车辆身份的真实性. 文献 [88] 利用以太坊平台建立分布式车辆通信系统, 中央服务器通过区块链云和车辆建立安全通信, 实现车辆、基础设施和智能交通系统其他参与者的数据安全交互. 文献 [89] 提出基于区块链的智能 IoV 架构, 构建由地区运输办公、交通管理、车辆认证、车辆保险、政府等机构组成的区块链网络, 通过对等网络实现安全透明的 V2X 通信. 文献 [85] 使用联盟区块链实现透明安全的数据交易. 当车辆向 RSU 发起交易请求时, 由 RSUs 构成的区块链在验证身份真实性后使用布隆过滤器快速排除重复数据并存储交易信息, 再基于智能合约实现自动付款, 保证交易的透明性和公平性.

针对利用区块链实现车联网数据分布式存储保证交易安全的研究, 文献 [90] 提出一种基于分层区块链的数据缓存方案. 车辆感知周围事件信息, 并传输到通信范围内的 RSU, RSUs 构成的 Ground-Chain 基于智能合约对交易信息进行审核, 基站构成的 Top-Chain 验证交易的签名以达成共识, 并将交易记录存储到 Ground-Chain 的分类账本中, 保证数据缓存的完整性和一致性. 为解决车辆高移动性和动态无线信道在设计最优内容缓存策略的不匹配问题, 文献 [84] 提议使用深度强化学习 (deep reinforcement learning, DRL) 和许可区块链实现分布式内容缓存. 具体来说, 认证中心基于椭圆曲线数字签名算法和非对称密码技术为车辆和基站分配身份信息和密钥, 保证车辆的身份隐私; 车辆发送缓存交易请求时, 基站在验证身份合法性后基于智能合约进行内容交付, 并将交易记录保存在区块链中, 保证交易的可追溯性; 同时, 基站利用深度强化学习预测 V2V 传输访问和连接时间, 并基于实用性证明共识执行缓存匹配决策最大化内容缓存. 为保证交易参与者和交易数据的匿名性, 文献 [91] 提

表 8 基于区块链的车联网数据共享安全对比

Table 8 Comparison of IoV/V2X data sharing security based on Blockchain

Proposal	Description	Method	BC techno.	BC nodes	Security properties
[93]	Autobiography sharing of smart cars based on BC	BC stores the autobiography of the vehicle	Public chain	Vehicles, service center, car vendor, government agency	Confidentiality, authenticity, integrity, privacy
[92]	Consortium BC-based data sharing	Proxy re-encryption realizes trusted data sharing	Consortium Blockchain	Service sectors, RSUs	Confidentiality, integrity, non-repudiation
[94]	BC-based trust management and data sharing	Smart contract ensures data provenance and data integrity	Own	RSUs	Reliability, integrity
[95]	BC-based event-information sharing	BC stores verified event messages	Own	RSUs	Reliability, integrity
[96]	BC-based vehicle data sharing	Decoupled block structure	Permissioned Blockchain	RSUs	Integrity, privacy, non-repudiation
[97]	BC-based asynchronous federated learning for secure data sharing	Vehicles are trained on the local DAG, and the Blockchain is globally aggregated	Hybrid Blockchain	Permissioned BC: RSUs; DAG: vehicles	Reliability, privacy
[98]	BC-enabled federated learning for knowledge sharing	Ground-Chain integrates vehicle and local training results into Top-Chain	Top-Chain, Ground-Chain	Top-Chain: BS; Ground-Chain: RSUs	Integrity, reliability
[99]	Data sharing based on DPoS consensus	Optimizing consensus management using reputation and contract theory	Own	Vehicles	Traceability
Wang	Permissioned BC-based resource sharing	Reputation-based PBFT consensus	Permissioned Blockchain	Vehicles	Traceability

议使用区块链超级节点基于卖方传输的交易数据生成卖方地址公钥和数据哈希值, 并通过使用拜占庭容错达成共识后存储在公有链中, 保证交易数据的真实性; 买方在基于 zk-SNARK (zero-knowledge succinct non-interactive argument of knowledge) 验证交易后通过智能合约完成匿名支付.

5.2 基于区块链的车联网数据共享安全

车辆之间共享的诸如轨迹、交通信息和多媒体等数据可以有效改善驾驶体验和服务质量. 然而, 现有车辆数据共享面临着两个关键挑战 [92]: 首先, 现有的数据共享方案过于集中化, 存在单点故障、可扩展性差等问题; 其次, 恶意节点共享的虚假消息严重危害汽车驾驶效率和安全性. 基于区块链的车联网数据共享安全研究主要表现在两方面: 利用区块链存储技术实现分布式数据共享安全; 利用区块链安全机制保证数据共享的效率和安全性. 相关文献对比表格如表 8 [92~99] 所示.

在利用区块链技术实现车联网数据分布式安全共享的相关研究中, 文献 [93] 引入汽车自传 (autobiography) 的概念来记录汽车寿命周期内的数据, 并将加密的自传快照存储在以智能合约为中心的区块链中, 为智能汽车所有者提供安全、透明和可审计的数据共享. 文献 [92] 提出基于联盟区块链的智能交通数据安全共享方案, 利用联盟区块链存储车载数据, 防止单点故障和数据垄断; 服务部门利用基于属性的代理重加密算法根据车载单元的关键字和属性集控制数据访问权限, 防止串通攻击, 实现安全可信的数据共享. 文献 [94] 面向 VANET 提出基于区块链的信任管理和数据共享方案, 车辆在作为 CA 的 RSU 上注册获得基于物理不可克隆函数的加密指纹, 保护通信的身份隐私; 由 RSUs 构成

的区块链网络为车辆分配公私钥用于通信的加密, 并保存车辆注册证书. 同时, 智能合约 SC1 (smart contract one) 检查证书的有效性, 保证数据来源的可信, 智能合约 SC2 (smart contract two) 则实现数据的自动存储和检索, 保证数据共享的完整性. 文献 [95] 提出基于区块链的车辆安全事件数据共享方案, 集中式云服务器存储车辆身份、RSUs 身份、RSUs 密钥对, 以及车辆的临时身份, 而由 RSUs 构成的区块链存储车辆的真实身份和临时身份. 在安全事件共享时, 车辆在邻近的 RSU 上注册, 云服务器基于其他证实车辆的身份和真实车辆确认事件消息的真实性, RSU 在收到云服务器的确认消息后, 将事件消息、车辆/RSU 的 ID 保存在新区块中, 保证数据共享的安全性.

为提高车联网数据共享的效率和智能性, 文献 [96] 面向智慧城市提出将区块结构解耦的数据共享方案, 将许可区块链的区块头与区块体分离, 从而允许数据快速添加到区块体中, 缩短新区块创建的时间, 实现车辆和 RSUs 间的快速数据共享. 同时, 一些研究也探索了将 AI 和区块链结合的方法. 文献 [97] 提议将混合区块链和联邦学习结合到 IoV 中提高区块计算效率和数据共享的可靠性. 具体来说, 采用基于 Actor-Critic 的深度强化学习选择资源较多的车辆节点在本地 DAG 将模型参数和数据共享事件进行异步训练并执行本地聚合, RSUs 基于本地模型进行全局聚合并在验证后添加到许可区块链中, 保证共享数据的可靠性. 由于常见的联邦学习模型未考虑异构交通区域的数据特征, 文献 [98] 提出基于分层区块链的联邦学习知识共享系统, 多个 Ground-Chain 记录各 RSUs 收集的车辆节点训练的本地模型, Top-Chain 将 RSUs 的训练结果和本地训练结果整合到区块交易中, 提高知识共享的可靠性和安全性.

由于区块链中存在矿工投票勾结和验证共谋的攻击, 难以保证可靠的数据共享. 对此, 文献 [99] 提出基于增强委托权益证明 (delegated proof-of-stake, DPoS) 共识的数据共享方案, 车辆基于多权重主观逻辑模型计算 RSUs 的信誉值并存储在区块链中, 当 RSU 的信誉值高于信誉阈值时即可成为矿工候选者参与共享数据区块的验证; 进一步地, 该方案利用合同理论激励信誉较高的候选矿工参与共识投票过程, 防止旷工内部串通, 支持安全的 P2P 车辆数据共享. Wang 等 [100] 面向停车资源共享提出基于多权重主观逻辑的 PBFT 共识机制, 根据历史交互信息和车辆推荐意见计算停放车辆的信誉值. 类似于文献 [99] 中的做法, 该方案利用服务提供商选择信誉较高的停放车辆节点, 并基于 PBFT 共识参与区块验证; 同时, 服务提供商使用基于合同理论的激励机制促进更多停放车辆参与存储资源共享服务, 最大化停放车辆的效用.

总体而言, 基于区块链的车联网数据安全依赖区块链基础架构中数据层相关的哈希函数、数据加密、零知识证明等技术, 保证数据在交易和共享过程中的安全. 综合现有文献来看, 现有研究尚未考虑数据在采集、传输、使用、迁移和销毁等过程中面向数据全生命周期的安全保护机制, 无法满足数据在处理、共享、使用等业务流程中的保密性、完整性、可用性需求, 使得用户在访问车联网应用时仍然面临一定的风险, 需对此作进一步研究.

6 基于区块链的车联网应用安全

车联网是实现 ITS 和自动驾驶的核心组成部分, 也是未来智慧城市的重要组成部分. 区块链引入到车联网中可以提升车联网应用的效率、可扩展性、安全性. 本章根据需求对象不同, 将现有基于区块链的车联网应用安全分为 3 类: 车辆管理安全、交通管理安全、事故取证安全.

6.1 区块链辅助的车辆安全管理

车辆管理主要是对车辆和驾驶员进行技术监督和安全管理, 包括车辆档案管理、驾驶员档案管理、

表 9 基于区块链的车辆安全管理对比

Table 9 Comparison of vehicle security management based on Blockchain

Class	Proposal	Description	Method	BC techno.	BC nodes	Security properties
Vehicle using security	[102]	BC-based firmware update for AVs	Smart contract defines firmware update access strategy	Consortium Blockchain	Vehicle manufacturer	Authenticity, integrity, availability, reliability
Vehicle using security	[103]	Car-sharing control based on smart contract and BC	Smart contract defines car sharing	Ethereum	BS	Immutability, reliability, integrity
Vehicle using security	[104]	BC-based parking payment	Ethereum-based payment program	Ethereum	–	Integrity, confidentiality, immutability
Vehicle driving security	[105]	A secure priority vehicle movement based on BC	BC stores location and path information	Own	Authority, RSUs	Privacy, integrity
Vehicle driving security	[106]	BC-based tracking system for car actions	ECDSA guarantees the integrity of vehicle driving information	Exonum-based BC	–	Integrity, confidentiality
Vehicle driving security	[107]	Vehicle platooning based on path information matching and BC	Payment for platooning service based on smart contract	Own	Vehicles, RSUs	Privacy, integrity

行车安全管理、用车记录管理等方面, 其目的在于提升车辆使用效率和驾驶安全. 当前, 研究者将区块链技术引入到车联网中构建去中心化车辆管理系统 [101], 保证用车安全和行车安全, 极大地提高了车辆安全管理力度. 相关文献对比表格如表 9 [102~107] 所示.

在基于区块链的用车安全相关研究中, 由于现有固件更新、汽车共享、智能共享停车方案均采用客户端 – 服务器模式, 存在单点故障问题. 对此, 文献 [102] 提出基于区块链的自动驾驶汽车 (autonomous vehicles, AVs) 固件更新方案, 由车辆制造商组成的联盟链通过编写固件更新相关的智能合约, 保证固件更新内容的完整性和真实性, 并利用基于属性的加密技术支持制造商设置访问策略, 防止未授权的固件更新请求. 文献 [103] 提出基于智能合约和区块链的汽车共享控制方案, 基站构成的以太坊节点代替集中式的第三方服务器共同承担数据存储和计算, 并利用智能合约实现对车辆的动态管理和访问控制. 文献 [104] 设计基于区块链的停车共享智能支付平台, 使用以太坊平台 TESTNET Ropsten 上的智能合约管理车辆通信和停车支付, 保证车辆管理系统、停车支付系统、车辆通信系统的安全性.

在基于区块链的行车安全的相关研究中, 文献 [105] 提出基于两层区块链的专用车辆优先通行系统, 授权区块链根据共识协议的票据完成 RSUs 的注册验证, RSU 在对车辆身份进行验证后将车辆生成的诸如交通拥堵、道路状况等位置和路径信息存储在 RSUs 区块链中, 以支持专用车辆 (例如: 救护车、警车、军用车辆等) 查询信任位置、评估路线移动的可信度, 确保专用车辆的安全行驶. 文献 [106] 提出基于区块链的 AVs 行为跟踪系统, 利用椭圆曲线数字签名算法对车辆行驶信息进行完整性保护后存储在区块链中, 避免信息被篡改. 为提高道路车辆的行驶效率, 减少交通事故, 文献 [107] 提出基于区块链和路径信息匹配的 AVs 编队行驶方案, 将路径匹配成功的车辆分组在同一编队, 并利用基于信誉值的排头选择方法激励车辆成为编队头, 有利于初始编队队列的形成; 同时, 车辆可通过发送编队服务请求给 RSUs 并基于智能合约支付相关费用成为编队成员, 极大提升道路车辆的行驶效率.

6.2 区块链辅助的交通安全管理

车联网海量信息的应用可提高交通管理的效率, 并加快推动智能交通的发展. 当前, 交通系统安全

表 10 基于区块链的交通安全管理对比

Table 10 Comparison of traffic security management based on Blockchain

Proposal	Description	Method	BC techno.	BC nodes	Security properties
[109]	BC-based traffic event validation and trust verification	PoE consensus verification event message	Own	RSUs	Integrity, reliability
[110]	BC-enabled targeted information dissemination	BC stores reliable information	Own	Vehicles, RSUs	Reliability, privacy
[111]	BC-based traffic signal control	BC stores vehicle information	Own	Vehicles, RSUs	Traceability, integrity
[112]	BC-based real-time traffic monitoring	Verification and storage of vehicle traffic information based on BC	Own	Traffic administration	Reliability, privacy, authenticity
[108]	Seven-layer ITS model based on BC	ITS-oriented model for standardizing major components of BC	–	–	–
[113]	BC and IoT-based ITS	ITS' design and implementation	Own	OBU, RSU, ISU	Confidentiality, integrity, availability
[114]	BC and fog computing-based service allocation	BC stores auction results	Own	Cloud data center	Integrity

管理主要面临两个问题: 第一, 恶意节点通过篡改、窃听、拒绝服务等攻击可破坏交通系统的可用性、安全性, 影响交通信息共享、交通信号控制、交通监控等. 第二, 智能交通系统面临可扩展性差、信任等安全问题. 区块链可以建立安全、可信和去中心化的智能交通生态系统 [108], 相关文献对比表格如表 10 [108~114] 所示.

针对恶意攻击破坏交通系统引发的安全问题, 相关研究从交通事件共享、交通信号控制、交通监控 3 方面作出了贡献. 在交通事件共享研究上, 文献 [109] 面向 VANETs 提出基于区块链的交通事件和信任验证方法, 本地 RSUs 链收集车辆间的协作交通信息 (速度、位置等) 到 Merkle Patricia Trie 结构中, 并基于事件证明共识 (proof-of-event, PoE) 验证事件信息的可靠性, 避免虚假消息的传播; 同时, 区块的最后创建者在指定时间里将本地数据提交到全球 RSUs 链, 有效地提高交通管理系统的安全性和可靠性. 类似地, 文献 [110] 面向车载网络提出基于区块链的交通信息传播架构, 车辆在权威机构验证获得证书 (包含信誉值和公钥) 后进入系统, 并将收集的事故信息发送给 RSU; RSU 基于车辆信誉值和信息可信度将事故信息汇总后上传到区块链网络, 以便所有节点基于 DPoS 共识存储包含事故信息的区块, 保证交通管理系统的稳定性和可靠性. 在交通信号控制研究上, 文献 [111] 提出基于区块链的交通信号控制系统, 利用区块链记录带有时间戳的车辆 VIN (vehicle identification number)、车辆轨迹等数据, 保证数据的可追溯性; 并设计一种新的共识机制使得 RSU 和目击车辆共同对源数据进行验证, 防止目击车辆、现场 RSUs 和攻击者发起欺骗攻击. 在交通监控方面, 文献 [112] 提出基于区块链的实时交通监控系统, 以实现交通管理局 (traffic administration, TA) 和车辆之间高效、可靠的信息交易, 解决传统交通监控方案的高成本问题. 具体而言, TA 轻量级节点发布交通信息收集任务, 车辆在接收任务后将加密和签名的交通信息发送给 TA, TA 使用基于预算拍卖机制的智能合约给车辆分发奖励, 激励更多车辆承担收集任务; 而 TA 全节点使用基于声誉的委托权益证明共识在达成一致后将交易信息保存在全节点区块链上, 保证交易信息的可靠性和效率.

针对 ITS 面临的单点故障和信任的问题, 文献 [108] 首次尝试设计基于区块链的 ITS 的 7 层概念模型, 并面向 ITS 标准化区块链系统的典型体系结构、主要组件和功能, 证实了区块链具有建立安全、

表 11 基于区块链的事故安全取证对比

Table 11 Comparison of accident security forensics based on Blockchain

Proposal	Description	Method	BC techno.	BC nodes	Security properties
[115]	Vehicle forensics system based on permission BC	Ledger stores data of all parties	Permissioned Blockchain	Drivers, maintenance centers, car manufacturers, law enforcement	Integrity, privacy, non-repudiation
[116]	BC-enabled vehicle accident detection and notification	BC stores accident transactions	Own	Cloud server	Integrity, forward secrecy, backward secrecy
[117]	BC-based accident detection	BC stores accident-related data	Private BC, public BC	–	Integrity
[118]	Vehicular Blocktrees-based recorded events	Blocktrees stores recorded events	Own	Vehicles	Traceability
[119]	BC-inspired event recording	BC stores event recording	Own	Vehicles	Integrity, traceability

可信、分布式 ITS 的潜力, 为未来的研究工作提供有益的指导和参考. 进一步地, 文献 [113] 对基于区块链的 ITS 进行了系统设计和实现, 该系统主要包括汽车、RSU、ISU (intermedia server unit)、基于云的区块链平台等组件; ISU 和 RSU 区块链记录车辆收集的交通状况信息, 防止数据被篡改; 云服务器通过分析区块链中记录的数据, 给车辆提供交通状态分析、交通因子计算和分析、交易令牌系数评估等智能交通服务. 针对 ITS 中不可信车辆攻击导致的服务不稳定问题, 文献 [114] 提出基于区块链和移动雾计算的资源拍卖分配方案, RSU 雾节点在广播拍卖任务信息后收集车辆雾节点的投标信息, 并基于 Vickrey-Clarke-Groves 的拍卖算法发布投标结构和支付相关费用, 保证资源分配的公平性; 同时, RSU 定期将交易列表上传到云服务器区块链, 保证拍卖结果一致性.

6.3 区块链辅助的事故安全取证

物联网技术的发展使得装载车载诊断端口和事件数据记录器的汽车可以记录汽车速度信息、油门/刹车状态、位置变化信息等数据, 为车辆事故取证提供有利证据. 相关部门可通过对车辆数据的捕获和分析查找事故产生原因, 解决驾驶员、保险公司、制造商、维护中心之间的事故赔偿纠纷. 区块链去中心化、不可篡改等特性契合于事故取证的可审计性, 因此, 基于区块链的车辆事故存证以及验证成为研究热点, 相关文献对比表格如表 11 [115~119] 所示.

针对现有车辆事故取证无法真实还原事件本身的问题 (车辆存储空间有限, 无法保证事故数据的完整性), 文献 [115] 提出基于许可链的车辆取证系统, 使用分布式分类账本存储车辆维护信息、历史记录、汽车诊断报告实现可追溯的事故分析; 同时将 PKI 结合到许可区块链用于构建包含车辆假名身份的证书, 保证身份隐私. 文献 [116] 提出基于区块链和证书的事故消息交易方案, 车辆在道路上检测到事故后, 将事故交易转发给 CH; CH 通过 RSU 将该交易发送给边缘服务器; 边缘服务器构建包含交易、数字签名和 Merkle 树根的部分区块, 并转发到云服务器完成区块的创建、验证、添加, 保证车辆事故检测的完整性. 文献 [117] 提出基于区块链的在线事故检测模型和离线事故检测模型. 其中, 在线检测模型针对事故附近存在交通基础设施的场景, 使用私有链存储事故目击者 (基站、汽车、行人等) 陈述的事故事实, 或使用公有链基于 PoW 共识验证事故的真实性; 离线检测模型针对交通事故附近没有目击者的场景, 经过事故的车辆利用基于哈希和时间戳的签名方式将事故数据存入区块链中, 保证参与者尽可能拥有全部事故信息, 并验证事故起因.

针对车辆虚假数据影响事故取证真实性的问题, 文献 [118] 在车辆区块树中提出分布式物理证明共识机制, 基于物理定律和事故附近车辆签名的观测值对事故信息进行验证, 并将验证结果存入车辆区块树中, 保证信息的可追溯性, 以便后续的事故取证和分析. 文献 [119] 在自动驾驶汽车事件记录系统中提出具有动态联合的事件证明共识机制, 将事故车辆和观测车辆的事件消息和基于 SHA256 的哈希摘要广播到 IoV 中形成随机联合组, 并在验证后存入区块链中, 帮助 AVs 实现完整、可追溯的事件记录和取证.

总体而言, 基于区块链的车联网应用安全主要包括利用智能合约定义车辆应用、利用以有区块链平台开发服务、利用分布式账本保证交通类数据的完整性和事故类数据的可追溯性. 综合现有文献来看, 基于区块链的车联网应用安全正处于初级阶段, 尚未满足日益增多的车辆用户对多样化应用场景的期望 (例如: 汽车与电力资源、汽车供应链管理等), 有待进一步探索. 文献 [11] 认为 IoV 可以利用区块链的附加加密货币的概念和激励机制来催生更多车路协同类应用. 同时, 随着用户对车联网应用服务的需求加剧, 基于区块链的车联网安全体系架构在网络性能和安全性能方面也有待进一步提升.

7 基于区块链的新型车联网安全体系架构

当前, 多种技术被应用于基于区块链的车联网安全体系架构中, 例如: 边缘计算 (edge computing, EC)、软件定义网络、网络功能虚拟化 (network functions virtualization, NFV) 等. 区块链在不同的架构中扮演着不同的角色, 例如: 利用区块链与 SDN/NFV 融合实现架构安全, 与边缘节点融合构建具备安全特性的资源共享平台 [120]. 本节对区块链技术在车联网安全体系架构的研究上进行了总结. 目前, 基于区块链的新型车联网安全体系架构设计的研究主要集中在 3 个方面: 基于区块链和 EC 的车联网安全体系架构; 基于区块链和 NFV 的车联网安全体系架构; 基于区块链和 SDN 的车联网安全体系架构, 相关文献对比表格如表 12 [121~129] 所示.

7.1 基于区块链和 EC 的车联网安全体系架构

边缘计算将车辆节点的计算密集型任务从中央服务器卸载至网络边缘, 实现低延时的服务. 一些学者在基于区块链的车联网安全体系架构中引入 EC, 将挖矿、共识等计算任务卸载至边缘实体以缓解中央服务器的计算负载 [130], 解决了新兴的车联网架构的可扩展性问题.

为解决区块链技术应用于车联网架构中存在的可扩展性问题, 文献 [121] 提出基于可信区块链和边缘计算的 IoV 架构, 利用边缘服务器处理、存储车辆的消息, 保证数据的安全性; 设计基于联邦拜占庭协议和位置证明的共识机制, 缩短区块的生成时间, 提高系统的可扩展性. 5G 网络下由于大量事件驱动消息 (event driven message, EDM) 的分发给车联网系统带来极大的带宽消耗和响应延迟, 从而致使系统的可扩展性较差, 文献 [122] 提出利用边缘节点构建私有区块链分布式处理和存储 EDMs, 保证 EDMs 的可审计性和可靠性, 并采用轻量级多接收器签密方案实现低延时的 EDMs 的访问控制.

为了满足新兴的车联网应用 (例如: 实时导航系统、自动驾驶、道路监控) 的计算和存储需求, 文献 [123] 提出基于区块链和 AI 的车辆边缘计算架构, RSUs 联盟区块链存储和处理车辆的元数据并将处理后的数据转发至云服务器; 云服务器学习数据后获得车辆 AI 模型, 并通过 RSU 转发至车辆自动触发应用程序的更新; 同时, 云服务器会将一些计算任务下放至边缘节点, 优化云服务器的计算资源. 车辆对交通异常情况的完整上下文感知对实时交通管理至关重要, 文献 [124] 提出基于区块链和雾计算的 IoV 架构, 分布式的车辆雾节点感知完整的交通信息并发送到区块链网络, 所有区块节点在基于消逝时间量的共识验证后将感知数据存储在分布式账本中, 确保车辆对异常交通情况作出正确决策.

表 12 基于区块链的新型车联网安全体系架构对比

Table 12 Comparison of novel IoV/V2X security system architecture based on Blockchain

Class	Proposal	Description	Method	BC techno.	BC nodes	Advantage
BC+EC	[121]	IoV architecture based on trustworthy BC and EC	Edge server processes and stores messages	Permissioned Blockchain	Edge server	Scalability, security
BC+EC	[122]	5G enabled vehicular EC and BC-based emergency driven message	Edge nodes to record the EDM	Own	RSUs	Scalability, security, low latency
BC+EC	[123]	Vehicular edge computing architecture based on BC and AI	RSUs process and store vehicle metadata	Consortium Blockchain	RSUs	Smart, secure, efficient
BC+EC	[124]	IoV architecture based on BC and fog computing	Vehicle fog nodes aware full context	Own	Vehicles	Efficient and resilient P2P network
BC+EC	[125]	VANET architecture based on BC and mobile edge computing	Edge nodes handle computationally intensive work	Own	RSUs	Data security
BC+NFV	[126]	BC-enabled network function virtualization management and orchestration	BC assists MANO system to automatically manage and orchestrate cloud resources	Permissioned Blockchain	–	High throughput, low latency
BC+SDN	[127]	Vehicle clouds collaboration mechanism based on BC and SDN	Software-defined service collaboration	Own	Cloud server	Service quality assurance based on dynamic optimization
BC+SDN	[128]	BC-based software-defined vehicular networks	Virtualization of computing resources and network resources based on BC' trust	Permissioned Blockchain	BS, Cloud server	High throughput
BC+SDN	[129]	BC-based software defined vehicular networks	Authorize legitimate vehicles to access the SDN controller	Own	Vehicles, RSUs, SDN controller	High scalability, security

上述研究专注于边缘计算资源的管理, 未考虑车辆移动性带来的区块链网络不稳定的问题, 文献 [125] 提出基于区块链和移动边缘计算 (mobile edge computing, MEC) 的 VANET 安全架构, 感知层利用 RSUs 组成的区块链实现对数据进行分布式存储, 保证数据的安全性 (此处指防篡改和可追溯性); 边缘计算层采用 MEC 将共识任务和其他大型计算任务卸载至边缘节点处理, 减轻中心实体和车辆的计算负载, 确保区块链网络的稳定性.

7.2 基于区块链和 NFV 的车联网安全体系架构

NFV 网络架构利用虚拟化技术实现通用硬件上基于软件的网络服务, 具有低成本、弹性灵活的优势 [131]. 管理和编排 (management and orchestration, MANO) 作为 NFV 的核心技术能够实现网络资源、虚拟化网络功能、用户服务的自动化管理, 可用于提高车联网网络管理和协调的灵活性. 然而, 在多场景、多应用的车联网环境下, 异构 MANO 的消息同步存在安全和信任问题, 文献 [126] 提出基于区块链和多接入边缘计算 (multi-access edge computing, MEC) 的分布式 NFV-MANO 框架, 海量移动服务在接入到网络后基于 NFV 技术以分布式方式部署到 MEC 服务器; 多个 MANO 系统在基于动态信任区块链的辅助下实现云端资源的自动化管理和编排, 保证资源分配的安全性; 同时, MEC 服务器用于处理区块链中计算密集型任务, 有助于提高区块链网络的吞吐量和资源分配的效率.

7.3 基于区块链和 SDN 的车联网安全体系架构

SDN 是一种新型的网络架构, 其核心思想是将网络控制 (控制平面) 和转发功能 (数据平面) 分离开来简化网络管理. SDN 应用于车联网具有以下优势: 第一, 控制和转发功能分离可直接编程车联网网络控制; 第二, 逻辑上的集中控制可提高车联网资源的利用率; 第三, 网络可编程性使得应用程序可选择合适的接口传输数据 [132].

针对车云协作性差导致异构车辆协作效率低下的问题, 文献 [127] 提出基于区块链和 SDN 的车云协同服务架构 —— JointCloud, 将区块链网络部署在数据平面和控制平面中用于构建去中心化的服务度量、价值交换和协同信任机制, 基于智能合约实现协同服务的自动可靠结算, 实现 JointCloud 网络的事件审计和追溯, 确保车云协作服务的质量和安全性.

针对分布式软件定义车载网络 (software-defined vehicular network, SDVN) 中 SDN 控制器的共识问题, 文献 [128] 提出基于区块链和深度学习的 SDVN, 由基站和服务器组成的许可区块链用于 SDN 控制器间的消息安全同步, 并结合区块节点信任值虚拟化节点计算资源和网络资源, 有效地提高区块网络的吞吐量; 并利用 Q-learning 算法解决区块链网络视图变化、计算资源分配和网络资源分配的联合优化问题.

针对 SDVN 中的数据包重定向、丢弃和未经授权的访问等安全问题, 文献 [129] 面向 SDVN 提出基于区块链的身份认证和访问控制方法, 将全局的区块链网络划分为管理特定地域的子区块链网络, 用于验证、撤销和控制 OBUs, RSUs 的访问; 使用智能合约创建/更新/吊销存储在区块链中的车联网设备的 X.509 证书, 并基于 TLS 和 X.509 证书实现跨子网的身份认证; 通过检查 SDN 控制器是否授权指定地理区域内的访问来决定是否通过 RSU 和车辆的连接, 保证合法 RSU 和车辆对 SDN 控制器的访问.

总体而言, 基于区块链的车联网安全架构正朝着边缘化的计算存储、自动化的资源管理、智能化的网络资源编排等方向持续演进. 车联网增强应用对服务质量 (quality of service, QoS) 的多样化需求日趋增加, EC/NFV/SDN 等技术可在多维资源分配和动态服务供应方面发挥更多的潜力. 本文认为, 融合区块链/EC/NFV/SDN 的新型车联网安全架构还可在上述研究基础上作进一步创新, 例如: 将用于计算卸载的 VNF (virtual network functions) 链接/放置到边缘节点实现资源利用率的最大化、在分层 SDN/NFV 架构中实现部署成本的最小化、在车辆发送不同请求的场景中编排 MEC 服务器的通信/计算/缓存资源实现服务决策的最优化 [133,134], 可为支撑基于区块链的车联网安全发展增添新助力.

8 总结和展望

本文在总结现有基于区块链的车联网安全关键技术的研究上, 分析了当前基于区块链的车联网通信安全、数据安全、应用安全的防护手段与方案, 梳理了基于区块链的新型车联网安全体系架构. 结合区块链和车联网的发展趋势, 本文提出了 10 项基于区块链的车联网安全未来研究方向 (如图 3 所示), 现详细阐述如下.

(1) AI-enabled 智能合约. 在基于区块链的车联网中, 数据在车辆上生成, 并转发到 Cloud/Fog 等边缘节点上进行分析, 其中一个关键的挑战是如何识别不熟悉的数据模式并根据不同需求对数据进行分类. 当前智能合约的开发工作主要由软件从业者来完成, 其编写的智能合约在完备性上可能会存在逻辑上漏洞. 所以, 在数据存储的智能合约中嵌入智能模型, 智能地识别和分类新的数据模式, 而不是

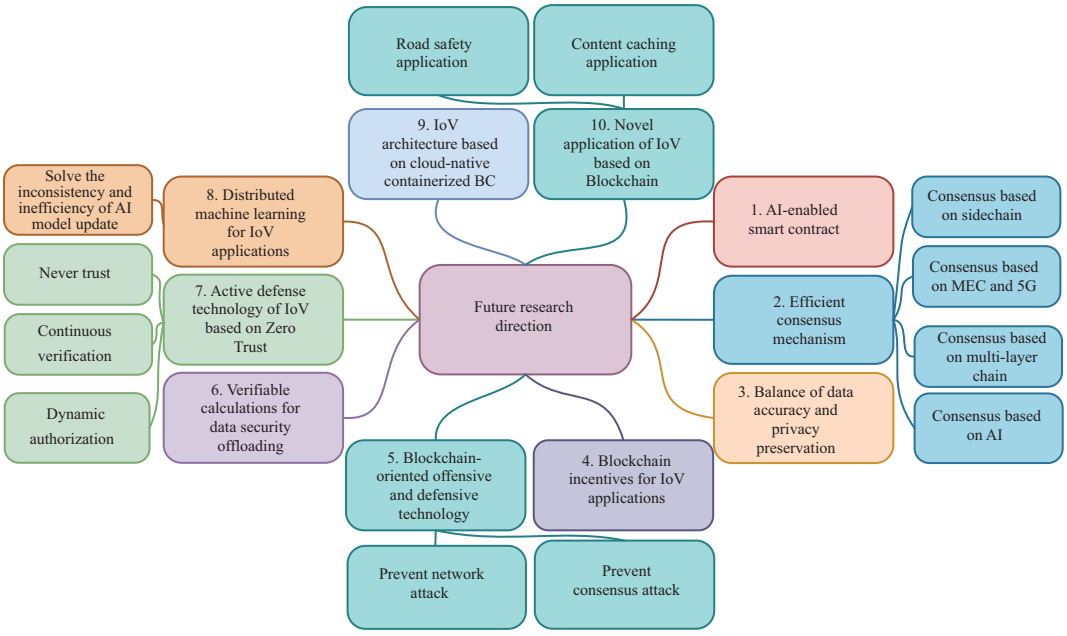

图 3　基于区块链的车联网安全未来研究方向

Figure 3　The future research direction of IoV/V2X security based on Blockchain

静态地定义这些数据, 可以充分保障数据的安全. 因此, 探索支持 AI 的智能合约是基于区块链的车联网安全的研究重点.

(2) 高效的共识机制. 受限于车联网节点的计算能力、存储能力, 当前主流区块链共识机制 (如 PoW, PoS, PBFT 等) 面临可扩展性差、计算消耗大、交易确认效率低、节点容错差和性能难以平衡的问题, 需要从以下几个方面进行优化:

(a) 依赖 “主干” 区块链的安全性, 不同的侧链制定自己的共识规则, 以支持多种基于区块链的用例; 除少数不可避免的链上操作外, 大多数交易都在侧链内执行, 实现共识机制的可伸缩性和互操作性.

(b) 考虑将 RSUs 用作边缘服务器, 并设计高效的点对点通信协议加速区块形成; 利用多接入边缘计算和 5G 重新设计共识算法, 以实现超可靠的低延迟通信, 解决交易确认效率低下的问题.

(c) 探索大规模分布式的共识机制, 建立多层共识机制, 依次在不同层级建立共识, 直至达到全网共识, 降低吞吐量, 解决算力消耗大的问题.

(d) 研究面向传统共识机制的智能化方法, 利用深度强化学习的感知和决策能力, 对传统共识机制的计算消耗、节点选择进行智能改进, 达到合理分配算力、增强网络容错性的目的, 解决节点容错性差的问题.

(3) 探索数据准确性和隐私保护的平衡点. 差分隐私保护机制可以作为一种基于区块链的车联网隐私保护解决方案. 在车联网场景中, 差分隐私通过对位置以及身份进行数据扰动, 保证位置和车辆的隐私, 并通过添加一定数量的噪声来实现数据的安全存储. 扰动程度越高的数据可以增强隐私保护的程度, 但给数据的准确性带来影响. 这种准确性和隐私性的不平衡可能会给需要准确数据的车联网应用程序带来难题. 因此找到数据准确性和隐私性的平衡点, 也是未来车联网场景下隐私保护的主要研究内容之一.

(4) 面向车联网应用的区块链激励机制. 基于公有/联盟链的车联网通常依赖一个或多个实体的贡献以实现新区块的认证、数据生成和区块存储. 针对车联网的应用, 应提出相应的激励机制, 为参与者提供相关激励, 加速块链相关活动的完成. 在基于区块链的车联网中, 如何实现不同的资源价值定量, 并利用定价理论优化各方的利润来保证各方积极参与区块的形成; 如何构建适当和实际可行的机制, 以便建立节点间长期稳定的联系; 如何在交易资源时利用智能合约来确保和维持实体的可信; 如何发现恶意或不诚实的实体; 如何正确量化因连接中断而下线的参与者的利润和奖励; 这些都是面向车联网应用的区块链激励机制应该考量的问题.

(5) 面向区块链的攻防技术研究. 区块链网络的安全威胁主要表现在: 客户端用户地址和交易信息被攻击者获取, 导致用户隐私泄露的危险; 区块节点间的通信可能被恶意攻击者阻断, 例如: 通过隔离目标节点并对其实施路由欺骗、存储污染、拒绝服务以及 ID 劫持等攻击, 导致服务不可用或用户受欺骗的危害; 共识攻击将会导致数据传输平台的区块链产生分叉, 历史交易被篡改, 数据完整性被破坏. 因此, 研究面向区块链的攻防技术, 发现区块链的潜在安全威胁, 对于提升区块链自身的安全, 构建安全的基于区块链的车联网具有重要的意义.

(6) 面向数据安全卸载的可验证计算. 车联网的高移动性和异构性使得车辆需要采用边缘计算来完成数据的安全卸载, RSUs 作为边缘节点, 能够提供一种可行的方式来执行区块链计算和存储. 而不可信的第 3 方的 RSUs 可能会导致安全问题. 例如: 边缘节点获得的区块处理结果不完全可信. 为确保结果的可信赖性, 应确保边缘处理的正确性和可验证性. 因此, 设计面向数据安全卸载的可验证计算是未来基于边缘计算和区块链的车联网系统研究的关键技术之一. 具体而言, 轻量级的实体将某些功能的计算任务分流到功能更强大的计算节点上, 而功能强大的计算节点将证明自身可信的结果发送回去, 以便轻量级实体能够验证计算是否已正确执行.

(7) 基于零信任的车联网主动防御技术. 在云计算的大背景下, 网络、计算、存储等资源被虚拟化和池化, 各类租户和用户分时复用共享池化资源, 虚机间、网络间、用户间、租户间、业务间的物理边界消失, 这导致传统基于边界的防御思路难以有效实施; 其次 “堡垒更容易从内部突破”, 攻击者或恶意用户一旦以合理身份进入车联网内, 便可对任意节点发起各类攻击. 零信任网络安全理念, 假设网络边界的内部和外部都存在攻击者, 不自动信任任何设备, 通过 “永不信任、持续验证、动态授权” 的方式, 变边界防护思维的 “面防御” 为零信任架构下的 “点防御”. 因此, 构建面向高安全等级防护的 “零信任” 内生安全的车联网, 使其具备广义鲁棒、自适应微隔离和自主防御检测能力, 实现不依赖先验攻击知识的主动式防御、具备零信任安全模型的车联网环境微隔离, 对于构建基于区块链的车联网安全具有重要的意义.

(8) 面向车联网应用的分布式机器学习. 文献 [123] 提出将 AI 部署到 Fog 服务器上会产生 AI 模型更新的不一致性和低效率的问题. 具体而言, AI 模型在 Fog 服务器上更新, Fog 服务器从连接的区块链接收数据. 在单独的 Fog 服务器上运行 AI 更新会导致不同位置的 AI 模型之间的不一致, 可能影响应用程序的性能. 因此, 同一应用模型的一致性聚合机制至关重要. 开发分布式机器学习模型, 利用 Fog 服务器的集群和分布式特性, 使用从不同位置并行接收的大数据来更新 AI 模型, 可有效提升模型更新的一致性.

(9) 基于云原生容器化区块链的车联网网络架构. 基于区块链的车联网架构受区块链版本、开发工具及部署环境的限制, 使开发者难以聚焦区块链上层应用的开发及业务创新, 导致应用解决方案迭代效率低下, 周期较长. 云原生容器化区块链解决方案利用容器封装区块链节点, 实现区块链网络功能的编排、创建、运维和资源管理, 从而提供标准化的软件打包分发能力, 使区块链基础设施可以在各种异构环境下实现低成本、高效的部署; 依托编排调度工具, 实现网络中统一的资源管理及调度; 解决

兼容性差导致的多个不同侧链之间交易难以达成一致性共识、可扩展性差导致系统运行效率低下、新区块生成时延增大等问题; 利用 Namespace 隔离、网络策略等机制与区块链安全治理机制整合, 提供坚实的底层安全保障; 将网络服务功能解耦, 并以微服务方式部署于 Docker 中, 从而利用 Docker 动态生成/删除区块链上的微服务, 使系统架构能够根据负载需求动态变化, 提供动态可伸缩的网络服务能力.

(10) 探索基于区块链的车联网新应用. 区块链和智能合约在车联网的应用中发挥重要作用, 以下为基于区块链和智能合约的潜在车联网新型应用.

(a) 道路安全应用. 区块链与道路安全应用结合后, 车辆和信任的 RSUs 建立区块链网络, 区块链网络实时收集多方数据并进行分析, 当发生道路安全事件时, RSUs 和车辆保存记录并告知所有人采取必要措施来规避潜在风险.

(b) 内容缓存. 车联网数据传输密集型的应用多采用内容缓存的方式, RSUs 和车辆的存储资源作为云服务器的存储资源补充以受到越来越多的关注. 区块链可以在车联网中实现高效、经济可行的内容缓存. 例如利用区块结构, 仅保留缓存内容的轻量级区块头, 可以实现高效的车辆和缓存节点的信任; 利用智能合约为缓存贡献者发放激励.

9 结束语

车联网产业是学科交叉及汽车、电子、通信、道路交通等行业深融合的新兴产业, 车联网的发展对于构建汽车和交通服务新业态、提升行车安全、提高交通效率、促进跨产业融合发展具有重要意义. 然而, 安全问题是车联网产业健康发展的巨大隐患, 区块链作为一种去中心化、极难篡改、可追溯性、可编程性、安全可信的新兴基础架构与分布式计算范式, 能够为车联网提供有效的安全可信保障. 在全球加速布局区块链发展的大背景下, 构建基于区块链的跨企业、跨行业的车联网互信互认互通安全体系, 对于推动车联网规模化、高质量发展意义深远.

致谢 本文的撰写得到了时岩老师、徐晖老师的帮助, 在此向她们表示感谢!

参考文献

1 Chen S Z, Hu J L, Shi Y, et al. LTE-V2X car networking technology, standards and applications. Telecommun Sci, 2018, 4: 1–11 [陈山枝, 胡金玲, 时岩, 等. LTE-V2X 车联网技术、标准与应用. 电信科学, 2018, 4: 1–11]

2 Chen S Z, Hu J L. Cellular Vehicle-to-Everything (C-V2X). Beijing: Posts & Telecom Press, 2021 [陈山枝, 胡金玲. 蜂窝车联网 (C-V2X). 北京: 人民邮电出版社, 2021]

3 Ma X B, Peng J H, Xue L, et al. Integrated security of cyber-physical vehicle networked systems in the age of 5G. Sci Sin Inform, 2019, 49: 1640–1658 [马小博, 彭嘉豪, 薛磊, 等. 5G 时代车联网信息物理融合系统综合安全研究. 中国科学: 信息科学, 2019, 49: 1640–1658]

4 Chen S Z, Hu J L, Shi Y, et al. LTE-V: a TD-LTE-based V2X solution for future vehicular network. IEEE Int Things J, 2016, 3: 997–1005

5 Chen S Z, Hu J L, Shi Y, et al. A vision of C-V2X: technologies, field testing, and challenges with chinese development. IEEE Int Things J, 2020, 7: 3872–3881

6 Mollah M B, Zhao J, Niyato D, et al. Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey. IEEE Int Things J, 2021, 8: 4157–4185

7 Yuan Y, Wang F Y. Current status and prospects of Blockchain technology development. Act Autom Sin, 2016, 42: 481–493 [袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42: 481–493]

8 Taiyaba M, Akbar M A, Qureshi B, et al. Secure V2X environment using Blockchain technology. In: Proceedings of Evaluation and Assessment in Software Engineering, New York, 2020. 469–474

9 Tripathi G, Ahad M A, Sathiyanarayanan M. The role of Blockchain in Internet of vehicles (IoV): issues, challenges and opportunities. In: Proceedings of International Conference on Contemporary Computing and Informatics, Singapore, 2019. 26–31

10 Noby D A, Khattab A. A survey of Blockchain applications in IoT systems. In: Proceedings of the 14th International Conference on Computer Engineering and Systems, Cairo, 2019. 83–87

11 Kumar S, Velliangiri S, Karthikeyan P, et al. A survey on the Blockchain techniques for the Internet of vehicles security. Trans Emerging Tel Tech, 2021. doi: 10.1002/ett.4317

12 Li C C. Research on secure mechanism in Internet of vehicles for information security issues. Dissertation for Ph.D. Degree. Beijing: Beijing Jiaotong University, 2019 [李聪聪. 面向车联网信息安全问题的安全机制研究. 博士学位论文. 北京: 北京交通大学, 2019]

13 Liu T Y, Zhang Y S, Shi Y, et al. On the design of key life cycle demonstration based on Blockchain technology. J Cryptologic Res, 2020, 7: 404–420 [刘天野, 张艳硕, 石钰, 等. 基于区块链技术的密钥生命周期演示设计. 密码学报, 2020, 7: 404–420]

14 Li X C, Yin X C. Blockchain-based group key agreement protocol for vehicular ad hoc networks. Comput Commun, 2022, 183: 107–120

15 Ma Z, Zhang J W, Guo Y Z, et al. An efficient decentralized key management mechanism for VANET with Blockchain. IEEE Trans Veh Technol, 2020, 69: 5836–5849

16 Chen Y L, Hao X H, Ren W, et al. Traceable and authenticated key negotiations via Blockchain for vehicular communications. Mobile Inf Syst, 2019, 2019: 1–10

17 Lei A, Cruickshank H, Cao Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Int Things J, 2017, 4: 1832–1843

18 Wang Q. Research on security mechanism and key technology of Internet of vehicles. Dissertation for Ph.D. Degree. Nanjing: Nanjing University of Science and Technology, 2016 [王群. 车联网的安全机制及关键技术研究. 博士学位论文. 南京: 南京理工大学, 2016]

19 Li Q, Shu Z X, Yu X, et al. Authentication mechanism in Blockchain systems. J Command Control, 2019, 5: 1–17 [李强, 舒展翔, 余祥, 等. 区块链系统的认证机制研究. 指挥与控制学报, 2019, 5: 1–17]

20 Labrador M, Hou W Y. Implementing Blockchain technology in the Internet of vehicle (IoV). In: Proceedings of International Conference on Intelligent Computing and its Emerging Applications, Tainan, 2019. 5–10

21 Zhang L, Luo M X, Li J T, et al. Blockchain based secure data sharing system for Internet of vehicles: a position paper. Veh Commun, 2019, 16: 85–93

22 Kamal M, Srivastava G, Tariq M. Blockchain-based lightweight and secured V2V communication in the Internet of vehicles. IEEE Trans Intell Transp Syst, 2020, 22: 3997–4004

23 Hu W, Hu Y, Yao W H, et al. A Blockchain-based byzantine consensus algorithm for information authentication of the Internet of vehicles. IEEE Access, 2019, 7: 139703

24 Wang X L, Zeng P J, Patterson N, et al. An improved authentication scheme for Internet of vehicles based on Blockchain technology. IEEE Access, 2019, 7: 45061–45072

25 Eddine M S, Ferrag M A, Friha O, et al. EASBF: an efficient authentication scheme over Blockchain for fog computing-enabled Internet of vehicles. J Inf Security Appl, 2021, 59: 102802

26 Malik N, Nanda P, Arora A, et al. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In: Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy, New York, 2018. 674–679

27 Kaur K, Garg S, Kaddoum G, et al. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In: Proceedings of IEEE International Conference on Communications Workshops, Shanghai, 2019. 1–6

28 Lasla N, Younis M, Znaidi W, et al. Efficient distributed admission and revocation using Blockchain for cooperative ITS. In: Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security, Paris, 2018. 1–5

29 Xu Z, Liang W, Li K C, et al. A Blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of vehicles. J Parallel Distrib Comput, 2021, 149: 29–39

30 Akhter A F M S, Ahmed M, Shah A F M S, et al. A Blockchain-based authentication protocol for cooperative vehicular ad hoc network. Sensors, 2021, 21: 1273

31 Arora A, Yadav S K. Blockchain based security mechanism for Internet of vehicles (IoV). In: Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies, Jaipur, 2018. 267–272

32 Xu C, Liu H Z, Li P F, et al. A remote attestation security model based on privacy-preserving Blockchain for V2X. IEEE Access, 2018, 6: 67809–67818

33 Theodouli A, Moschou K, Votis K, et al. Towards a Blockchain-based identity and trust management framework for the IoV ecosystem. In: Proceedings of Global Internet of Things Summit, Dublin, 2020. 1–6

34 Rowan S, Clear M, Gerla M, et al. Securing vehicle to vehicle communications using Blockchain through visible light and acoustic side-channels. 2017. ArXiv:1704.02553

35 Wang M Z, Liu D, Zhu L H, et al. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing, 2016, 98: 685–708

36 Xie R N, Li H, Shi G Z, et al. Blockchain-based access control mechanism for data traceability. J Commun, 2020, 41: 82–93 [谢绒娜, 李晖, 史国振, 等. 基于区块链的可溯源访问控制机制. 通信学报, 2020, 41: 82–93]

37 Ye Q. Research on secure access control policy in Internet of vehicles. Dissertation for Master's Degree. Chongqing: Chongqing University of Posts and Telecommunications, 2017 [叶青. 车联网环境下的安全访问控制策略研究. 硕士学位论文. 重庆: 重庆邮电大学, 2017]

38 Liu Y N, Xiao M, Zhou Y Y, et al. An access control mechanism based on risk prediction for the IoV. In: Proceedings of the 91st Vehicular Technology Conference, Antwerp, 2020. 1–5

39 Kchaou K, Ayed S, Abassi R, et al. Smart contract-based access control for the vehicular networks. In: Proceedings of International Conference on Software, Telecommunications and Computer Networks, Split, 2020. 1–6

40 Liu Y N, Xiao M, Chen S Z, et al. An intelligent edge-chain-enabled access control mechanism for IoV. IEEE Int Things J, 2021, 8: 12231–12241

41 Yang Z. Research on security mechanisms and key technologies in vehicular networks. Dissertation for Ph.D. Degree. Beijing: Beijing University of Posts and Telecommunications, 2019 [杨哲. 面向车联网的安全机制与关键技术研究. 博士学位论文. 北京: 北京邮电大学, 2019]

42 Li H, Pei L S, Liao D, et al. FADB: a fine-grained access control scheme for VANET data based on Blockchain. IEEE Access, 2020, 8: 85190–85203

43 Jiang M, Wang H, Zhang W, et al. Location-based data access control scheme for Internet of vehicles. Comput Electrical Eng, 2020, 86: 106716

44 Liu A D, Du X H, Wang N, et al. Research progress of Blockchain technology and its application in information security. J Softw, 2018, 29: 2092–2115 [刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展. 软件学报, 2018, 29: 2092–2115]

45 Zhang J S. Research and implementation of trust management mechanism in VANET. Dissertation for Master Degree. Beijing: Beijing University of Posts and Telecommunications, 2020 [张劲松. 车联网信任管理机制的研究和实现. 硕士学位论文. 北京: 北京邮电大学, 2020]

46 Li W J, Song H B. ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans Intell Transp Syst, 2016, 17: 960–969

47 Huang X M, Yu R, Kang J W, et al. Distributed reputation management for secure and efficient vehicular edge computing and networks. IEEE Access, 2017, 5: 25408–25420

48 Singh P K, Singh R, Nandi S K, et al. Blockchain-based adaptive trust management in Internet of vehicles using smart contract. IEEE Trans Intell Transp Syst, 2021, 22: 3616–3630

49 Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks. IEEE Int Things J, 2019, 6: 1495–1505

50 Khelifi H, Luo S, Nour B, et al. A Blockchain-based architecture for secure vehicular named data networks. Comput Electrical Eng, 2020, 86: 106715

51 Singh M, Kim S. Trust Bit: reward-based intelligent vehicle commination using Blockchain paper. In: Proceedings

of the 4th World Forum on Internet of Things, Singapore, 2018. 62–67
52 Yao Y L, Chen W D, Chen W, et al. A Blockchain-based privacy preserving scheme for vehicular trust management systems. In: Proceedings of International Conference on Internet of Things and Intelligent Applications, Zhenjiang, 2020. 1–5
53 Lu Z J, Wang Q, Qu G, et al. BARS: a Blockchain-based anonymous reputation system for trust management in VANETs. In: Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, New York, 2018. 98–103
54 Zhang H B, Liu J J, Zhao H L, et al. Blockchain-based trust management for Internet of vehicles. IEEE Trans Emerg Top Comput, 2020, 9: 1397–1409
55 Shrestha R, Bajracharya R, Shrestha A P, et al. A new type of Blockchain for secure message exchange in VANET. Digital Commun Netw, 2020, 6: 177–186
56 Lu Z J. Research on privacy preserving scheme for vehicle ad-hoc networks. Dissertation for Ph.D. Degree. Wuhan: Huazhong University of Science And Technology, 2018 [鲁赵骏. 车联网隐私保护方案研究. 博士学位论文. 武汉: 华中科技大学, 2018]
57 Cheng L C, Liu J Q, Xu G Q, et al. SCTSC: a semicentralized traffic signal control mode with attribute-based Blockchain in IoVs. IEEE Trans Comput Soc Syst, 2019, 6: 1373–1385
58 Amiri W A, Baza M, Banawan K, et al. Privacy-preserving smart parking system using Blockchain and private information retrieval. In: Proceedings of International Conference on Smart Applications, Communications and Networking, Sharm El Sheik, 2019. 1–6
59 Li M, Zhu L H, Lin X D. Efficient and privacy-preserving carpooling using Blockchain-assisted vehicular fog computing. IEEE Int Things J, 2019, 6: 4573–4584
60 Gao F, Zhu L H, Shen M, et al. A Blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Netw, 2018, 32: 184–192
61 Noh J, Jeon S, Cho S. Distributed Blockchain-based message authentication scheme for connected vehicles. Electronics, 2020, 9: 74
62 Yao Y Y, Chang X L, Misic J, et al. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Int Things J, 2019, 6: 3775–3784
63 Li M, Zhu L H, Lin X D. CoRide: a privacy-preserving collaborative-ride hailing service using Blockchain-assisted vehicular fog computing. In: Proceedings of International Conference on Security and Privacy in Communication Systems, Washington, 2019. 408–422
64 Yang Y, Chen J L, Zheng X H, et al. Blockchain-based incentive announcement system for Internet of vehicles. In: Proceedings of IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, Xiamen, 2019. 817–824
65 Li L, Liu J Q, Cheng L C, et al. CreditCoin: a privacy-preserving Blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans Intell Transp Syst, 2018, 19: 2204–2220
66 Li M, Weng J, Yang A, et al. Toward Blockchain-based fair and anonymous ad dissemination in vehicular networks. IEEE Trans Veh Technol, 2019, 68: 11248–11259
67 Mei Q, Xiong H, Zhao Y, et al. Toward Blockchain-enabled IoV with edge computing: efficient and privacy-preserving vehicular communication and dynamic updating. In: Proceedings of IEEE Conference on Dependable and Secure Computing, Aizuwakamatsu, 2020. 1–8
68 Sharma R, Chakraborty S. BlockAPP: using Blockchain for authentication and privacy preservation in IoV. In: Proceedings of IEEE Globecom Workshops, Abu Dhabi, United Arab Emirates, 2018. 1–6
69 Shi K X, Zhu L H, Zhang C, et al. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. Multimed Tools Appl, 2020, 79: 8085–8105
70 Guehguih B, Lu H W. Blockchain-based privacy-preserving authentication and message dissemination scheme for VANET. In: Proceedings of the 5th International Conference on Systems, Control and Communications, New York, 2019. 16–21
71 Zhang J, Yang F, Ma Z, et al. A decentralized location privacy-preserving spatial crowdsourcing for Internet of

vehicles. IEEE Trans Intell Transp Syst, 2020, 22: 2299–2313
72 Li B, Liang R, Zhou W, et al. LBS meets Blockchain: an efficient method with security preserving trust in SAGIN. IEEE Int Things J, 2021, 9: 5932–5942
73 Luo B, Li X H, Weng J, et al. Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Trans Veh Technol, 2020, 69: 2034–2048
74 Joy J, Gerla M. Internet of vehicles and autonomous connected car-privacy and security issues. In: Proceedings of the 26th International Conference on Computer Communication and Networks, Vancouver, 2017. 1–9
75 Li X H, Zhong C, Chen Y, et al. Survey of Internet of vehicles security. J Cyber Secur, 2019, 4: 17–32 [李兴华, 钟成, 陈颖, 等. 车联网安全综述. 信息安全学报, 2019, 4: 17–32]
76 Raja G, Manaswini Y, Vivekanandan G D, et al. AI-powered Blockchain-a decentralized secure multiparty computation protocol for IoV. In: Proceedings of IEEE Conference on Computer Communications Workshops, Toronto, 2020. 865–870
77 Zheng Z H, Pan J P, Cai L. Lightweight Blockchain consensus protocols for vehicular social networks. IEEE Trans Veh Technol, 2020, 69: 5736–5748
78 Mershad K, Said B. A Blockchain model for secure communications in Internet of vehicles. In: Proceedings of the 17th International Conference on Computer Systems and Applications, Antalya, 2020. 1–6
79 Gao J B, Agyekum K O B O, Sifah E B, et al. A Blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. IEEE Int Things J, 2020, 7: 4278–4291
80 Hassija V, Chamola V, Han G, et al. DAGIoV: a framework for vehicle to vehicle communication using directed acyclic graph and game theory. IEEE Trans Veh Technol, 2020, 69: 4182–4191
81 Liu M T, Teng Y L, Yu F R, et al. Deep reinforcement learning based performance optimization in Blockchain-enabled Internet of vehicle. In: Proceedings of IEEE International Conference on Communications, Shanghai, 2019. 1–6
82 Ministry of Industry and Information Technology. Technology specification for data security of Internet of vehicle information service. 2020 [中华人民共和国工业和信息化部. 车联网信息服务数据安全技术要求. 2020] https://std.samr.gov.cn/hb/search/stdHBDetailed?id=AFC9FE3F29D8B96EE05397BE0A0AFF12
83 Liu X J, Yin Y D, Chen W, et al. Secure data sharing scheme in Internet of vehicles based on Blockchain. J Zhejiang Univ (Eng Sci), 2021, 55: 957–965 [刘雪娇, 殷一丹, 陈蔚, 等. 基于区块链的车联网数据安全共享方案. 浙江大学学报 (工学版), 2021, 55: 957–965]
84 Dai Y Y, Xu D, Zhang K, et al. Deep reinforcement learning and permissioned Blockchain for content caching in vehicular edge computing and networks. IEEE Trans Veh Technol, 2020, 69: 4312–4324
85 Sadiq A, Javaid N, Samuel O, et al. Efficient data trading and storage in Internet of vehicles using consortium Blockchain. In: Proceedings of International Wireless Communications and Mobile Computing, Limassol, 2020. 2143–2148
86 Dorri A, Steger M, Kanhere S S, et al. BlockChain: a distributed solution to automotive security and privacy. IEEE Commun Mag, 2017, 55: 119–125
87 Hassan M A, Habiba U, Ghani U, et al. A secure message-passing framework for inter-vehicular communication using Blockchain. Int J Distrib Sens Netw, 2019, 15: 1–11
88 Jabbar R, Kharbeche M, Al-Khalifa K, et al. Blockchain for the Internet of vehicles: a decentralized IoT solution for vehicles communication using ethereum. Sensors, 2020, 20: 3928
89 Das D, Banerjee S, Mansoor W, et al. Design of a secure Blockchain-based smart IoV architecture. In: Proceedings of the 3rd International Conference on Signal Processing and Information Security, Dubai, 2020. 1–4
90 Chai H Y, Leng S P, Zeng M, et al. A hierarchical Blockchain aided proactive caching scheme for Internet of vehicles. In: Proceedings of IEEE International Conference on Communications, Shanghai, 2019. 1–16
91 Ou W, Deng M, Luo E. A decentralized and anonymous data transaction scheme based on Blockchain and zero-knowledge proof in vehicle networking (workshop paper). In: Proceedings of International Conference on Collaborative Computing: Networking, Applications and Worksharing, London, 2019. 712–726
92 Wang D, Zhang X H. Secure data sharing and customized services for intelligent transportation based on a consortium Blockchain. IEEE Access, 2020, 8: 56045–56059
93 Ferdous M S, Chowdhury M J M, Biswas K, et al. Immutable autobiography of smart cars leveraging Blockchain

technology. Knowl Eng Rev, 2020, 35: 1–24
94 Javaid U, Aman M N, Sikdar B. DrivMan: driving trust management and data sharing in VANETs with Blockchain and smart contracts. In: Proceedings of the 89th Vehicular Technology Conference, Kuala Lumpur, 2019. 1–5
95 Dwivedi S K, Amin R, Vollala S, et al. Blockchain-based secured event-information sharing protocol in Internet of vehicles for smart cities. Comput Electrical Eng, 2020, 86: 106719
96 Michelin R A, Dorri A, Steger M, et al. SpeedyChain: a framework for decoupling data from Blockchain for smart cities. In: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, 2018. 145–154
97 Lu Y L, Huang X H, Zhang K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles. IEEE Trans Veh Technol, 2020, 69: 4298–4311
98 Chai H Y, Leng S P, Chen Y J, et al. A hierarchical Blockchain-enabled federated learning algorithm for knowledge sharing in Internet of vehicles. IEEE Trans Intell Transp Syst, 2020, 22: 3975–3986
99 Kang J W, Xiong Z H, Niyato D, et al. Toward secure Blockchain-enabled Internet of vehicles: optimizing consensus management using reputation and contract theory. IEEE Trans Veh Technol, 2019, 68: 2906–2920
100 Wang S M, Huang X M, Yu R, et al. Permissioned Blockchain for efficient and secure resource sharing in vehicular edge computing. 2019. ArXiv:1906.06319
101 Leiding B, Memarmoshrefi P, Hogrefe D. Self-managed and Blockchain-based vehicular ad-hoc networks. In: Proceedings of ACM International Joint Conference on Pervasive and Ubiquitous Computing, New York, 2016. 137–140
102 Baza M, Nabil M, Lasla N, et al. Blockchain-based firmware update scheme tailored for autonomous vehicles. In: Proceedings of IEEE Wireless Communications and Networking Conference, Marrakesh, 2019. 1–7
103 Zhou Q H, Yang Z, Zhang K, et al. A decentralized car-sharing control scheme based on smart contract in Internet of vehicles. In: Proceedings of the 91st Vehicular Technology Conference, Antwerp, 2020. 1–5
104 Jabbar R, Fetais N, Kharbeche M, et al. Blockchain for the Internet of vehicles: how to use Blockchain to secure vehicle-to-everything (V2X) communication and payment? IEEE Sens J, 2021, 21: 15807–15823
105 Saini A, Sharma S, Jain P, et al. A secure priority vehicle movement based on Blockchain technology in connected vehicles. In: Proceedings of the 12th International Conference on Security of Information and Networks, New York, 2019. 1–8
106 Narbayeva S, Bakibayev T, Abeshev K, et al. Blockchain technology on the way of autonomous vehicles development. Transp Res Procedia, 2020, 44: 168–175
107 Chen C, Xiao T, Qiu T, et al. Smart-contract-based economical platooning in Blockchain-enabled urban Internet of vehicles. IEEE Trans Ind Inf, 2019, 16: 4122–4133
108 Yuan Y, Wang F Y. Towards Blockchain-based intelligent transportation systems. In: Proceedings of the 19th International Conference on Intelligent Transportation Systems, Rio de Janeiro, 2016. 2663–2668
109 Yang Y T, Chou L D, Tseng C W, et al. Blockchain-based traffic event validation and trust verification for VANETs. IEEE Access, 2019, 7: 30868–30877
110 Zhao P C, Fu Y C, Li F, et al. Blockchain-enabled targeted information dissemination framework in vehicular networks. In: Proceedings of the 92nd Vehicular Technology Conference, Victoria, 2020. 1–5
111 Li W X, Nejad M, Zhang R. A Blockchain-based architecture for traffic signal control systems. In: Proceedings of IEEE International Congress on Internet of Things, Milan, 2019. 33–40
112 Guo J X, Ding X J, Wu W L. Reliable traffic monitoring mechanisms based on Blockchain in vehicular networks. IEEE Trans Rel, 2022, 71: 1219–1229
113 Ren Q L, Man K L, Li M Q, et al. Intelligent design and implementation of Blockchain and Internet of things-based traffic system. Int J Dis Sens Netw, 2019, 15: 1–12
114 Lee Y, Jeong S, Masood A, et al. Trustful resource management for service allocation in fog-enabled intelligent transportation systems. IEEE Access, 2020, 8: 147313
115 Cebe M, Erdin E, Akkaya K, et al. Block4Forensic: an integrated lightweight Blockchain framework for forensics applications of connected vehicles. IEEE Commun Mag, 2018, 56: 50–57
116 Vangala A, Bera B, Saha S, et al. Blockchain-enabled certificate-based authentication for vehicle accident detection

and notification in intelligent transportation systems. IEEE Sens J, 2020, 21: 15824–15838
117 Davydov V, Bezzateev S. Accident detection in Internet of vehicles using Blockchain technology. In: Proceedings of International Conference on Information Networking, Barcelona, 2020. 766–771
118 Joy J. Vehicular blocktrees. In: Proceedings of IEEE Vehicular Networking Conference, Torino, 2017. 147–150
119 Guo H, Meamari E, Shen C-C. Blockchain-inspired event recording system for autonomous vehicles. In: Proceedings of the 1st IEEE International Conference on Hot Information-Centric Networking, Shenzhen, 2018. 218–222
120 Mendiboure L, Chalouf M A, Krief F. Survey on Blockchain-based applications in Internet of vehicles. Comput Electrical Eng, 2020, 84: 106646
121 Lahiri P K, Das D, Mansoor W, et al. A trustworthy Blockchain based framework for impregnable IoV in edge computing. In: Proceedings of the 17th International Conference on Mobile Ad Hoc and Sensor Systems, Delhi, 2020. 26–31
122 Nkenyereye L, Tama B A, Shahzad M K, et al. Secure and Blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing. Sensors, 2020, 20: 154
123 Hammoud A, Sami H, Mourad A, et al. AI, Blockchain, and vehicular edge computing for smart and secure IoV: challenges and directions. IEEE Int Things M, 2020, 3: 68–73
124 Bonadio A, Chiti F, Fantacci R, et al. An integrated framework for Blockchain inspired fog communications and computing in Internet of vehicles. J Ambient Intell Hum Comput, 2020, 11: 755–762
125 Zhang X D, Li R, Cui B. A security architecture of VANET based on Blockchain and mobile edge computing. In: Proceedings of the 1st IEEE International Conference on Hot Information-Centric Networking, Shenzhen, 2018. 258–259
126 Fu X Y, Yu F R, Wang J Y, et al. Performance optimization for Blockchain-enabled distributed network function virtualization management and orchestration. IEEE Trans Veh Technol, 2020, 69: 6670–6679
127 Yin B, Mei L S, Jiang Z X, et al. Joint cloud collaboration mechanism between vehicle clouds based on Blockchain. In: Proceedings of IEEE International Conference on Service-Oriented System Engineering, San Francisco, 2019. 2271–2275
128 Qiu C, Yu F R, Xu F M, et al. Blockchain-based distributed software-defined vehicular networks via deep Q-learning. In: Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, New York, 2018. 8–14
129 Mendiboure L, Chalouf M A, Krief F. A scalable Blockchain-based approach for authentication and access control in software defined vehicular networks. In: Proceedings of the 29th International Conference on Computer Communications and Networks, Honolulu, 2020. 1–11
130 Rahman M A, Rashid M M, Barnes S J, et al. A Blockchain-based secure Internet of vehicles management framework. In: Proceedings of the UK/China Emerging Technologies, Glasgow, 2019. 1–4
131 Chen X Y, Gao Y Z, Tang H L, et al. Research progress on big data security technology. Sci Sin Inform, 2020, 50: 25–66 [陈性元, 高元照, 唐慧林, 等. 大数据安全技术研究进展. 中国科学: 信息科学, 2020, 50: 25–66]
132 Gu X H, Zhang G A. Survey of SDN application in vehicular networks. Comput Sci, 2019, 47: 237–244 [谷晓会, 章国安. SDN 在车载网中的应用综述. 计算机科学, 2019, 47: 237–244]
133 Zhuang W H, Ye Q, Lyu F, et al. SDN/NFV-empowered future IoV with enhanced communication, computing, and caching. Proc IEEE, 2019, 108: 274–291
134 Lin S C, Chen K C, Karimoddini A. SDVEC: software-defined vehicular edge computing with ultra-low latency. IEEE Commun Mag, 2021, 59: 66–72

A survey of Internet of vehicles/vehicle to everything security based on Blockchain

Yuanni LIU[1], Yi LI[1] & Shanzhi CHEN[2*]

1. *School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing* 400065*, China*;
2. *National Key Laboratory of Wireless Mobile Communications* (*China Information and Communication Technology Group Co., Ltd.*)*, Beijing* 100191*, China*
* Corresponding author. E-mail: chensz@cict.com

Abstract With the acceleration of the intelligent and networking processes of the automobile and transportation industries promoted by the IoV/V2X technology, the security problem of IoV/V2X is becoming increasingly serious. As an integrated application of distributed data storage, peer-to-peer transmission, consensus mechanism, encryption algorithms, and other technologies, Blockchain provides a new IoV/V2X security solution. This paper summarizes the research on Blockchain-based IoV/V2X security. First, it outlines the existing IoV/V2X security threats and protection methods, specifies the research value of Blockchain and IoV/V2X integration, and analyzes the Blockchain-based IoV/V2X security technology. Then, it sorts the existing Blockchain-based IoV/V2X security protection methods and their security architecture from the perspectives of communication security, data security, and application security. Finally, it proposes the development direction and research effort of Blockchain-based IoV/V2X security.

Keywords IoV/V2X security, Blockchain, communication security, data security, application security