基于区块链的车联网安全研究综述

曾 萍[1] 闫 坤[2*] 赵 耿[1] 马英杰[1]
[1](北京电子科技学院电子与通信工程系 北京 100070)
[2](西安电子科技大学通信工程学院 陕西 西安 710071)

摘 要 区块链技术的发展为车联网安全提供了新的解决思路。介绍区块链特点及其对应的可解决的车联网安全问题,结合相关文献分类讨论区块链在车联网车辆身份认证、车辆数据隐私保护及系统安全构建三个方面的应用情况,同时对融合系统的性能评估及安全性分析进行讨论,对该领域未来的发展方向进行展望。

关键词 区块链 车联网安全 身份认证 隐私保护

中图分类号 TP301 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.08.001

A SURVEY OF RESEARCH ON INTERNET OF VEHICLES SECURITY BASED ON BLOCKCHAIN

Zeng Ping[1] Yan Kun[2*] Zhao Geng[1] Ma Yingjie[1]
[1](*Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China*)
[2](*School of Telecommunication Engineering, Xidian University, Xi'an 710071, Shaanxi, China*)

Abstract The development of blockchain technology provides new solutions for the security of internet of vehicles. The paper introduced the characteristics of blockchain and the corresponding solvable security problems of the internet of vehicles. We discussed the application of blockchain in the three aspects of the internet of vehicles: vehicle identity authentication, vehicle data privacy protection, and system security construction in combination with related literature classifications. Meanwhile, the security analysis and performance evaluation of the fusion system was briefly described. The future research direction of the field was prospected.

Keywords Blockchain Internet of vehicles security Authentication Privacy security

0 引 言

车联网技术革命性的发展,让车联网环境中的车辆终端可以利用传感器及其他车载单元实现车与车、车与人、车与基础设施、车与云等 V2X(Vehicle to Everything)间的信息交互,通过对这些信息进行合理的采集、处理可大大减少交通事故及交通拥堵等问题。目前,车联网的安全问题重点集中在身份认证、数据隐私保护、系统安全三个方面。传统的密码安全技术[1-3]已不能满足车联网环境高分散、高动态及低延迟的特性,区块链技术的出现,其去中心化、分布式存储、不可篡改、高度安全的特征,可以较好地解决现阶段车联网的安全需求。因此近几年,将区块链与传统安全技术结合以解决车联网安全问题已经成为国内外该领域的研究热点。

1 区块链在车联网安全中的研究现状

区块链作为比特币的底层技术,于 2008 年由 Nakamoto[4] 首次提出,并开始进入人们的视线。本质上区块链就是一个分布式数据库,用来记录交易信息,但它与传统分布式数据库最大的不同在于其单个节点亦可对全局数据进行处理,摆脱了传统分布式数据库的权力中心化。同时,由于区块链特殊的数据结构,让整个区块链系统中的所有节点在数据、权限、安全等方

收稿日期:2021-02-23。国家自然科学基金项目(61772047);北京电子科技学院一流学科建设项目(3201017)。**曾萍**,教授,主研领域:车联网安全,区块链安全。**闫坤**,硕士生。**赵耿**,教授。**马英杰**,副教授。

面均平等,并且一旦数据存储入区块链后便不可任意篡改。除此之外,区块链系统中还包含加密算法、P2P(Peer to Peer)网络、智能合约、共识机制等,这些技术的共同作用下,造就了区块链的诸多特征[5]。利用区块链的特性去解决车联网环境在不断发展的过程中所暴露出的缺陷汇总如表 1 所示。

表 1 区块链技术特点及其在车联网安全中的应用

区块链特点	在车联网中的应用	目标
去中心化	将集中控制的网络分散至多个实体独立控制	降低系统数据泄露的风险; 增强用户体验
分布式存储	对接入网络的所有节点进行数据同步与复制,避免单点故障造成的数据差异	提高系统鲁棒性; 保护数据安全与隐私
不可篡改	为车联网系统提供高度可信的信息存储方案	信息防篡改
共识机制	为车联网环境中不受信任的实体间建立互信机制	提高信息传输效率
智能合约	消除车联网系统对第三方机构的依赖	降低运营成本; 避免信息泄露

RSU(Road Side Unit)作为车联网通信的主要组成部分,建设在道路旁边或车道上方,利用无线信道与车载单元进行实时高速通信。一般来说,RSU 在计算能力、信息存储、抵御攻击等方面远优于 OBU(On-Board Unit),因此目前大多数方案将区块链部署在 RSU 中,实现车联网系统分布式管理。

1.1 车辆身份认证

目前,针对车联网认证安全的研究主要分为基于嵌入式安全模块终端的结构研究[6]和基于身份的加密机制的研究[7]两类。对于前者而言,由于身份认证和授权在物理层实现,认证效率可大幅度提升,同时认证双方的信号均在各自物理层的接收并检验,从而可避免信号被恶意攻击者利用,但其最大的缺陷就是认证模块成本高,并且针对不同认证模块,其安全性也会存在很大的差异。而对于后者,由于公钥的基础结构对证书的依赖较少的缘故,可以在保障安全的同时减少通信负担。因此基于公钥的区块链技术在车联网认证方面的应用得到了广泛的探讨,同时借助智能合约亦可消除传统认证方案中对第三方机构的依赖。

对于基于身份的加密机制类方案,车联网节点的身份验证通过中心节点完成,这就对中心节点的安全与通信能力提出了很高的要求,在此之前诸多方案[8-10]均是通过增强中心节点的安全性、提高其通信能力来满足车联网的安全需求,区块链借助其去中心化的特征为此提出了新的方案,对于区块链在车联网场景的部署主要有 TA(Trusted Authority)、RSU 和车辆之间两种。

大多数现有身份验证协议都与集中式结构和单个 TA 网络模型有关,因此车辆只能通过中间节点 RSU 与一个 TA 进行相互身份验证,这样的结构导致身份验证协议的效率极易受到 TA 的通信能力及计算资源的影响。在文献[11]中,针对车联网环境,作者基于区块链技术设计了一种 RSU 辅助的多 TA 网络系统,用于实现身份验证及密钥协商,其架构如图 1 所示。由于 RSU 计算资源较为丰富,此系统借助中间点 RSU 帮助 TA 与车辆节点之间实现相互认证,在认证过程中,协议通过智能合约检查认证请求信息在区块链中是否存在,同时由于架构中区块链网络由所有的 TA 组成,数据信息可在节点间即时同步,这解决了 TA 计算和通信瓶颈所导致的认证效率低的问题,同时也解决了车辆跨 TA 认证的问题。

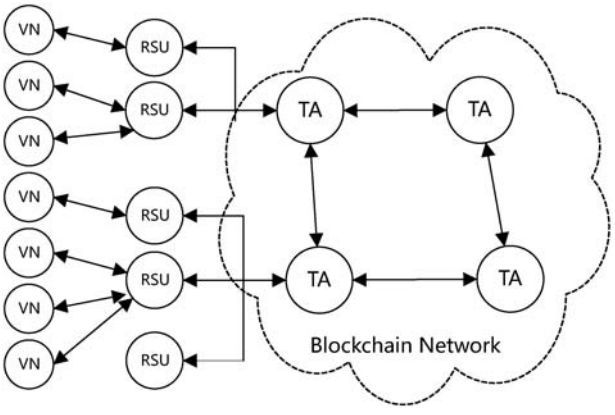

图 1 基于区块链的多 TA 网络模型

文献[12]引入区块链技术对车联网的架构进行改进:删除了中心节点,将所有节点功能权限平等化,同时系统借助基于时间序列和 gossip 协议的拜占庭共识算法实现去中心化的共识认证。由于不存在中心节点,车辆与 RSU 均为时区块链的平等节点,因此认证速度大大提高,同时拜占庭共识算法提升了整个系统服务效率。Mendiboure 等[13]利用区块链技术为已集成 SDN 技术的 IoV 架构构建新的身份验证和授权系统,在本系统中作者为 SDN 控制器和应用程序提供了一种 SD-IoV 可信赖的安全环境,即便是某一应用程序遭到攻击者的破坏,由于区块链的分布式特性,也不会对整个车联网系统产生太大的影响。

除了借助区块链技术实现认证的中心化外,Wang 等[14]利用区块链框架开发出一套新的证书颁发机制,通过将区块链与 PKI 身份验证机制相结合来解决车辆、服务器及 RSU 之间的身份认证,同时解决用户账户的管理问题。利用区块链对用户信息存储时,借助其加密特征对车辆身份信息进行加密处理,防止隐私

信息泄露。认证过程中,当 RSU 接收到车辆的身份 ID 及公钥信息时,对其进行有效性判断,然后将车辆信息发送给云服务提供商,由共识机制控制的多个云服务提供商收到信息后,查询车辆 ID 来确定车辆的身份,并通过 RSU 将证书颁发给车辆,同时将车辆信息记录在区块链中,与其他云服务提供商之间进行信息同步。Zhou 等[15]基于区块链技术设计出一种存储已连接汽车身份信息的块结构,并借助散列函数和非对称密码算法实现在不泄露私人信息的前提下对互联网汽车进行身份验证。Vangala 等[16]设计了一种新的基于区块链及证书的认证方案 BCAS-VADN,用于解决车联网环境中的事故检测等问题,通过该认证机制在 IoV 系统中的事故报告的各个参与者之间建立密钥,来保证报告的透明性与不变性。同时针对车辆的证书管理问题文献[17 - 18]也给出了基于区块链的解决方案。

1.2　车辆数据隐私保护

据调研预计到 2025 年,中国车联网市场的总体规模将达 2 100 亿美元[19]。巨大的经济市场下,对于车联网系统中的大量数据,如何在保证隐私的情况下进行安全存储、传输及共享是亟需解决的问题。同时在复杂的交通环境中,V2X 之间只有建立了可靠的互信关系后,才可保证数据的安全共享,因此对环境中车辆的信誉问题也需要进行衡量与管理。

对于车联网系统的隐私问题,大多数采用文献[20 - 21]的方案采用车辆的请求信息进行加密来解决,然而大多数加密算法复杂度高,无法满足车联网环境的实时性要求。相对而言,假名、匿名等方式更能满足通信与服务需求。

Pu 等[22]利用区块链设计出一种高效可靠的车联网隐私保护方案,方案借助化名机制通过隐藏车辆的真实身份信息来实现匿名化。在方案中边缘站点会为其所管理范围内的车辆随机分配 GroupID 作为车辆的通信假名,并且 GroupID 会不间断随机更新,保证 GroupID 的有效性。在车辆通信及消息验证过程中,云服务提供商为区块链的主要节点,边缘站点为共识节点,通过 PBFT 共识将经过验证过的消息存储在链中,同时根据 GroupID 追溯虚假消息的发送车辆,进行进一步的处理。在整个通信过程中,消息均是通过 GroupID 进行交互,车辆的隐私信息并未暴露在系统内,从而在保证车辆的隐私的条件下满足车辆的服务需求。同样借助区块链去中心化、分布式、集体维护的特点,Li 等[23]设计出新型的去中心化 VANET 架构,通过动态阈值加密和 k-匿名两种方式实现 VANET 中实体之间的集中化、互不信任、身份和位置隐私等问题。Cebe 等[24]将车辆的公钥的基础架构(VPKI)集成在区块链中,并且将与车辆有关的信息散列化后存储入分布式账本中,同时使用假名技术对车辆身份进行识别,全方位保护车辆和用户的隐私安全。Bao 等[25]为将区块链用于车联网的分散化假名管理系统中,区块链的去中心化以及工作量证明两大特征让此系统对已知的隐私问题及安全攻击更具弹性。

零知识证明在不向验证者提供任何有用信息的情况下实现双方对某一论断的共识,在区块链的隐私保护方面有广泛的应用[26 - 27]。文献[28]提出了一种基于零知识证明的用于车联网系统的分散式位置隐私保护空间众包方案 PriSC,它可以使车辆用户安全地参与空间众包,同时确保任务的位置策略隐私并为车辆的位置提供多级隐私保护。PriSC 系统架构如图 2 所示,借助区块链来消除空间众包服务器对车辆用户数据的控制,将加性同态加密和基于圆的位置验证结合在一起,来保证确保任务位置策略的机密性,利用车辆所处位置的网格大小来实现其位置的多级隐私保护,而此网格的大小由车辆用户自己设定,保障隐私保护的动态性。在消息验证过程,对记录在区块链中的订单信息验证通过零知识证明实现双方的共识。除此外,文献[29 - 31]也同样借助零知识证明来解决融合系统中的隐私问题。

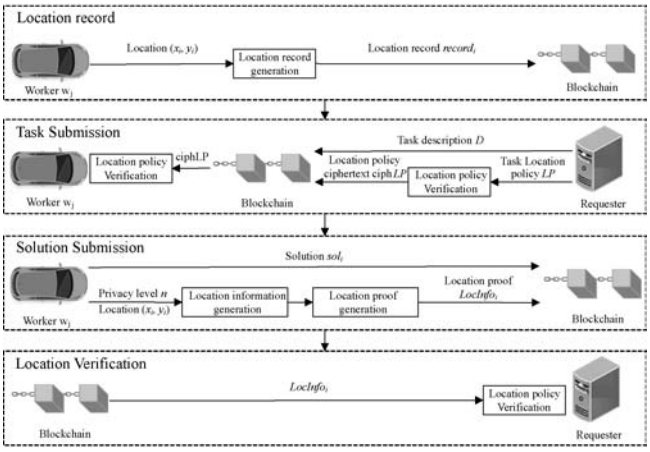

图 2　PriSC 系统架构

完善的信誉管理方案对于车联网环境尤为重要,同样基于信誉的数据信息共享系统也更容易保证系统内数据的安全可信。如文献[32]中,作者在基于区块链的车联网系统中引入 DPoS(Delegated Proof-of-Stake)共识机制,同时借助基于信誉的投票机制来选择矿工,以及智能合约来激励待命矿工去参与区块的验证,确保整个数据上链过程完整与可靠。整个方案分为两个阶段,第一阶段首先通过衡量车辆过去的信息交互情况以及其他车辆的推荐意见,借助多权重的主观逻辑

方案来计算矿工候选人的声誉值,然后通过基于信誉的投票方式来选择矿工,具有较高声誉的候选人被选为活跃矿工和备用矿工。第二阶段激励备用矿工使用智能合约参与区块信息的验证,进一步防止活跃矿工的内部串通,对信息数据进行造假。同样地,在文献[33]基于联盟链为车联网环境设计出信誉机制,来确保链上数据与链下数据之间的互信,通过基于数据质量的拍卖模型,来实现对数据评估的期望最大化,由此保证链上与链下之间的数据互信。文献[34 – 35]同样借助区块链技术,构建出集信誉管理、隐私保护、数据共享于一体的车联网安全系统,在保证数据可信赖的同时又起到保护车辆隐私的效果。

1.3 系统安全构建

随着对融合方案的不断研究,基于区块链技术的车联网应用场景逐渐形成如图 3 所示的安全架构模型[36]。

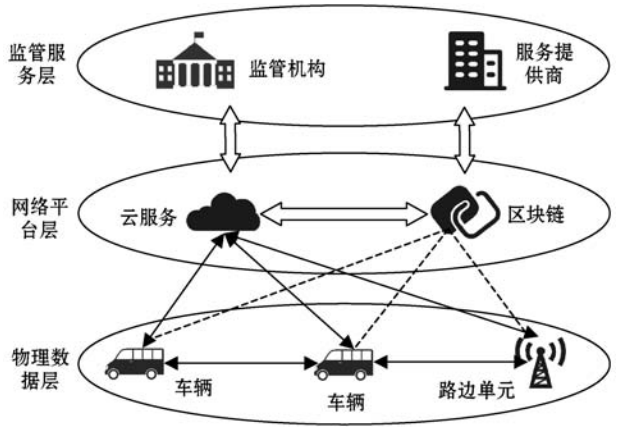

图 3 基于区块链的车联网安全架构模型

图 3 中物理层主要由车联网环境中的车辆、路边单元等设备组成,在基于区块链的车联网系统中,这些也是区块链的各个数据节点。物理数据层主要是利用车载传感器、车载单元对路况信息进行采集然后与路边单元进行信息交互,为网络平台层提供数据支撑;而处于中间的网络平台层大都包含有区块链和云服务平台,区块链主要用于对底层的数据进行存储,以及处理各个节点间的共识,而云服务主要是对数据进行进一步的处理来满足上下层的需求;监管服务层主要包括交通监管部门、汽车服务提供商、车联网技术提供商、保险公司等,它们可以对从网络平台层拿到的数据进行统计分析来处理车联网环境中的各类事务,保证交通环境良好有序地发展。

Singh 等[37]利用区块链技术提出一种新的基于区块链的分散式安全系统,通过可互操作框架对车辆健康情况的处理,全面提升车联网系统的安全性、可用性、可靠性等。同样 Narbayeva 等[38]提出一种基于区块链技术的车联网服务基础设施安全机制,该机制通过追踪和记录区块链中车联网设备的每个动作来实现客户和出租车驾驶员之间的机密性和透明性,达到提升网络安全性的目的。除此之外,针对区块链共识机制算力大、区块链系统内部隐私透明等问题,在融合系统的构建方面常常还会将其他相关技术融入,具体如表 2 所示。

表 2 其他技术在系统安全构建中的作用

技术	作用	参考文献
边缘计算	• 对区块链中的计算资源进行管理 • 解决车联网设备无法承载的区块链中共识算法的资源消耗 • 平衡计算工作量,为终端设施提供实时的响应策略	文献[39 – 40]
云计算	• 解决区块的算力制约问题 • 动态分配网络资源,实现融合架构的低延迟、可伸缩及安全传输	文献[41 – 43]
软件定义网络	• 动态配置区块链网络,实现车联网节点在不同链间切换的交叉共识 • 虚拟化系统内的计算资源、网络资源,提升系统的吞吐率 • 抵御集成环境中的中间人攻击、分布式拒绝访问、窃听的恶意攻击	文献[44 – 45]
机器学习	• 解决区块链融合系统梯度计算过程中的数据持有者的隐私问题 • 检测并阻止融合网络中多数恶意攻击的发生 • 减少由于服务水平协议导致的网络延迟,提升系统服务质量 • 借助相似学习处理系统中具有争议的相关数据	文献[46 – 48]

还有不少方案结合多种技术构造更为完善的融合系统,如 Xiao 等[49]利用 SDN、边缘计算、区块链结合机器学习(贝叶斯网络)为车联网设计出可用来监测虚假消息的网络计算框架 QcFND,系统主要部署在集成 SDN 和区块链技术的 SDRSU 中,其中 SDN 控制器用于实现车联网系统的负载平衡,而区块链用于记录车辆提交的报告。再利用贝叶斯网络对消息的先验概率、持续时间、车辆信誉及收集到的报告进行综合评估得到后验概率进行进一步判断,实现消息真伪性的检测。

2 性能评估

现有如 Bitcoin、Ethereum 等区块链平台由于其共识机制等原因导致能源消耗的问题日趋凸显,基于这些平台构建的车联网系统自然也存在这样的缺陷。本

节着重对算力消耗以及融合系统方案的评估进行讨论。

2.1　能耗与算力制约

由于区块链特殊的数据结构设计,导致其需要花费大量能源去实现共识。据统计,比特币系统单笔交易耗电约为 623.47 kWh,相当于美国一个普通家庭 21.07 天的用电量。通过计算,就年度能耗而言比特币系统是 VISA 的 75 倍[50],由此可见,就单纯的区块链系统而言,能耗问题就已值得去重点关注。

同时对于车联网设备而言,其哈希率通常用单位 MH/s 来衡量,而对于大多数挖矿机器,其算力均用 TH/s 来衡量,由此可见传统车联网设备很难去满足区块链挖矿的巨大算力[51]。相较于专业挖矿设备而言,车联网等物联网设备其传感器及 CPU(Central Processing Unit)的数据计算、处理能力有限,并且能源供应与存储空间也相对有限,同时高动态的车辆让高质量的网络通信难以保证,这就使得对硬件、能源、网络要求较高的区块链很难达到较高的算力水平,进而影响整个融合系统的信息处理能力,同时也增加了整个系统的信息处理时间。

针对能耗与算力制约问题,目前的解决方案主要有两种:第一种即文献[41 - 42,44],借助云计算、边缘计算将算力分摊至 RSU、云服务器、边缘设备等算力较强的终端,减缓车载单元的运算能耗;第二种如文献[52 - 54]基于交通环境及现有交通管理手段设计适合车联网环境的轻量级共识机制,在满足交通管理的情况下,解决共识机制带给车联网系统的算力问题。

并且大部分车联网平台,其通信与存储空间均有限,如大多数车联网低功耗节点内存均以 KB 来衡量,而区块链大多数节点其内存衡量单位基本为 GB[55]。因此目前针对基于区块链的车联网系统数据存储的研究基本采用链上链下混合解决方案,通常将车辆地理位置、速度、车主信息等涵盖车辆隐私安全的数据存放在链上,而其他不重要的数据利用传统技术进行链下存储,如此来缓解当前将区块链应用于车联网系统的存储小、算力弱、能耗高等缺陷。

2.2　方案性能评估

就目前而言,用于模拟仿真设计好的方案的系统,大多暂未考虑对融合技术的全面评估,因此无法尽可能接近现实场景对方案进行模拟与评估。针对前面给出的参考文献,本节对文献中已标注的模拟仿真平台进行比较,结果如表 3 所示。

表 3　仿真平台统计

文献	仿真平台	仿真内容
[14]	OMNet ++, SUMO, Veins	基于区块链系统的加密耗时 基于区块链系统的通信开销 基于区块链的认证效率
[18]	Hyperledger Caliper	系统可伸缩性评估; 交叉认证及访问控制性能评估
[20]	SUMO	不同环境下系统的计算开销与通信开销; 方案的灵活性
[23]	OPNET, Ethereum	系统处理信息的耗时情况; 系统内车辆平均间距对隐私保护的影响
[25]	OMNet ++	系统内假名重用频率,并量化重用效率; 系统处理任务规模与耗时的关系
[32]	MATLAB	信誉机制的性能; 基于智能合约的激励政策的性能

像文献[14]所使用的仿真框架总体基于 OMNet ++ 来实现,而对车辆的运行状态使用 Veins 来实现,同时又利用库 Eigen 实现中继节点对数据包的存储、组合及转发性能的评估,最后利用 SUMO 来评估集成了区块链的车联网系统的性能。就目前来说,Veins 作为车联网仿真开源框架,主要用于仿真的参数设置、事件的运行、检测及模拟,而 OMNeT ++ 主要用于对设计好的方案进行离散化的网络模拟,SUMO 旨在对道路交通进行模拟。最常用的这三个仿真平台只是单纯地用于模拟车联网环境,而缺少对区块链技术进行特殊优化。而在文献[32]作者为了测试融合系统中区块链的性能情况而选择了 MATLAB 作为仿真平台,但又一定程度上忽略了车联网性能方面的测试。

3　安全性分析

对于区块链技术而言,其分布式账本旨在为通信双方提供安全有效的信息传输方式,却无法验证用户所传输数据信息的正确性,这使得攻击者可通过恶意节点来向系统传输不正确的数据信息,进而破坏整个系统[56]。现有区块链共识机制并未将此类情况考虑其中,虽然目前可通过历史数据及车辆周围设备来验证信息的安全、正确,避免恶意节点的信息传输,但此类方法存在太大的局限性,并且对于节点相对较少的情况下,若攻击者同时控制了 51% 节点,那就相当于掌握了整个融合系统的控制权[57]。除上述攻击情况外,针对区块链的威胁最大攻击还有 Sybil 攻击、Eclipse 攻击和 DDoS 攻击,其具体特征如表 4 所示[58],车辆作为

将区块链应用于车联网后的系统节点,攻击者完全可以借助一辆或者多辆汽车实现上述三种攻击方式,对整个系统造成不可挽回的损失。因此针对融合系统去设计特定的共识机制,以及引进区块链中针对各类攻击的预防措施也是当下融合系统设计时亟需解决的问题之一。

表 4 三种攻击对比

特征	Sybil 攻击	Eclipse 攻击	DDoS 攻击
方法	恶意节点伪造多重身份对单个节点进行攻击	添加足够多的虚假节点至被攻击节点周围	借助 C/S 技术,联合多台攻击设备实现成倍提高拒绝服务攻击
途径	虚假节点接入 误导节点路由 发布虚假资源	侵占节点路由破坏网络拓扑分割网络连接	主动:向攻击节点发送虚假信息,攻击消息后访者; 被动:等待节点请求,发送虚假信息
影响	单个节点影响大 网络整体影响小	单个节点致命网络整体影响小	网络整体致命
措施	每个节点接入前进行身份认证	限制主动连接的节点数目	尽可能保持服务,同时可迅速恢复服务

自区块链 2.0 引入智能合约后,智能合约在所有区块链中承担起重要的作用。然而 the DAO 事件的出现[59],让开发者认识到对智能合约的开发不可仅限于功能的探究,还要保证它的安全防护。与大多数基于区块链的金融系统不同,对于基于区块链的车联网的系统而言,若系统中的智能合约中存在漏洞,被黑客利用攻击,那么将会直接威胁到整个交通系统的安全。

4 研究展望

区块链在车联网安全领域的应用注定会成为焦点,但目前仍处于研究的初级阶段,针对现阶段研究中出现的问题,本文认为未来基于区块链的车联网安全系统发展研究方向有以下三个方面:

(1) 结合交通环境设计适合车联网的新型共识机制。现有工作量证明、权益证明、委托权益证明、验证池等共识机制几乎都是针对数字货币设计,由于用于计算的服务器算力充足,因此这类共识机制大都只考虑如何更好地解决交易过程中的各类作假问题,而用于车联网中的共识机制在保证共识的前提下,需要着重考虑算力和能耗的问题,可以尝试结合交通规则、车辆信息、交通环境、驾驶员信息等数据对需要共识的事件进行衡量,来替换传统共识机制中大量哈希计算或反复的投票过程,从而实现可部署在车辆终端的轻量级共识机制。

(2) 针对第 1 节提到的三大将区块链应用于车联网安全的场景,特别是隐私类,也存在着值得探究的方向。目前对于基于公有链的融合系统而言,所有存储在区块链账本中的数据均是对内公开透明的,倘若攻击者入侵系统后,那么所有系统内车辆的数据、交易、位置等隐私信息则会通通泄露。1.2 节中提到的相关方案,大都是借助区块链技术实现融合系统内各个车辆间自身的隐私问题,而尚未将区块链系统自身无隐私的特征考虑进去,这就导致倘若融合系统被入侵,其对外便毫无隐私可言。对于此类问题,可考虑在车辆间部署私有链或联盟链,同时借助同态加密,零知识证明等手段对重要的隐私信息进行隐藏,两方面保证隐私数据的安全。

(3) 如何在满足车联网环境的情况下,对融合系统中区块链性能进行完整有效的仿真评估,目前仍然没有一个切实可行的解决方案,现有解决手段都是针对不同的部分,分开进行仿真评估,这也就会导致评估结果缺乏完整性。在未来的研究中可以尝试去设计针对基于区块链的车联网仿真平台,或是在现有平台的基础上设计符合仿真需求的插件,让仿真结果更加真实准确。

5 结 语

一种技术的发展初期,研究人员更着眼于此技术的功能与构建,但随着技术的不断发展,其漏洞和不足便会慢慢显现。针对车联网发展过程中出现的安全问题,区块链的引入为其带来了新的机遇。本文分析并总结区块链在车联网环境中车辆身份认证、数据隐私保护及系统安全构建三方面的安全应用,同时对融合方案的性能评估问题及安全性问题进行研究,最后对未来的挑战与发展进行展望。

随着车联网技术不断发展,应用于其中的其他相关技术也愈来愈多,当使用其他技术来弥补自身技术的缺陷时,其他技术的缺陷也被带入其中。因此,未来针对将区块链应用于车联网,在不断更深层次地完善融合技术外,还需要借助其他技术去弥补区块链自身的缺陷。与此同时,随着 5G 通信技术的大规模商用,车联网及区块链的网络综合性能会进一步提升,这使得两者间的融合更为完善与深入。

参 考 文 献

[1] Lo N, Tsai J. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without

pairings[J]. IEEE Transactions on Intelligent Transportation Systems,2016,17(5):1319 – 1328.

[2] Florian M, Finster S, Baumgart I. Privacy-preserving cooperative route planning[J]. IEEE Internet of Things Journal, 2014,1(6):590 – 599.

[3] Wu H, Horng G. Establishing an intelligent transportation system with a network security mechanism in an Internet of vehicle environment[J]. IEEE Access, 2017, 5: 19239 – 19247.

[4] Nakamoto S. A peer-to-peer electronic cash system[EB/OL]. (2008 – 12 – 14)[2021 – 02 – 23]. https://bitcoin.org/bitcoin.pdf.

[5] Mollah M, Zhao J, Niyato D, et al. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey[J]. IEEE Internet of Things Journal,2020,8(6): 4157 – 4185.

[6] Soni N, Malekian R, Andriukaitis D, et al. Internet of vehicles based approach for road safety applications using sensor technologies[J]. Wireless Personal Communications,2019, 105:1257 – 1284.

[7] Liu S, Zhang Y, Liu Y, et al. An 'Internet of Things' enabled dynamic optimization method for smart vehicles and logistics tasks[J]. Journal of Cleaner Production,2019,215: 806 – 820.

[8] Lo N, Tsai J. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings[J]. IEEE Transactions on Intelligent Transportation Systems,2015,17(5):1319 – 1328.

[9] Liu Y, Wang Y, Chang G. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm[J]. IEEE Transactions on Intelligent Transportation Systems,2017,18(10):2740 – 2749.

[10] He D, Zeadally S, Xu B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security,2015,10(12):2681 – 2691.

[11] Xu Z, Liang W, Li K, et al. A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles[J]. Journal of Parallel and Distributed Computing,2021,149:29 – 39.

[12] Hu W, Hu Y, Yao W, et al. A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles[J]. IEEE Access, 2019, 7: 139703 – 139711.

[13] Mendiboure L, Chalouf M, Krief F. Towards a blockchain-based SD-IoV for applications authentication and trust management[C]//International Conference on Internet of Vehicles,2018:265 – 277.

[14] Wang X, Zeng P, Patterson N, et al. An improved authentication scheme for internet of vehicles based on blockchain technology[J]. IEEE Access,2019,7:45061 – 45072.

[15] Zhou Y, Liu Q, Liu M, et al. Research on blockchain-based identity verification between IoV entities[C]//2020 International Conference on High Performance Big Data and Intelligent Systems,2020:1 – 6.

[16] Vangala A, Bera B, Saha S, et al. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems[J]. IEEE Sensors Journal,2020,21(14):15824 – 15838.

[17] Cho E, Perera M. Efficient certificate management in blockchain based internet of vehicles[C]//2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing,2020:794 – 797.

[18] Mendiboure L, Chalouf M, Krief F. A scalable blockchain-based approach for authentication and access control in software defined vehicular networks[C]//2020 29th International Conference on Computer Communications and Networks, 2020:1 – 11.

[19] Du J, Ouyang D. Progress of Chinese electric vehicles industrialization in 2015: A review[J]. Applied Energy, 2017,188:529 – 546.

[20] Sherif A, Rabieh K, Mahmoud M, et al. Privacy-preserving ride sharing scheme for autonomous vehicles in big data era [J]. IEEE Internet of Things Journal, 2016, 4(2):611 – 618.

[21] Li H, Yang Y, Luan T, et al. Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data[J]. IEEE Transactions on Dependable and Secure Computing,2015,13(3):312 – 325.

[22] Pu Y, Xiang T, Hu C, et al. An efficient blockchain-based privacy preserving scheme for vehicular social networks[J]. Information Sciences,2020,540:308 – 324.

[23] Li H, Pei L, Liao D, et al. Blockchain meets VANET: An architecture for identity and location privacy protection in VANET[J]. Peer-to-Peer Networking and Applications, 2019,12:1178 – 1193.

[24] Cebe M, Erdin E, Akkaya K, et al. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles[J]. IEEE Communications Magazine,2018,56(10):50 – 57.

[25] Bao S, Cao Y, Lei A, et al. Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems[J]. IEEE Access,2019,7: 80390 – 80403.

[26] Goldwasser, S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems[J]. SIAM Journal on computing,1989,18(1):186 – 208.

[27] Sasson E, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin [C]//2014 IEEE Symposium on Security and Privacy, 2014: 459 - 474.

[28] Zhang J, Yang F, Ma Z, et al. A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(4): 2299 - 2313.

[29] Huang H, Zhu P, Xiao F, et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data[J]. Computers and Security, 2020, 99: 102010.

[30] Gabay D, Akkaya K, Cebe M. A privacy framework for charging connected electric vehicles using blockchain and zero knowledge proofs[C]//2019 IEEE 44th LCN Symposium on Emerging Topics in Networking, 2019: 66 - 73.

[31] Kouicem D, Bouabdallah A, Lakhlef H. An efficient and anonymous blockchain-based data sharing scheme for vehicular networks[C]//2020 IEEE Symposium on Computers and Communications, 2020: 1 - 6.

[32] Kang J, Xiong Z, Niyato D, et al. Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2906 - 2920.

[33] Chen W, Chen Y, Chen X, et al. Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees [J]. IEEE Internet of Things Journal, 2019, 7(3): 1625 - 1640.

[34] Javaid U, Aman M, Sikdar B. DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts[C]//2019 IEEE 89th Vehicular Technology Conference, 2019: 1 - 5.

[35] Lu Z, Wang Q, Qu G, et al. Bars: A blockchain-based anonymous reputation system for trust management in VANETs [C]//2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, 2018: 98 - 103.

[36] Liu J, Zhang G, Sun R, et al. A blockchain-based conditional privacy-preserving traffic data sharing in cloud[C]// ICC 2020 - 2020 IEEE International Conference on Communication, 2020: 1 - 6.

[37] Singh P, Singh R, Nandi S. V-CARE: A blockchain based framework for secure vehicle health record system [EB]. arXiv: 2007. 13647, 2020.

[38] Narbayeva S, Bakibayev T, Abeshev K, et al. Blockchain technology on the way of autonomous vehicles development [J]. Transportation Research Procedia, 2020, 44: 168 - 175.

[39] Xiao K, Shi W, Gao Z, et al. DAER: A resource pre-allocation algorithm of edge computing server by using blockchain in intelligent driving [J]. IEEE Internet of Things Journal, 2020, 7(10): 9291 - 9302.

[40] Guo S, Dai Y, Guo S, et al. Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5549 - 5561.

[41] Qiu C, Yao H, Jiang C, et al. Cloud computing assisted blockchain-enabled Internet of Things [J]. IEEE Transactions on Cloud Computing, 2019, 10(1): 247 - 257.

[42] Jiao Y, Wang P, Niyato D, et al. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(9): 1975 - 1989.

[43] Tosh D, Shetty S, Liang X, et al. Data provenance in the cloud: A blockchain-based approach [J]. IEEE Consumer Electronics Magazine, 2019, 8(4): 38 - 44.

[44] Qiu C, Yu F, Xu F, et al. Blockchain-based distributed software-defined vehicular networks via deep q-learning [C]//8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 2018: 8 - 14.

[45] Aujla G, Singh M, Bose A, et al. BlockSDN: Blockchain-as-a-service for software defined networking in smart city applications[J]. IEEE Network, 2020, 34(2): 83 - 91.

[46] Podgorelec B, Turkanović M, Karakatič S. A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection[J]. Sensors, 2020, 20(1): 147.

[47] Xiong W, Li X. Smart contract based data trading mode using blockchain and machine learning [J]. IEEE Access, 2019, 7: 102331 - 102344.

[48] Adhikari A, Rawat D, Song M. Wireless network virtualization by leveraging blockchain technology and machine learning[C]//ACM Workshop on Wireless Security and Machine Learning, 2019: 61 - 66.

[49] Xiao Y, Liu Y, Li T. Edge computing and blockchain for quick fake news detection in IoV[J]. Sensors, 2020, 20(16): 4360.

[50] Ma J, Gans J, Tourky R. Market structure in bitcoin mining [C]//National Bureau of Economic Research, 2018.

[51] Liu Y, Wang K, Lin Y, et al. LightChain: A lightweight blockchain system for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3571 - 3581.

[52] Zheng Z, Pan J, Cai L. Lightweight blockchain consensus protocols for vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5736 - 5748.

(下转第 27 页)

位置与夹爪实际抓取位置进行比较,计算两者之间存在的相对误差,得到的实验数据如表 2 所示。

表 2　实验数据分析　　单位:mm

序号	计算位置	夹爪位置	位置误差
1	(221.38, -81.80, 688.00)	(216.08, -86.53, 681.80)	(5.30,4.73, 6.20)
2	(256.89,79.33, 686.21)	(251.94,72.93, 679.11)	(4.95,6.40, 7.10)
3	(284.22,57.84, 687.30)	(289.72,51.72, 679.00)	(-5.50,6.12, 8.30)
4	(337.21, -70.40, 689.10)	(331.21, -65.52, 683.50)	(6.00, -4.88, 5.60)
5	(363.46,107.62, 687.60)	(356.07,114.42, 679.50)	(7.39, -6.80, 8.10)
6	(425.57, -121.15, 688.20)	(417.15, -127.85, 684.60)	(8.42,6.70, 3.60)
7	(573.64,132.11, 686.90)	(562.34, -139.91, 681.00)	(11.30, -7.80, 5.90)

在 X 轴方向的误差范围为 -5.50 ~ 11.30 mm,在 Y 轴和 Z 轴方向的误差范围在 10 mm 以内。由于目标物体本身的高度为 20 cm,对于抓取的影响比较小可以满足实验的要求。从位置 1 到位置 7,随着距离的增大位置误差也在不断增大,且位置 7 未实现抓取。造成这个现象的原因可能是随着距离增大,识别的误差也在增大,且机械臂对于边缘点的抓取不是很准确,因此未能完成此次实验。

5　结　语

本文以 ROS 作为开发平台,对基于机器视觉的抓取进行设计。首先对图像进行预处理,利用颜色识别获取目标位置信息,然后通过坐标转换得到相对于机械臂的位置,最后完成目标抓取。通过实验数据验证了系统的可行性和可靠性。对于机械臂自主抓取研究有重要意义。

参　考　文　献

[1] 张劲恒,魏郅琦. 工业机器人及智能制造发展现状分析[J]. 记者观察,2018(36):112.

[2] Yamamoto H. A view of construction science and robot technology implementation[C]//37th International Symposium on Automation and Robotics in Construction, 2020.

[3] 张文辉,叶晓平,季晓明,等. 国内外空间机器人技术发展综述[J]. 飞行力学,2013,31(3):198 - 202.

[4] 董靖川,张成君,王一成,等. 面向机器人智能抓取任务的视觉定位实验[J]. 实验技术与管理,2020,37(3):56 - 59.

[5] 郑振峰. 基于机器视觉运用于工业机器人抓取技术的研究[J]. 南方农机,2020,51(15):46 - 47,52.

[6] 徐呈艺,刘英,贾民平,等. 木板抓取机器人手眼标定方法[J]. 农业机械学报,2019,50(12):420 - 426.

[7] 杜惠斌,宋国立,赵忆文,等. 利用 3D 打印标定球的机械臂与 RGB-D 相机手眼标定方法[J]. 机器人,2018,40(6):835 - 842.

[8] 朱明秀. 基于图像处理技术的车牌识别方法研究[J]. 信息记录材料,2019,20(3):224 - 226.

[9] 侯宾,张文志,戴源成,等. 基于 OpenCV 的目标物体颜色及轮廓的识别方法[J]. 现代电子技术,2014,37(24):76 - 79,83.

[10] 王鹏,王太勇,董靖川. 基于 EEMD 时频谱二值化的振动信号微弱特征提取方法[J]. 天津大学学报(自然科学与工程技术版),2016,49(7):667 - 673.

[11] Hassani N, Farnand S P. Color discrimination threshold for medical test devices[J]. Electronic Imaging, 2017(18): 60 - 66.

[12] 李金良,张斌,杨学顺,等. 6R 选矸机械臂运动学仿真分析[J]. 煤矿机械,2021,42(2):70 - 72.

(上接第 8 页)

[53] Chai H, Leng S, Zhang K, et al. Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles[J]. IEEE Access,2019,7:175744 - 175757.

[54] Su Z, Wang Y, Xu Q, et al. LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue[J]. IEEE Transactions on Dependable and Secure Computing, 2022,19(1):19 - 32.

[55] Ramachandran G, Krishnamachari B. Blockchain for the IoT: Opportunities and challenges[EB]. arXiv: 1805.02818,2018.

[56] Sun G, Dai M, Zhang F, et al. Blockchain enhanced high-confidence energy sharing in internet of electric vehicles[J]. IEEE Internet of Things Journal,2020,7(9):7868 - 7882.

[57] Wang Y, Su Z, Zhang N. BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network[J]. IEEE Transactions on Industrial Informatics,2019, 15(6):3620 - 3631.

[58] Zhou Z, Wang B, Dong M, et al. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems,2019,50(1):43 - 57.

[59] Maskey S, Badsha S, Sengupta S, et al. BITS: Blockchain based intelligent transportation system with outlier detection for smart city[C]//2020 IEEE International Conference on Pervasive Computing and Communications Workshop,2020: 1 - 6.