电信科学
Telecommunications Science
ISSN 1000-0801,CN 11-2103/TN

《电信科学》网络首发论文

题目：区块链在轨道交通边缘计算网络中的应用探讨
作者：谢高畅，卢华，唐琴琴，朱涵，梁成昊，文雯，谢人超
收稿日期：2021-03-01
网络首发日期：2021-10-20
引用格式：谢高畅，卢华，唐琴琴，朱涵，梁成昊，文雯，谢人超．区块链在轨道交通边缘计算网络中的应用探讨[J/OL]．电信科学.
https://kns.cnki.net/kcms/detail/11.2103.TN.20211019.1151.002.html

网络首发时间：2021-10-20 17:10:49
网络首发地址：https://kns.cnki.net/kcms/detail/11.2103.TN.20211019.1151.002.html

区块链在轨道交通边缘计算网络中的应用探讨

谢高畅[1,3]，卢华[2]，唐琴琴[1]，朱涵[1]，梁成昊[1]，文雯[1]，谢人超[1,3]
（1. 北京邮电大学网络与交换技术国家重点实验室，北京 100876；
2. 广东省新一代通信与网络创新研究院，广东 广州 510663；
3. 网络通信与安全紫金山实验室，江苏 南京 211111）

摘　要：多接入边缘计算（multi-access edge computing，MEC）能为城市轨道交通中的计算密集型业务和时延敏感型业务提供高质量的服务能力，然而轨道交通边缘计算网络中的大量边缘设施暴露在开放式环境中，其隐私保护和传输安全面临着很大的挑战。区块链（blockchain）具有分布式账本、共识机制、智能合约、去中心化应用等功能特性，因此，利用区块链可以为分布式轨道交通边缘计算网络构建系统性的安全防护机制，从而保障网络安全和数据安全，实现高质量的城市轨道交通服务。首先，介绍了区块链的基本概念；其次，设计了轨道交通边缘计算网络架构，提出了融合区块链的轨道交通边缘计算网络安全防护机制和应用实例；最后，对该安全防护机制面临的问题和挑战进行了分析和展望。

关键词：区块链；边缘计算网络；安全防护机制；城市轨道交通

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-0801.2021238

Application of blockchain in urban rail transit edge computing network

XIE Gaochang[1,3], LU Hua[2], TANG Qinqin[1], ZHU Han[1], LIANG Chenghao[1], WEN Wen[1], XIE Renchao[1,3]
1. State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Guangdong Communications & Networks Institute, Guangzhou 510663, China
3. Purple Mountain Laboratories, Nanjing 211111, China

Abstract: Multi-access edge computing (MEC) can provide high-quality service capabilities for computing-intensive services and delay-sensitive services in urban rail transit. However, many edge facilities in rail transit edge computing network are exposed to an open environment, and their privacy protection and transmission security are facing great challenges. Blockchain has functional characteristics such as distributed ledger, consensus mechanism, smart contract, and decentralized application. Therefore, the use of blockchain can build a systematic security protection mechanism for the distributed rail transit edge computing network to ensure network security and data security and realize high-quality urban rail transit services. Firstly, the basic concept of the blockchain and the urban rail transit edge computing network architecture were introduced. Then, the structure and application content of the

收稿日期：2021-03-01；修回日期：2021-10-18
通信作者：卢华，luhua@gdcni.cn
基金项目：北京市自然科学基金-丰台轨道交通前沿研究联合基金资助项目（No.L201002）
Foundation Item： Beijing Municipal Natural Science Foundation-Fengtai Rail Transit Frontier Research Joint Foundation（No.L201002）

rail transit edge computing network security protection mechanism integrated with the blockchain was discussed in detail. Finally, the open research issues and challenges of the security protection mechanism were analyzed.

Key words: blockchain, MEC network, security protection mechanism, urban rail transit

1 引言

近年来，我国城市轨道交通发展迅速，路网规模不断扩大，载客流量稳步上升，城市轨道交通成为了人们重要的出行方式[1]。城市轨道交通信息传输网络承载了轨道交通运行过程中的各类信息，保障轨道交通各个部门和环节的运行和管理的安全性和高效性[2]。随着城市轨道交通线路中的设备不断增多，城市轨道交通对通信网络服务质量的要求也越来越高。针对城市轨道交通网络中的计算密集型业务和时延敏感型业务，多接入边缘计算（multi-access edge computing，MEC）能满足其对缓存能力、计算能力、转发能力的需求，成为了实现城市轨道交通智能化的关键技术[3]。

在轨道交通边缘计算网络中，针对通信设施分布空间广阔、异构性强的特点，在车站子系统和车辆段子系统中部署边缘服务集群，将处理计算、应用服务、缓存转发等能力下沉到列车、车站、车辆段等网络底层，使边缘设备通过访问边缘服务器进行服务请求、任务卸载等工作，可以确保轨道交通时延敏感型业务的实时响应，并减少 IP 主干网络中的冗余流量。然而，由于边缘设备暴露在开放式环境中，数据隐私和通信安全不容易得到保障，同时异构设备使用的安全协议各不相同，插件化、填补化的防护方式难以满足其安全需求，因此从网络内部建立一套整体化的安全防护体系，是解决轨道交通边缘计算网络安全问题的关键[4]。

区块链（blockchain）技术的分布式可信、去中心化等特点为构建智能化交通边缘计算网络安全体系提供了新的思路[5]，文献[6]提出了利用区块链的分布式车辆数据管理系统，通过基于信誉的数据共享方案提高对异常车辆的检测率。文献[7]提出了一种智能交通信号管理体系，可以根据车辆的位置、间距等属性智能控制车辆通行并引入区块链保障运行记录数据和信号管理信令不可被篡改。尽管学界已经有一些研究人员针对基于区块链的交通边缘计算网络安全问题进行了研究，但目前该领域的研究主要针对道路上的特定设施及技术，缺乏考虑区块链在城市轨道交通边缘计算场景应用的实际问题，也没有深入研究如何在资源有限的轨道交通边缘设施上合理部署消耗较多资源的共识和证明机制[8]。

本文面向利用边缘计算网络对轨道交通边缘设备管控的场景，提出了一种分布式、多接入的轨道交通边缘计算网络架构，该架构通过轨道交通控制平台、线路主干网和边缘子系统 3 部分结构协同工作，实现边缘业务的低时延运行。针对该边缘计算网络架构在安全防护方面的问题，提出在边缘节点及核心服务器利用区块链构建网络安全防护机制，该机制利用边缘节点的冗余资源部署区块链安全系统，在边缘子系统、控制平台、外部网系统采取不同的安全防护及权限管控策略，实现安全可信的轨道交通边缘计算智能化系统。

2 区块链概述

自中本聪在 2008 年提出比特币系统后，区块链作为其核心技术受到了越来越多的关注。区块链不只应用于数字货币，它通过智能合约对多种金融场景进行优化，发展到近年来通过去中心化应用对包括轨道交通通信网络等各领域的认证和信任机制提供新型解决方案[9]。区块链的链式结构如图 1 所示[10]，主要由区块头（block header）和区块体（block body)构成。区块头中含有以下信息：块哈希（block hash)，包括上一个区块的哈希值；区块链的版本（version)，用于检验其遵循的区块链版本；时间戳（timestamp)，用来记录区块产生的时刻；随机数（nonce)，矿工对随机数进行计算，其他节点可以根据随机数验证是否符合条件。区块体中最重要的信息是事务（transaction，TX)，它是区块链中的数据记录。随着区块链技术的发展，出现了基于有向无环图（directed acyclic graph，DAG）的新型结构区块链[11]，但不同结构的区块链都具有共识机制、智能合约、去中心化网络等功能特点。

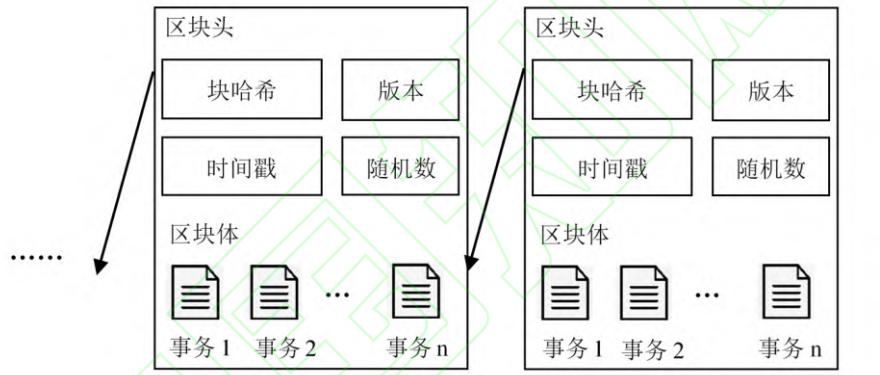

图 1　区块链的链式结构

（1）共识机制

区块链是一个分布式系统，由于不存在第三方账本管理机构，因此必须通过共识机制保障区块链系统中节点上账本的一致性。在拥有大量数据采集和存储设备的边缘计算网络内部署区块链，会造成随时有大量新的区块节点加入链中，因此需要选择合适的共识算法使整个区块链节点达成共识并尽量减少对边缘资源的消耗[12]。

（2）智能合约

智能合约是区块链中一种特殊的交易合约，大多数在区块链上的节点一旦将合约验证，合约就可以根据协议执行。当触发规定的条件时，节点会先去验证契约的合法性，然后由编译器执行代码，执行代码后新的事务产生，同时智能合约更新，最终所有的更新信息都被传输到区块链上，并受共识机制的验证。因此，当边缘计算网络中的用户向系统请求数据时，智能合约可以自动地对用户权限进行判定，之后返回相应数据[13]。

（3）去中心化网络

在区块链系统中，由于没有中心化节点，区块链上的节点通过共识和认证机制获得信任和不可篡改的信息。因此，去中心化网络依靠的是数据分布式存储与更新，并通过密码学算法提供认证信息。边缘网络中的异构交通设备将收集和转发的数据存入分布式数据库或分布式文件系统中，之后提取关键信息及其哈希值存入区块中，调用数据时，请求者通过信息共享智能合约请求数据，实现数据安全可信共享[14]。

3 轨道交通边缘计算网络架构

随着城市轨道交通规模的不断扩大，其通信网络数据量和接入的终端异构设备量出现了爆炸式增长，同时乘客对轨道交通服务质量的要求也越来越高，这些都要求轨道交通通信网络具备大带宽、低时延和多接入的网络能力。利用边缘计算网络对轨道交通边缘设备进行管控，并部署边缘服务器将处理数据、提供服务的能力下沉到接近用户的网络边缘，可以降低传输时延和成本，同时减少通信主干网的带宽压力[15]。本文基于轨道交通系统的层次体系，设计了一种城市轨道交通边缘计算网络。该网络的架构如图 2 所示，主要由 3 部分组成：轨道交通控制平台、轨道交通线路主干网和边缘子系统。这 3 部分结构协同工作，构成了由上而下的分布式、多接入的云-边缘网络，下面介绍它们各部分的设计原理。

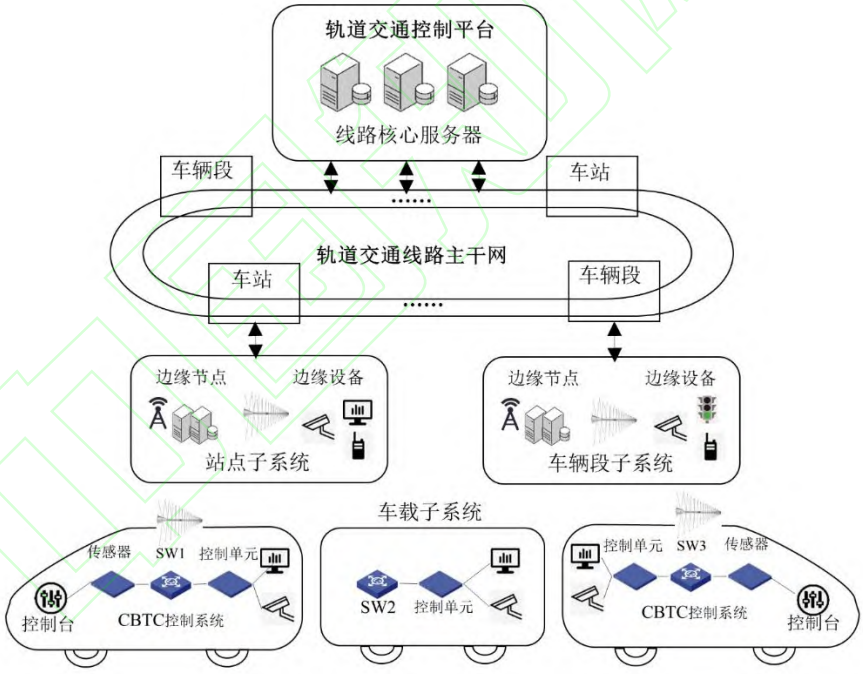

图 2 城市轨道交通边缘计算网络架构

（1）轨道交通控制平台

轨道交通控制平台是轨道交通边缘计算网络的云核心，它负责轨道交通线路关键数据的收集与处理。根据权限的不同，控制平台中的核心服务器可以管理单条线路或者多条线路，因此这些服务器所放置的位置也不同。管理单条线路的服务器放置在该线路的控制单元中，而管理多条线路甚至全部线路的核心服务器放置在轨道交通公司中，同时这些核心服务器可以选择使用云服务商的云计算服务，运行在第三方云计算平台上。另外，由于轨道交通与社会公共安全息息相关，在控制平台上还会有监管部门以及第三方机构的相关设备。

（2）轨道交通线路主干网

轨道交通线路主干网将各站点子系统、车辆段子系统以及轨道交通控制平台链接在一起，为它们提供数据传输的能力。边缘服务器就近为网络中的用户提供服务，但相关状态和运行关键数据还需要通过主干网上传到控制总平台，如运行日志和告警信息。同时控制平台通过主干网由上而下地控制各边缘集群的工作。另外，由于轨道交通列车运行速度快，高峰期列车间隔短，各边缘子系统之间还要进行数据交互，以实现智能化控制列车正常运行。

（3）边缘子系统

边缘子系统包括站点子系统、车辆段子系统和车载子系统。站点子系统和车辆段子系统中部署有边缘服务器和小基站，通过无线阵列与列车通信，与监控摄像头、显示大屏、轨道信号灯以及多种传感器构成相应边缘子系统。车载子系统是由列车上的车辆核心控制设备和边缘接入设备组成，包括控制单元、车载传感器、CBTC 控制器等。车载子系统通过天线阵列与另外两类子系统通信，与边缘服务器交互信息，保障车辆的正常运行。

本节设计的城市轨道交通边缘计算网络简化了传统轨道交通的核心网络结构，形成了云-边缘网络结构。将核心网的存储和计算能力下沉到边缘集群和部分边缘设备，提供灵活低耗的控制、转发能力。然而边缘计算节点暴露在开放式环境中，异构设备的安全防护措施往往各不相同，非常容易遭到集中攻击并被挟持。与传统云计算架构对比，其网络层面临着指数级增长的攻击流量。一旦被入侵，就会造成大量隐私数据泄露、计算能力丧失，这不仅会导致边缘网络大面积瘫痪，被劫持的边缘节点也可以伪装为正常节点，影响边缘网络数据传输和控制单元的决策，对城市轨道交通的运营带来重大安全隐患。因此，必须构建从云核心到边缘节点的一体化内生安全防护体系，增强边缘计算网络抵抗各种安全风险的能力，并使边缘节点之间具备数据可信共享的能力。

4 融合区块链的轨道交通边缘计算网络安全防护机制

4.1 区块链在轨道交通边缘计算网络中的应用优势

在轨道交通边缘计算网络场景中，将区块链应用部署在边缘计算平台上具有多方面的优势。第一，区块链是边缘计算网络构建内生安全体系的重要解决方案。由于轨道交通系统中大量异构设备的生产厂家和批次不同，其安全防护策略和遵循的协议也各有异同，大量更换通信和车辆设备是不现实的，从长远来看即使使用统一的安全策略也有被破解入侵的风险。因此目前轨道交通系统采取的安全防护策略只能为插件化、补丁化的策略，这就造成了不同设备之间信息交互障碍较多且难以实现全局信任。内生安全机制聚焦网络由内而外的稳定运行能力，需要系统灵活且智能地在源头上处理安全问题[4]。在这种情况下，区块链是构建轨道交通边缘计算网络内生安全机制为数不多的选择之一。第二，边缘计算与区块链融合，有利于节约云端资源以及减少网络中的带宽消耗，提高物联设备整体效能[16]；第三，分布式区块链系统靠近边缘设备，将部分账本数据直接存储在边缘上，可以提高认证、可信机制的运行效率，降低传输时延；第四，

由于轨道交通智能化管理需求越来越高，大多数应用服务和数据记录工作都不再依靠人工，因此使用区块链的共识机制、智能合约等能力，可以构建针对轨道交通边缘计算网络中的共享类应用、存证类应用、安全类应用的智能化安全防护机制[17]。

4.2 融合区块链的轨道交通边缘计算网络安全防护机制

由于边缘服务器的物理分布具有分散性，边缘计算网络一般是分布式网络。区块链系统具有独特的去中心化分布式结构，在移动环境中部署区块链，边缘设备收集的关键数据与哈希值一起保存到区块链中，智能合约则可以保障其调用过程的可信性[18]。这种思路也在产业界中得到了应用，去年落地的云原生区块链框架 CITA-Cloud 尝试在联盟链框架中构建数据安全保护机制。考虑到轨道交通系统对运营数据隐私安全、权限分级具有极高的要求，私有链与联盟链结合的安全防护机制更加符合该行业未来发展方向。另外，以轨道交通中的视频数据采集和传输需求为例，区块链能实现更高速率的视频转码及传输工作[19]，也能实现视频证伪等功能。

针对第 3 章中设计的城市轨道交通边缘计算网络的安全需求，考虑在靠近底层的边缘子系统部署私有区块链系统，依靠共识和认证机制保障节点的安全和接入设备的身份，将具备不同功能的区块链子系统部署在边缘节点上，以合理利用边缘服务器资源并提供低时延的服务；在控制总平台部署私有区块链系统，确保线路服务器和核心服务器的数据安全，并通过边缘网关实现一部分计算压力的分流；在外部网系统中部署联盟链，结合身份权限分级以及智能合约实现全域安全可信、跨域数据共享。设计出融合区块链的轨道交通边缘计算网络安全防护机制如图 3 所示。

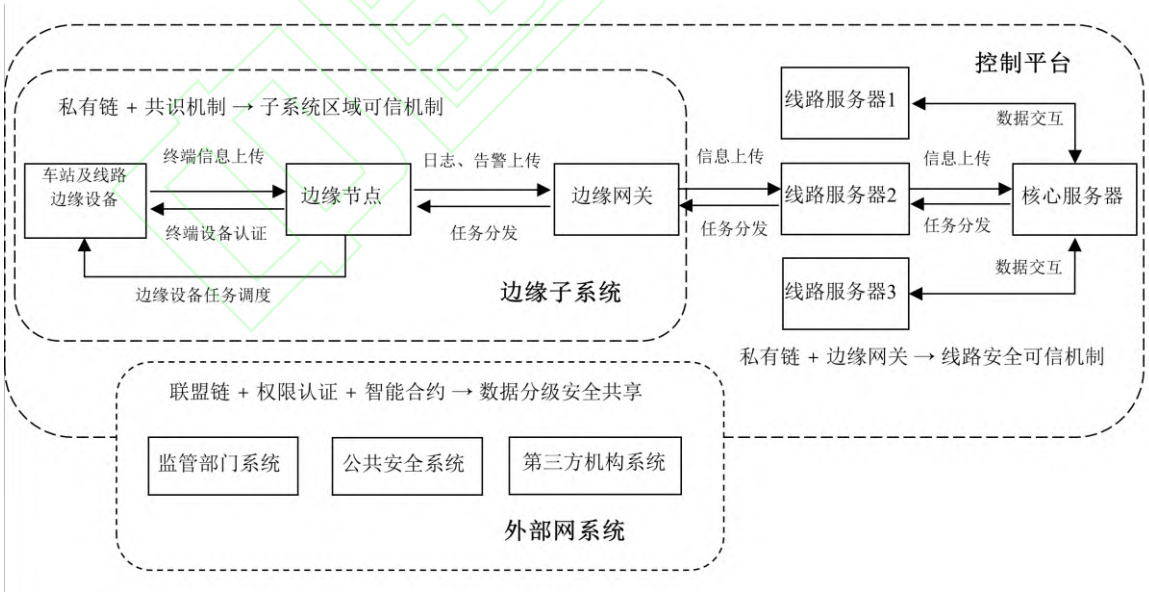

图 3　融合区块链的城市轨道交通边缘计算网络安全防护机制

该安全防护机制的运行流程主要有以下步骤。

（1）将各类边缘子系统中的边缘设备和边缘集群加入私有链中，边缘设备在出厂时可以被写入公私钥和自签名数字证书，区块链将直接验证并记录它们的证书。

（2）借助多因素身份认证技术确保接入边缘计算网络的用户是有权限的，终端设备采集信息和上传

数据上传至站点子系统或车辆段子系统边缘节点，由边缘节点负责将关键数据（日志、告警信息等）上传至私有链，保证设备安全、任务可信执行的同时，也减少边缘计算网络中的冗余流量。

（3）将边缘网关运行在线路私有链中，边缘网关确保子系统与核心服务器之间流量的控制转发，防止异常流量侵入控制平台，确保边缘网络资源调度过程安全及跨域编排任务可信。

（4）轨道交通线路私有链上运行着多种安全管理系统，这些基于区块链的管理系统多数运行在边缘集群中，在 4.3 节中将详细介绍这些系统。相关系统依靠区块链的不可篡改和点对点加密传输，实现控制平台中的线路核心服务器与边缘子系统之间告警信息上传与边缘网络任务分发的可信性。

（5）利用联盟链可以使轨道交通监管部门、公共安全部门以及第三方业务机构按照不同的需求和权限获取准确而安全的跨域数据共享服务，同时智能合约可以灵活地针对轨道交通边缘计算系统进行自动化的安全防护。

该方案利用分布式边缘节点的框架和资源部署区块链存储及共识机制，与第 3 节中设计的轨道交通边缘计算网络原生兼容，实现其内生安全。具体来说有以下几点：该安全方案利用边缘计算网络的特性，在不增加新的层次和框架的基础上，横向负责验证边缘网络内所有异构边缘设备的安全证书，纵向跨越边缘子系统、控制平台、外部网系统验证用户准入权限，破解“外挂式”、“补丁式”安全机制的问题；该方案使用分布式存储，本地数据不再全部上传到控制总平台，同时将摘要信息存储在区块链上，这不仅意味着边缘计算网络的网络带宽压力减小，相关摘要信息也可以被复制分发到全网，对避免产生单点故障具有意义；该方案要求车辆在广播交通信息时实时进行签名和加密，通过检验签名的有效性和公钥加密的机密性实现传输过程中的安全，同时监管边缘网关的控制转发行为，从多个层次实现内生安全；最后，该方案并未否决受信任的中心化部件，考虑到轨道交通应用的特殊性，将运营方、监管方、第三方全部纳入联盟链中根据权限共享可信数据，这种设计思路是为在根本上解决轨道交通数据易篡改、监管难的问题。该技术愿景囊括了轨道交通边缘计算网络各个层级和完整通信流程的安全防护，它应该是开放的，这意味着共识机制、通信协议、控制策略等技术选型必须根据不同需求具体探讨且应该是多样的，该蓝图的具体实现将依赖于未来轨道交通边缘计算网络的发展和演进。

4.3 安全防护机制应用场景

融合区块链的城市轨道交通边缘计算网络安全防护机制主要利用边缘节点的资源部署相关区块链子系统，本节介绍其应用实例以及涉及的相关区块链安全管理子系统。

（1）跨集群边缘业务数据同步

边缘集群收集边缘设备数据并进行本地处理，在轨道交通场景中，车载子系统和其他边缘子系统的信息交互数据量大、移动性高，为了保证轨道通信设备在移动和切换过程中的业务连续性，必须确保边缘节点间、边缘节点与线路服务器之间数据的高可信同步性、一致性。因此，利用区块链分布式账本的特性，在所有边缘服务器和线路服务器上部署区块链数据同步系统，对跨集群交互的数据提供数据授权和追踪、一致性校验等功能，以实现业务数据同步过程中的安全可信性。

（2）视频存证

轨道交通边缘计算系统中有大量的视频存证需求，视频信息存储了轨道交通运行全过程的信息。视频存证中存在着记录方和监督方，记录方为轨道交通公司或相关设备服务商，监督方为上级管理部门和公共安全部门。为了避免存储时间过长的视频被篡改或被恶意删除，在视频采集的设备上部署区块链视频服务应用，定时将视频文件摘要信息发送到边缘集群中的区块链节点，最后将摘要信息存储在整个网络中。当管理人员需要查看视频时，区块链视频服务应用使用视频文件生成新的摘要，如果该摘要与网络上存储的信息符合，则可以完成视频验真。

（3）传感器数据防伪存储

轨道交通中具有大量传感器设备，如车站中的声光传感器、线路上的位移、水平传感器、列车中的红外、烟雾传感器等。这些传感器可以采集大量物联网数据，通常这些数据会先经边缘服务器处理后，再上传到线路服务器或云端平台上，然而传统的传输方式不仅占用大量带宽资源，还难以保障海量异构设备的数据安全。因此，传感器将采集数据分别发送到相关的边缘节点上，再发送到边缘节点上的区块链系统，通过这种方式区块链将物理隔离、协议不同的传感器进行一体化的安全可信管理。

（4）线路设备巡检

在轨道交通设备的日常巡检工作中，面对大量异构的交通设备，巡检耗时长、效率低、容易出现数据记录错误的问题，也无法杜绝第三方设备公司巡检信息造假的情况。因此，在边缘集群部署区块链巡检系统，利用节点的网络及存储资源，一方面对于智能化巡检的数据自动上链，防止篡改；另一方面要求人工巡检数据及时上传并记录巡检人信息，同线路控制中心与轨道交通公司一起构成分布式的安全可信体系，方便公司将总节点运行在云计算平台上，线路和站点节点就近运行在边缘服务器上。

（5）线路设备运维

轨道交通站点、车辆段、列车中的通信设备的日志、告警信息等数据对轨道交通系统的维护和控制十分重要，为了满足考核管理标准，在运维中可能会出现人为的故障瞒报或修改数据的情况，由于轨道交通运维数据量大，数据出现问题后经常出现难以追溯操作的情况，导致控制中心无法实时掌握准确的轨道交通网络运维数据，产生严重的安全隐患。因此将区块链运维系统部署到边缘集群上，通过智能合约将重要数据或其哈希值传输到区块链上存储，并进行可信管理。如对于操作日志，操作人将个人信息、操作的时间、操作地点、操作行为等写入操作日志后上传到区块链运维系统上；对于设备的性能指标和告警信息，应该自动上传，实现相关信息的可信、可追溯。

（6）边缘设备认证

轨道交通公司定制的交通及通信设备出厂前，生产商就将公私钥写入设备，并向区块链系统提交记录申请，因此这些设备将得到系统的安全认证。在设备使用过程中，边缘计算系统随时可以向区块链认证系统请求对设备进行认证，边缘设备也可以通过该方式验证边缘服务的可信性，之后两者建立数据传输通道进行信息交互。

5 问题与挑战

利用区块链构建边缘计算网络安全防护机制为城市轨道交通网络的安全运行提供了具有可行性的方案，但是该机制在进一步的应用和发展中还面临着一些问题和挑战。

5.1 缺乏行业实际部署案例

当前各云计算服务商、通信运营商、设备制造商针对面向以轨道交通网络为例的垂直行业边缘计算系统的设计和部署尚处于技术研究和测试阶段，在一些垂直行业已经开展了分布式边缘计算的探索，然而暂未有大面积成熟运行的系统。区块链与边缘计算融合的轨道交通边缘计算在业内尚无共识的架构，在实现智能化控制和可信安全防护机制的融合方面还需要进一步的研究和设计，目前还不具备在轨道交通领域大面积使用的条件。

5.2 资源开销大

区块链具有分布式账本和共识认证等机制，由于位置越低的边缘节点通常资源量越少，因此在轨道交通网络中的区块链节点所消耗的存储、网络等资源是不可忽视的，区块链技术的应用可能会影响边缘节点的处理实验和处理并发性，因此必须针对轨道交通边缘网络的具体应用情况对区块链系统进行优化。

5.3 安全威胁复杂

本文提出的融合区块链的城市轨道交通边缘计算网络安全防护机制聚焦了轨道交通边缘计算网络的内生安全可信机制，保障接入网络的边缘设备安全可靠，同时使整个网络的边缘设备与上层服务器的信息交互安全、可追溯。然而轨道交通通信网络面临的安全问题是多方面的，如 DDoS 攻击、共识算法攻击、无线通信干扰等[20]，因此如何完善安全可信机制以应对多方面安全威胁是重要的研究方向。

6 结束语

边缘计算对管理轨道交通网络中海量的分布式异构设备具有处理时延低和计算能力强的优势，但其安全性存在着较大隐患，因此利用具有分布式账本等特点的区块链来构建其安全防护机制受到了业界内越来越多的关注。首先对区块链技术进行了介绍，设计了轨道交通边缘计算网络基本架构，并提出了一种融合区块链的城市轨道交通边缘计算网络安全防护机制。详细分析了该安全防护机制整体工作流程及此机制下具体的安全防护应用实例。最后，讨论了融合区块链的城市轨道交通边缘计算网络安全防护机制在实际应用中面临的问题与挑战。探讨了区块链在轨道交通边缘计算网络中的应用，但还存在一些不足之处，如对区块链消耗边缘计算资源过多以及轨道交通运输高峰时期如何使区块链节点之间快速交互信息以防止信任机制瘫痪等问题还未提出高效的解决方案。未来的工作将聚焦该安全防护机制的技术选型、实际应用等重点问题，最终实现该系统的落地运行。

参考文献：

[1] 傅佳伟. 城市轨道交通智能发展方向浅析[J]. 铁道勘测与设计, 2020(2): 82-84.
FU J W. Analysis on the development direction of intelligent urban rail transit[J]. Railway Survey and Design, 2020(2): 82-84.
[2] 祁经, 段罡, 丁国平. 城市轨道交通中 5G 通信技术的运用探讨[J]. 电子世界, 2020(8): 160-161.
QI J, DUAN G, DING G P. Discussion on the application of 5G communication technology in urban rail transit[J]. Electronics World, 2020(8): 160-161.
[3] 谢人超, 廉晓飞, 贾庆民, 等. 移动边缘计算卸载技术综述[J]. 通信学报, 2018, 39(11): 138-155.
XIE R C, LIAN X F, JIA Q M, et al. Survey on computation offloading in mobile edge computing[J]. Journal on Communications, 2018, 39(11): 138-155.
[4] 刘杨, 彭木根. 6G 内生安全：体系结构与关键技术[J]. 电信科学, 2020, 36(1): 11-20.
LIU Y, PENG M G. 6G endogenous security: architecture and key technologies[J]. Telecommunications Science, 2020, 36(1): 11-20.
[5] LI X, LIU S P, WU F, et al. Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications[J]. IEEE Internet of Things Journal, 2019, 6(3): 4755-4763.
[6] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.
[7] CHENG L C, LIU J Q, XU G Q, et al. SCTSC: a semicentralized traffic signal control mode with attribute-based blockchain in IoVs[J]. IEEE Transactions on Computational Social Systems, 2019, 6(6): 1373-1385.
[8] 武继刚, 刘同来, 李境一, 等. 移动边缘计算中的区块链技术研究进展[J]. 计算机工程, 2020, 46(8): 1-13.
WU J G, LIU T L, LI J Y, et al. Research progress on blockchain technology in mobile edge computing[J]. Computer Engineering, 2020, 46(8): 1-13.
[9] MOLLAH M B, ZHAO J, NIYATO D, et al. Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey[J]. IEEE Internet of Things Journal, 2021, 8(6): 4157-4185.
[10] 方俊杰, 雷凯. 面向边缘人工智能计算的区块链技术综述[J]. 应用科学学报, 2020, 38(1): 1-21.
FANG J J, LEI K. Blockchain for edge AI computing: a survey[J]. Journal of Applied Sciences, 2020, 38(1): 1-21.
[11]GAL A. The Tangle: An Illustrated Introduction[EB]. 2018.
[12] 李萌, 裴攀, 孙恩昌, 等. 人工智能与区块链赋能物联网：发展与展望[J]. 北京工业大学学报, 2021, 47(5): 520-529.
LI M, PEI P, SUN E C, et al. Empower artificial intelligence and blockchain to Internet of Things: development and prospect[J]. Journal of Beijing University of Technology, 2021, 47(5): 520-529.
[13] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展[J]. 计算机学报, 2021, 44(1): 55-83.
XU K, LING S T, LI Q, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 55-83.
[14] 郭才, 李续然, 陈炎华, 等. 区块链技术在物联网中的应用概述[J]. 物联网学报, 2021, 5(1): 72-89.
GUO C, LI X R, CHEN Y H, et al. Blockchain technology for Internet of Things: an overview[J]. Chinese Journal on Internet of Things, 2021, 5(1): 72-89.
[15]ETSI M. Mobile edge computing (mec); framework and reference architecture[J]. ETSI, DGS MEC, 2016, 3.
[16] 叶欣宇, 李萌, 赵铖泽, 等. 区块链技术应用于物联网: 发展与展望[J]. 高技术通讯, 2021, 31(1): 48-63.
YE X Y, LI M, ZHAO C Z, et al. Blockchain technology applied to the Internet of Things: development and prospect[J]. Chinese High Technology Letters, 2021, 31(1): 48-63.

[17] 中国移动 5G 联合创新中心.区块链+边缘计算技术白皮书(2020)[EB]. 2020.
China Mobile 5G Innovation Center. Blockchain + edge computing technology white paper (2020)[EB]. 2020.

[18] MA Z F, WANG X C, JAIN D K, et al. A blockchain-based trusted data management scheme in edge computing[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2013-2021.
[19] LIU Y M, YU F R, LI X, et al. Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11): 11169-11185.
[20] 赵军辉, 张丹阳, 贺林. 智慧城轨交通通信技术的分析与展望[J]. 电信科学, 2021, 37(4): 1-13.
ZHAO J H, ZHANG D Y, HE L. Analysis and prospect of communication technology in smart urban rail[J]. Telecommunications Science, 2021, 37(4): 1-13.

[作者简介]


谢高畅（1997- ），男，北京邮电大学网络与交换技术国家重点实验室博士生，主要研究方向为边缘计算、信息中心网络、物联网等。


卢华（1976- ），男，广东省新一代通信与网络创新研究院网络技术创新中心主任，主要研究方向为 5G 核心网、边缘计算、新型网络架构、软件定义网络、P4 可编程、虚拟化等。


唐琴琴（1994- ），女，北京邮电大学网络与交换技术国家重点实验室博士生，主要研究方向为边缘计算、物联网、资源分配等。

 朱涵（1998- ），女，北京邮电大学网络与交换技术国家重点实验室硕士生，主要研究方向为边缘计算、任务调度等。

 梁成昊（1997- ），男，北京邮电大学网络与交换技术国家重点实验室硕士生，主要研究方向为边缘计算等。

 文雯（2001- ），女，北京邮电大学网络与交换技术国家重点实验室硕士生，主要研究方向为边缘计算。

 谢人超（1984- ），男，博士，北京邮电大学教授、博士生导师，主要研究方向为边缘计算等。