

# 面向端边云协同架构的区块链技术综述

佟 兴<sup>1)</sup> 张 召<sup>1),2)</sup> 金澈清<sup>1),3)</sup> 周傲英<sup>1),3)</sup>

<sup>1)</sup>(华东师范大学数据科学与工程学院 上海 200062)

<sup>2)</sup>(桂林电子科技大学广西可信软件重点实验室 广西 桂林 541004)

<sup>3)</sup>(华东师范大学上海市大数据管理系统工程研究中心 上海 200062)

**摘 要** 近年随着边缘计算的兴起,边缘计算和云计算结合形成的终端-边缘-云(端边云)协同的层次型分布式架构尽管可在高计算能力服务、高存储能力服务和低延时服务等方面满足应用需求,但在数据安全和多方可信交互等方面仍面临很多挑战.作为一种去中心化的分布式账本技术,区块链具有数据不可篡改、不可伪造、可追溯和由多方共同维护的特点,将区块链融入到端边云架构中可以使多参与方之间进行互信的数据交互,确保数据完整和可用.但由于区块链在系统架构、隐私安全、对节点资源要求和多方共识方面的特点,其与端边云架构相融合时仍面临诸多挑战:区块链和端边云系统在架构上的不匹配使得二者难以融合;区块链账本数据透明,可能造成敏感数据泄露;区块链的全副本存储和共识过程会消耗更多端边云参与节点的资源;不同端边云场景所需的信任模型差异、终端和边缘节点资源受限和终端设备大规模接入等特点使得现有共识算法不能适应端边云的场景.针对以上问题,本文首先介绍端边云架构和区块链技术,接着讨论二者融合的可行性和优势,并整理归纳了相关研究进展;之后讨论端边云架构下区块链技术面临的技术问题;最后提出未来端边云架构下区块链技术的研究方向.

**关键词** 区块链;端边云架构;端边云协同;边缘计算;分布式计算

**中图法分类号** TP18

**DOI号** 10.11897/SP.J.1016.2021.02345

## Blockchain for End-Edge-Cloud Architecture: A Survey

TONG Xing<sup>1)</sup> ZHANG Zhao<sup>1),2)</sup> JIN Che-Qing<sup>1),3)</sup> ZHOU Ao-Ying<sup>1),3)</sup>

<sup>1)</sup>(School of Data Science and Engineering, East China Normal University, Shanghai 200062)

<sup>2)</sup>(Guangxi Key Laboratory of Trusted Software, Guilin University Of Electronic Technology, Guilin, Guangxi 541004)

<sup>3)</sup>(Shanghai Engineering Research Center of Big Data Management, East China Normal University, Shanghai 200062)

**Abstract** In recent years, with the rise of edge computing, although a hierarchical distributed computing model that integrates edge computing and cloud computing is capable of providing services with high computing capability, high storage capability and low response latency, it is still encountered with challenges like data security and trustworthy interactivity. As a decentralized ledger, blockchain has characteristics like non-tamperability, unforgeability, traceability, global consistency, so that the integration with blockchain can ensure data integrity and the service availability. However, due to the issues like system performance, privacy protection, scalability and requirements for hardware resources, it is challenging to integrate end-edge-cloud architecture with blockchain. First, the existence of significant difference in architecture makes it

收稿日期:2020-09-17;在线发布日期:2021-03-10. 本课题得到国家自然科学基金(61972152,U1911203)、广西可信软件重点实验室研究课题(编号 kx202005)资助. 佟 兴,博士研究生,主要研究方向为区块链. E-mail: xtong@stu.ecnu.edu.cn. 张 召,博士,教授,中国计算机学会(CCF)会员,主要研究领域为区块链、海量数据管理和数据挖掘. 金澈清(通信作者),博士,教授,中国计算机学会(CCF)杰出会员,主要研究领域为区块链、海量数据挖掘. E-mail: cqjin@dase.ecnu.edu.cn. 周傲英,博士,教授,中国计算机学会(CCF)会士,主要研究领域为 Web 数据管理、数据密集型计算、内存集群计算、大数据基准测试和性能优化.

difficult to integrate such techniques. Second, the data transparency may leak the privacy of the end-edge-cloud system. Third, full-replicate storage mechanism and consensus mechanism may consume huge resources of the end-edge-cloud system. Finally, the trustworthy model, limited edge node resources and large-scale nodes of end-edge-cloud architecture make the existing consensus algorithms unsuitable to work. To deal with such issues, we first introduce the end-edge-cloud architecture and blockchain technology. Then, we review the recent progress on the integration of end-edge-cloud system and the blockchain. Subsequently, we discuss some problems faced by the blockchain technology under the end-edge-cloud architecture, and point out the future research direction briefly finally.

**Keywords** blockchain; end-edge-cloud architecture; end-edge-cloud collaboration; edge computing; distributed computing

## 1 引 言

作为一种地理上分布式部署、在靠近数据源头处执行计算任务的计算模型<sup>[1]</sup>,边缘计算可以提升服务的响应速度,降低服务延迟.但由于边缘计算设备的计算和存储能力有限,一些对计算和存储要求较高的任务仍需要发往云端执行.因此相比于边缘计算单独发展,边缘计算的发展方向是和云计算结合形成终端-边缘-云(端边云)的层次型计算架构.相比于单纯的云计算或边缘计算,端边云计算模型有效整合二者优势,一方面可以利用云计算的资源优势来提供充足的计算和存储资源,满足资源密集型任务的需求;另一方面可以利用边缘计算的地理优势来满足延时敏感型任务对低延时的需求.

作为一种终端-边缘-云协同的架构,端边云架构可实现纵横两方面协同.纵向协同指端边云三层之间的协同,通过多层次的计算资源满足不同的任务需求;横向协同指同一层次下多节点之间的协同,通常指边缘层节点之间的协同,横向协同又分为单场景下多节点之间的协同(比如车联网的多个边缘计算节点之间的协同)和跨场景边缘节点之间的协同(比如车联网和交通管制节点之间的协同),后者可以满足更加复杂的应用需求.端边云的计算架构可以将云计算和边缘计算有机融合,但是在实际环境下,端边云架构仍然面临着以下四方面挑战:

(1) 如何保证数据的可信存储.端边云架构中的边缘计算设备一般在地理上分布式部署,数据的收集也是通过处于不同地理位置的节点进行.由于

边缘计算设备的安全防护措施有限,且处于开放环境之中,容易受到安全攻击<sup>[2-4]</sup>,数据的完整性和可用性受到威胁,不能确保数据可信存储;

(2) 如何保证可信计算.在端边云系统中,整个系统往往由多个互不信任组织组成,当系统作为一个整体对外提供服务或各方之间进行协同计算时,需要保证系统和各方之间计算过程透明,而目前端边云系统缺乏透明可信的计算平台,无法确保这一点;

(3) 如何保证数据的可信传递.在边缘场景下,各利益方之间互不信任,缺乏数据共享平台,导致各平台数据孤立;在缺乏激励的情况下,各方之间倾向于不分享数据.因此,目前缺乏一个在端边云环境下为多方建立信任并利用激励机制促进各方进行可信数据传递和共享的平台;

(4) 如何保证系统的可信管理.在边缘场景下包含各种类型的边缘和终端设备,这些设备呈现出一定的动态性,会随时加入和退出网络,另外这些设备可能会由于利益关系做出一些恶意的行为.因此需要通过安全的设备监管平台监控并记录设备的行为,而目前端边云系统缺乏一个可信的系统监管和审计平台.

近年来,随着比特币<sup>[5]</sup>等数字货币的快速发展,区块链作为其底层支撑技术受到了学界和工业界的广泛关注.区块链具有历史数据可追溯、数据不可否认、不可篡改和安全透明的特点,因此区块链可以作为过程监管和事后审计的多方交互平台,可以在网络中为互不信任的多方建立信任,使得多方能够在不可信的网络中进行有效的价值转移和数据交互.

区块链 2.0 系统以太坊中智能合约的应用使得

区块链进一步成为了一种分布式的计算模型,因此可以考虑利用区块链构建安全可信的端边云计算架构。区块链作为一种分布式的计算模型,而端边云架构同样是一种分布式计算模型,这个共通点使二者具有融合的前提。从融合效果来看,将区块链融入到端边云协作架构中,一是可以利用区块链作为一个拜占庭容错的多副本存储机制来保证端边云数据的完整性和可用性,实现数据的可信存储;二是可以基于区块链智能合约为端边云计算架构构建一个可信计算框架,实现可信计算;三是可以利用区块链作为数据共享平台促进端边云架构下参与方之间数据安全共享,实现数据可信传递;四是可以将区块链作为边缘场景下的系统设备监管和审计管理平台,实现端边云系统安全可监管,进而实现端边云系统可信管理。

尽管端边云架构融合区块链可以解决自身在存储、计算、数据传递和系统管理方面的安全性和可信问题,但是由于区块链系统自身的一些特点,使得端边云架构在与区块链进行融合时面临挑战。

从架构层面来讲,区块链本质上是一种“扁平”的单层架构;而端边云系统是由终端-边缘-云结合形成的层次型的分布式架构,从纵向的角度看,端边云架构呈现出一种分层的结构,横向来看,端边云架构中的每一层都是一种“扁平”结构。二者架构上的不完全匹配使得区块链和端边云架构融合时面临挑战。

从数据隐私角度来讲,在端边云架构中,终端和边缘计算设备会收集环境中的各种隐私数据,而区块链作为一种由多方共识形成的分布式账本,每个节点都会保存完整的账本数据,数据透明的特点会使得链上数据暴露在网络中,造成隐私数据的泄露。尽管限制区块链节点的加入可以限制隐私数据的传播范围,但是在端边云环境下,边缘节点的安全防护措施有限,攻击者可以攻击安全能力较差的边缘节点,节点一旦被攻破,区块链中的隐私数据将完全被泄露。

从资源角度来讲,端边云架构分为中心化的云计算层和分布式的边缘计算层,边缘计算层中包括边缘计算设备和众多的终端设备。相比于边缘计算节点,云计算节点的硬件条件比较充足,并且硬件结构较为统一;而边缘计算节点通常依据不同的场景设计,硬件结构多种多样,且硬件资源有限,因此端边云系统内部节点之间表现出了很强的异构性。端

边云节点的存储和计算能力差异较大;云端具有充足的存储和计算资源,而边缘计算节点的存储和计算资源相对有限。在边缘计算节点部署区块链时,区块链全副本存储机制和共识过程会消耗节点大量的存储和计算资源。

在端边云架构下,不同的端边云场景具有不同的信任模型,比如一些边缘场景由多个机构或组织共同参与,部分组织会部署多个节点,同属一个组织的节点互相信任,不同组织则不信任,因而整体呈现出一种“局部可信,全局不可信”的混合信任模型。从共识的角度来看,面向单一信任模型的拜占庭容错协议或非拜占庭容错的协议并不能很好的满足实际的场景需求;另外在边缘环境下,节点的硬件条件较差,计算和存储资源欠缺,需要保证共识过程不会给节点带来大的计算开销,比如 PoW(Proof of Work)<sup>[6]</sup>类的共识算法在边缘场景下并不适用;最后,在不同的场景下,系统具有不同的开放性,在无许可的环境中(Permissionless),在涉及大量节点接入时,需要保证系统不因节点数量增加而导致效率急剧降低,传统的基于投票的 BFT(Byzantine Fault Tolerance)类算法,如 PBFT(Practical Byzantine Fault Tolerance)<sup>[7]</sup>等面临严重的扩展性问题。

总结来说,区块链融入端边云架构时,会面临系统架构、数据隐私安全、参与节点资源和共识等多方面的挑战。本文将分析区块链和端边云协同如何融合、融合后能解决的问题以及在端边云环境下区块链技术面临的一些挑战,并综述目前端边云架构和区块链融合的研究进展。

部分文献综述了区块链和物联网融合<sup>[8]</sup>,区块链和边缘计算融合<sup>[9]</sup>等工作。端边云协同计算架构相比于单纯的云计算或边缘计算能够提供更加多样且高效的计算解决方案,将区块链融入到端边云架构中可以解决端边云架构中的安全性问题,但由于区块链自身特点,将区块链融入到端边云架构中会面临很多挑战。基于此,本文首先介绍边缘计算、端边云协同架构和区块链,之后以端边云架构的安全性问题为切入点,阐述端边云架构融合区块链的必要性,之后从区块链自身特点出发,深入阐述端边云融合区块链时区块链所面临的挑战,并介绍研究这些问题的现有研究工作,最后总结在端边云协同与区块链融合未来的发展方向。

本文第2节介绍边缘计算的由来和端边云协同

架构的意义;第3节从区块链数据结构、共识机制、密码学相关技术和智能合约四部分介绍区块链;第4节介绍端边云架构中存在的问题;第5节介绍如何利用区块链解决端边云架构面临的挑战;第6节讨论区块链和端边云架构融合时区块链面临的挑战;第7节提出了未来端边云架构融合区块链的研究方向;第8节总结全文.

2 边缘计算和端边云架构

2.1 边缘计算

在传统的物联网计算模型中,受限于物联网终端设备有限的存储和计算能力,大多数数据处理过程都是在云端完成的.云端具有较强的计算和存储能力,因此将计算任务放在云端是一种高效的数据处理手段.但是,随着物联网的快速发展,大量物联网设备接入网络会产生海量的数据,尽管云端数据处理能力也在不断增强,但海量数据的传输会给网络造成很大的压力,网络的带宽将成为瓶颈;同时对于一些延迟敏感的应用来说,云计算较高的延迟不能很好的满足应用需求;云计算中心机房会产生大量的能源消耗以及相对应的散热成本.

针对云计算模型的缺点,近年来出现了边缘计算模型,边缘计算本质上是在靠近数据源头的地方执行计算任务,无需再将终端设备产生的数据传送到云计算中心,因此具有如下优点.

- (1)减轻网络的压力.在网络边缘产生的大量数据无需再上传云端,减轻网络带宽的压力;
- (2)降低延时.在靠近数据源头的地方对数据进行处理,不需要请求云数据中心的响应,降低网络延时,提高系统效率;
- (3)降低隐私泄露风险.隐私数据可以在边缘计算层进行一些加密处理甚至保存在边缘计算层,降低数据泄露的风险;
- (4)降低云计算中心的能耗.数据在本地进行处理或预处理,云计算中心不再需要处理海量的数据,降低云计算中心的能耗;
- (5)灵活性更强.可以针对具体的应用场景设计相应的边缘服务,提高计算服务的灵活性.

根据边缘设备和网络类型的不同,边缘网络可以分为 Cloudlet<sup>[10]</sup>、雾计算<sup>[11]</sup>和移动边缘计算

(Mobile Edge Computing, MEC)<sup>[12]</sup>, Cloudlet 是一个部署在网络边缘的计算机或计算机集群,相比于一般的终端设备,Cloudlet 拥有更强的计算和存储能力,对外与互联网连接,对内为边缘设备提供计算服务,形成一个本地局域访问网络;雾计算由性能较弱、分散的功能计算机组成,比如路由器或交换机等<sup>[13]</sup>;移动边缘计算(Mobile Edge Computing, MEC)是在无线接入网内,在接近移动边缘设备的移动网络边缘提供计算服务,移动边缘计算服务器通常与无线网络基站共存,具有超低延迟、高带宽、位置感知等优点.

无论是 Cloudlet、雾计算还是移动边缘计算,彼此之间的区别主要在于边缘计算设备和网络类型的不同,但其核心思想都是将数据在靠近数据源头处进行处理,本质上都属于边缘计算的范畴.

文献[14]设计了针对具有能源收集功能的移动设备(Energy Harvesting, EH)的移动边缘计算系统.通过计算任务卸载结合能源收集来实现绿色的边缘计算模型,作者将执行开销作为性能指标开发了基于 Lyapunov 优化的动态计算卸载(LODCO)算法,动态地将终端设备中的计算任务分配到移动边缘计算服务器中.卸载之前将移动设备执行过程中 CPU 周期频率以及卸载过程中的能源消耗作为参考指标综合考量来做出卸载策略,通过边缘计算为终端设备提供计算服务,降低终端设备的计算压力.文献[15]针对计算任务卸载过程中存在的隐私泄露问题设计了两阶段的卸载优化策略,卸载过程中对卸载的效用和隐私的保护进行综合考量.第一阶段设计了基于 NSGA-III 的任务卸载方法,实现 ECU(Edge Computing Units,边缘计算单元)资源利用率最大化、时间成本最小化;第二阶段作者设计了一种权衡卸载效用和隐私保护的联合优化方法,实现隐私保护和高效执行性能的权衡.文献[16]实现了利用边缘计算降低无人机视频数据分析所需带宽资源的方法.作者结合带宽节省策略将计算任务卸载到边缘节点进行实时无人机视频分析.作者利用深度神经网络从无人机视频流选择性地传输数据,并利用早期丢弃策略结合即时学习、反馈和基于上下文的过滤等策略进一步提高带宽效率.

表 1 总结了不同场景下边缘计算的典型工作.

表 1 各领域中边缘计算相关工作

文献	应用场景	问题	边缘计算的作用
[17]	智慧城市	在智慧城市能源管理系统中,终端设备如何有效分析数据并采取相应能源管理措施.	利用边缘计算实现基于深度强化学习的物联网能源管理,边缘计算节点运行深度增强学习算法提升能源管理性能.
[18]	智慧电网/电动汽车	如何结合大数据分析,推动电动汽车运作的智能化,优化智能交通中电动汽车充电任务.	与电动汽车交互,收集电动汽车数据,分发数据,实现数据挖掘任务的分布式计算.
[19]	智能电网	如何解决基于云计算的智能电网场景在延时和带宽方面存在的弊端.	通过边缘计算进行海量数据的实时分析,提供低延时服务,提出基于任务分级的层次型决策预执行策略作为隐私保护策略.
[20]	智慧城市	如何解决基于云计算的智慧城市延迟较高的问题.	通过边缘计算实现无处不在的访问,提升服务质量,降低服务响应延时.
[21]	智能家居	如何高效管理本地可再生能源与智能家居中的家庭能源.	利用边缘计算实现家居环境中的高效能源管理框架,另外提出统一的能源管理框架降低边缘计算带来的能源开销.
[22]	智能家居	家居环境中会产生大量数据,机器学习模型位于云端,如何解决家居场景中云计算在隐私保护、数据安全和高服务延时方面的问题.	利用边缘计算在靠近数据源头处对数据进行处理,实现分布式的机器学习模型.
[23]	智能汽车	边缘计算服务器有限的计算能力会限制卸载服务的质量,如何在交通流量密集情况下高效处理车辆请求.	提出了一种基于云的分层车辆边缘计算(VEC)卸载框架,采用 Stackelberg 博弈论方法设计多级卸载方案,最大化车辆和边缘计算服务器效用.
[24]	智能医疗	在智能医疗场景,如何针对病人身体情况,及时响应紧急情况并提供个性化的医疗服务.	提出了一种基于边缘计算的智能医疗系统.该系统能够使用认知计算来监视和分析用户的身体健康,并根据用户的健康风险等级调整边缘计算网络的计算资源分配.
[25]	工业物联网	工业场景下,IoT-Cloud 架构在通信、电池资源和计算需求等方面受到限制,如何高效低延时处理海量数据.	在终端层和云计算层加入雾计算层,雾计算层运行 MQ 遥测传输代理(MQ Telemetry Transport)预测未来数据,作为网关层,执行卸载的计算任务降低服务延迟.

总结来说,在网络边缘处部署计算设备(即边缘计算)带来的优势主要分为四方面:一是可以将终端设备的计算任务卸载到边缘计算设备上,将边缘计算作为一种“平台即服务”的服务模式,降低终端设备的计算压力,实现计算任务的合理分配;二是边缘计算设备本身提供计算服务,将边缘计算作为一种类似于“软件即服务”的服务模式,在靠近终端的位置提供计算服务,降低服务延迟;三是利用边缘计算设备对数据进行预处理和过滤,通过边缘设备过滤和预处理数据,减少发送到云端的数据量,增强带宽效率,降低云计算中心能耗,另外在将数据发往云端之前,可以通过边缘计算对数据进行加密,保证云端数据的隐私性;四是将边缘计算设备作为云层的缓存设备,利用数据局部性的特点来缓存云层数据,降低云层数据访问延迟,加快终端读写数据速度,提升响应速度.

2.2 端边云架构

相比于云计算,边缘计算在降低服务延时等方面具有明显的优势,但是像数据分析型或数据统计型这类对计算和存储资源要求较高的任务,仍需要云计算来完成;另外在服务稳定性方面,边缘计算提供的服务稳定性远不及云计算提供的服务稳定性.所以边缘计算的定位是作为传统云计算的补充用来弥补现有云计算的一些缺陷.未来边缘计算的发展导向也将是终端、边缘和云的融合发展,最理想的效果是端边云架构高效融合,同时兼具云计算和边缘计算的优势.

端边云架构可以在纵向和横向进行协同.纵向协同是指端边云不同层次间的协同,旨在充分利用端边云不同层次间设备的特点来满足不同的应用需求,比如边缘设备可以充当云端设备的缓存设备向终端提供低延时服务,终端直接与边缘设备进行连接,满足终端设备低延时的访问需求;边缘层设备可以利用云端设备充足的存储资源来将数据卸载到云端进行存储,也可以将资源密集型任务卸载到云端,通过云端来完成终端设备的复杂计算任务;

横向协同是指在多方之间进行数据交互.为满足多样的应用需求,需要多方之间进行数据共享,在端边云架构下,数据主要在边缘层进行汇集,而边缘设备是地理上分布式部署的,因此需要边缘节点之间进行数据共享,满足多样的应用需求.

横向协同和纵向协同的内容会在第 5 节继续深入展开介绍.

相比于云计算,边缘计算可以大幅度提升服务的响应速度,但边缘计算的计算能力和可承担负载都有限,在网络请求急剧上升时,大量的计算负载会降低服务的响应速度.针对这个问题,文献[26]将服务的架构组织成层次型的结构,整体的思想就是在服务请求数量不多时,通过边缘计算来提升服务的响应速度;当请求达到高峰超出边缘服务的处理能力时,通过云计算的计算资源来提升服务的处理能力.另外,作者结合层次型的计算架构设计了相应的负载分配算法,该算法结合计算需求和通讯延迟两

个角度来对任务进行划分,决定计算任务执行位置.该工作的核心就是充分利用不同层次计算服务的特点来对不同任务负载的情况下最优化系统的运行效率.

在实际场景下,不同的任务有不同的延时需求,因此在边缘场景下,单纯的任务卸载并不能达到系统服务响应的最优化.针对这个问题,文献[27]在边缘云计算中,将一组边缘服务器部署在移动设备附近,以使这些设备可以以低延迟将作业卸载到边缘服务器.相比于文献[26]中的工作,文献[27]中不仅考虑了终端设备的任务卸载问题,同样考虑了任务卸载之后的任务调度问题,以使作业响应时间最小化的同时达到整体最优化.作者为该问题的解决提出了一个通用模型:作业在移动设备上以任意的顺序和时间生成,然后分发到服务器上.因为不同的任务具有不同的延时需求,因此根据每个任务对延迟的敏感程度分配了相应的权重,核心目标就是减少所有工作的总加权响应时间.同时该工作提出了针对任务分发和调度问题的在线可扩展算法 OnDisc.

在现有的针对端边云协同架构的工作中,通常从整体的角度去设计最优化的计算卸载策略,但在实际情况下,每个终端设备总是从自身需求出发采取最优的卸载策略,实现自身体验质量(Quality of Experience, QoE)最大化,而不会根据全局最优的角度去设计计算任务卸载策略.针对这个问题,文献[28]设计了 QoE 最大化框架,与前面提到的工作相同,终端设备根据计算需求和延迟要求设计最优的计算卸载策略;另外作者设计了多终端设备之间的计算卸载博弈策略,通过一种“无政府状态”的计算资源定价策略和多设备之间的计算资源竞争形成一种博弈的状态,作者证明了纳什均衡点的存在,同时为了解决确定均衡点的时间复杂度,作者提出了相应的资源分配算法.

总结来说,端边云计算架构相比于单纯的云计算或边缘计算架构,最大的特点是具有层次性和融合性,层次性在于其可以利用边缘和云端的不同特点的计算设备或计算服务构成多层次的架构,满足多样的终端应用需求;融合性在于其不仅仅是将边缘和云进行简单加和,而是将边缘和云进行高效的协作和融合,这样可以将边缘计算和云计算发挥出各自最大的价值.具体而言,端边云架构一方面是可以提供一套层次型的计算基础设施,终端设备可以利用这套基础设施部署各种类型的计算任务,满足自身计算需求,减轻自身计算负担;另一方面,可以通过端边云的架构提供层次型的计算服务,终端设

备根据自身需求分别请求不同层次下的计算服务,满足自身需求.

端边云架构中融合了不同类型的计算资源来满足不同的任务需求,通过多样化的计算资源来提供多样化的计算服务;但另一方面,多样的计算设备也带来了相应的安全性问题.

### 3 区块链

区块链已经被应用到了资产管理<sup>[29]</sup>、IoT (Internet of Things)<sup>[30]</sup>、医疗管理<sup>[31]</sup>、政务监管<sup>[32]</sup>等多个领域<sup>[33]</sup>.从网络层面来讲,区块链是一个对等网络(Peer to Peer, P2P),网络中的节点地位对等,每个节点都保存完整账本数据,系统的运行不依赖中心化节点,因此避免了中心化带来的单点故障问题.同时区块链作为一个拜占庭容错<sup>[34]</sup>的分布式系统,在存在少量恶意节点情况下可以作为一个整体对外提供稳定的服务.

区块链按照开放程度可分为公有链、联盟链和私有链:公有链是一种完全开放的区块链网络,任意节点都可以加入,但公有链交易速度慢,吞吐较低,典型的包括比特币和以太坊;联盟链面向部分特定的组织开放,只有这些组织才拥有对区块链数据的读写权限,相比于公有链,联盟链吞吐率较高,典型系统为 Hyperledger Fabric;私有链只对单个组织开放,系统效率和隐私性更高.

以下从区块链关键数据结构、共识机制、密码学相关技术和智能合约四个方面介绍区块链.

#### 3.1 区块链关键数据结构

区块链是一种按照时间顺序将数据区块通过哈希指针链接的链式数据结构,并借用密码学技术确保区块链数据难以篡改和伪造.区块链中的每个区块分为区块头和区块体两部分,区块头中主要包含前一个区块的哈希值、时间戳、随机数 Nonce、默克尔根等.在比特币中,矿工通过暴力的方式寻找合适的 Nonce 来破解满足工作量证明的哈希难题;默克尔根是默克尔哈希树的根节点,默克尔哈希树<sup>[35]</sup>是一种二叉树,叶子结点为区块体中交易的哈希值,中间节点是将其子结点的哈希值拼接之后进行哈希计算生成的哈希值.当修改默克尔哈希树中任意一个结点的数据时,会从下向上影响到根结点的值.默克尔哈希树的根结点作为区块内所有交易的摘要.当对一笔交易进行验证时,可以从该笔交易对应的叶子结点出发,直到根结点路径上所有结点的兄弟结点作为验证的证据,待验证交易可以与这个证据生成根

结点哈希值,若生成的哈希值和区块头中的哈希值相同,则交易得到正确性的验证. 这个验证过程称为 SPV(Simplified Payment Verification)验证,如图 1 所示,Hash1 和 Hash(3|4)是交易 2 的证据.

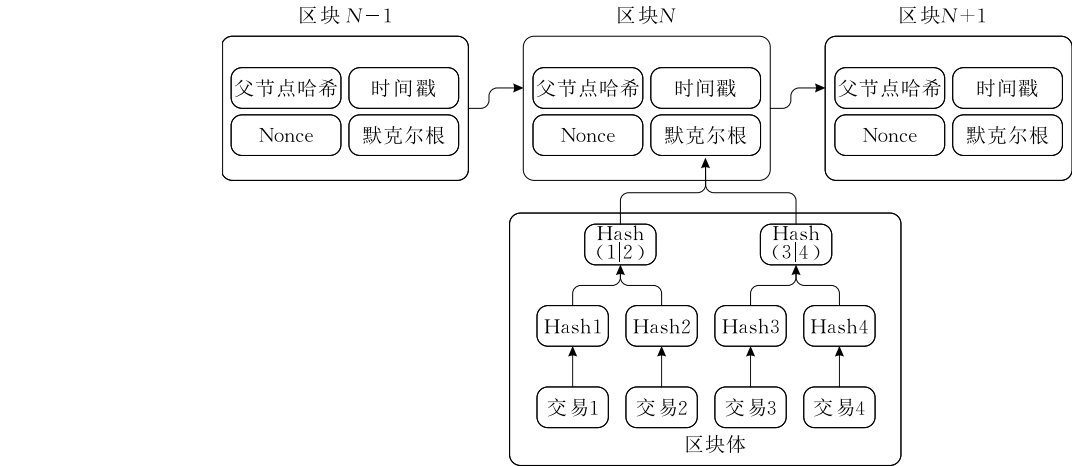


图 1 区块链链式数据结构

### 3.2 共识机制

区块链与传统的分布式多副本系统的不同之处在于前者是一个完全对等的(去中心化)网络,不存在中心化的可信节点,并且可以在存在少量恶意节点的情况下正常运行. 因此分布式系统中广泛使用的 Paxos<sup>[36]</sup> 及其变体<sup>[37-38]</sup>、Raft<sup>[39]</sup> 等共识算法不能应用在区块链系统中.

目前的区块链共识算法可以分为两类,一类是基于竞争的共识算法,主要应用在公有链中;另一类是基于投票的共识算法,主要应用在联盟链中. 基于竞争的共识算法的代表是 PoW,另外有 Proof-of-Capacity<sup>[40]</sup>、Proof-of-Elapsed-Time<sup>①</sup>、DPoS (Delegated Proof of Stake)<sup>②</sup>等;基于投票的共识算法典型的是 PBFT,这类算法在节点数量较多的情况下,系统的效率会相应降低. 目前有相关工作<sup>[41-45]</sup> 将区块链网络进行分片,每个分片独立运行,从而提高系统吞吐量. 也有部分工作利用侧链<sup>③④</sup>和链下交易<sup>⑤⑥</sup>来提高区块链系统的吞吐量.

### 3.3 密码学相关技术

区块链可以在网络中为互不信任的多方构建信任,其中密码学是其最重要的部件之一. 从区块链数据安全存储到多方之间安全交互,从区块链数据安全访问到区块链数据正确性验证,密码学都扮演着重要的角色. 区块链中应用的密码学工具主要包括哈希算法、加解密算法、签名算法等.

(1) 哈希算法,也称为散列算法. 主要的功能是将原始数据通过哈希函数编码,将其映射成固定长度的字符串,该字符串作为原始数据的哈希值(摘要). 哈希算法具有单向性,不能从哈希值反推得到

原始数据;另外哈希算法具有雪崩效应,原文细微的变化会导致哈希算法算出的哈希值有极大的不同.

(2) 加解密算法. 加解密算法是密码学的核心,算法本身公开且固定,密钥则需要特殊保护. 一般来说,同一种算法,密钥越长,安全性越高. 目前的加解密算法主要分为对称加密和非对称加密,对称加密中加密的密钥和解密的密钥相同,对称加密加密效率高;非对称加密中密钥分为公钥和私钥,私钥由用户自己保密持有,公钥公开,非对称加密效率相比于对称加密效率较低.

(3) 数字签名. 数字签名是基于非对称加密算法实现的消息加密与验证算法. 数字签名可以实现消息的认证,保证数据的完整性和不可否认. 数字签名不涉及加密,不能保证数据不被网络中的攻击者嗅探而泄露隐私. 数字签名过程中,持有私钥的用户对消息进行签名,签名之后,拥有对应公钥的用户可以根据公钥验证签名消息的合法性.

### 3.4 智能合约

智能合约的历史可追溯到 20 世纪 90 年代, Nick Szabo<sup>[46]</sup> 第一次提出了“智能合约”的概念,其

① <https://intelledger.github.io/introduction.html>  
② Delegated proof of stake. <http://docs.bitshares.org/bits-hares/dpo8.html>  
③ Enabling blockchain innovations with pegged sidechains. <http://www.opensciencereview.com/papers/123/enabling-blockchain-innovations-with-pegged-sidechains>  
④ Sidechains, Drivechains, and RSK 2-Way Peg Design. <http://www.rootstock.io/blog/sidechains-drivechains-and-rsk-2-way-peg-design>  
⑤ The bitcoin lightning network: Scalable off-chain instant payments. <http://lightning.network/lightning-network-paper.pdf>  
⑥ Raiden network. <https://raiden.network/>

设想为在一个计算机系统中,当一些事务被执行时,可以激发合约代码自动执行,并产生对应的输出.智能合约在区块链中的应用也使得区块链从一种分布式存储架构进化成了通用的分布式计算架构,大大丰富了区块链的应用场景.

从编程语言表达能力来看,可以将智能合约分为脚本型、图灵完备型、可验证合约型三种类型,其运行环境可以分为嵌入式运行、基于虚拟机运行和基于容器运行<sup>[47]</sup>.比特币支持简单的嵌入式运行的智能合约脚本,实现基于数字签名的电子货币交易;以太坊支持图灵完备的智能合约,合约代码运行在以太坊虚拟机中,以太坊虚拟机是一个独立运行的沙盒,保证了执行合约代码时不受外界影响,目前以太坊的智能合约一般由 Solidity、Serpent 编写;Fabric 同样支持图灵完备的智能合约,Fabric 中的智能合约称为链码,链码运行在 Docker 容器中,目前主要由 Go 语言编写.

总结来说,区块链是一种由网络中互不信任的多节点组成的分布式计算框架,具有数据不可篡改、数据不可否认、历史数据可追溯、数据安全透明、由多方共同维护等特点.利用这些特点,一是可以将区块链作为一种安全的数据管理系统,保证数据的完整性和可用性;二是可以将区块链作为一个安全的可信计算平台,利用区块链智能合约实现一个可信计算平台;三是可以将区块链可以作为一个通证流转平台,可通过代币实现激励机制,促进各方的数据共享,构造一个良好运作的多方协同框架;四是可以将区块链作为一个监管审计平台实现系统的安全透明监管.

4 端边云架构面临的问题

端边云架构作为一种层次型的分布式计算架构,可以利用其层次型和地理上分布式的特点提供多样的计算服务.但另一方面,在复杂的端边云系统中,数据会在不同层次和不同设备之间进行流转,这个过程中数据的完整性和可用性不能得到保障;端边云架构中包含各种类型的计算设备,这些设备彼此之间呈现出很强的异构性,一些安全防护能力较弱的节点容易受到安全攻击,同样,数据的安全性无法得到保证;开放型的端边云网络可能会接入恶意的终端设备或计算设备,这些设备会破坏系统的正常运行,系统的稳定性无法得到保障;端边云架构作

为一种地理上分布式的架构,数据会分布在不同的节点上,在不可信的环境下,数据的安全共享受到挑战.

具体来说,端边云架构面临的问题主要包含以下四点:

(1) 不能保证数据的可信存储

端边云架构边缘计算层是一种分布式的结构,其中终端设备或边缘服务器产生的数据会保存在边缘层中的多个边缘节点上,这些设备的安全防护能力有限,同时在复杂的边缘环境下会存在各种的攻击行为<sup>[3,48]</sup>,因此边缘层和终端层的设备容易被攻击者攻破;另一方面,相比于云端设备,边缘层和终端层中的设备稳定性较差,边缘节点容易因硬件条件或外界因素影响而宕机,这些情况都会导致存储在边缘层和终端层的数据丢失或被篡改,导致系统服务的可用性降低.在云层中,数据的安全性由云服务提供商进行背书,云服务的可靠性和性能就成为重要因素.总的来说,在端边云架构下,云层、边缘层和终端层的数据的完整性和可用性受到多方面的挑战.

(2) 缺乏可信计算框架

从纵向来看,端边云架构是一种由终端-边缘-云构成的层次型架构,不同的层次下的设备具有不同的特点:边缘端具有明显的位置优势,云端具备很强的弹性计算优势等,这些优势使得端边云架构可以基于不同层次的设备对外提供多样的服务;从横向来看,端边云系统由众多不同场景的设施组成,可以在多场景协同的情况下对外提供丰富且高效的计算服务.然而,不同场景的设施往往分属于不同的利益体,并且各利益体之间互不信任,彼此之间并不能进行高效的协同.在可信中心化节点存在的情况下,基于中心化协调节点的系统可以充分发挥端边云架构的优势,但是在中心化协调节点不存在的情况下,如何将端边云架构中的硬件和架构进行充分的利用,即基于端边云架构构造一个可信的计算框架并对外提供可信可靠且安全的服务具有重要意义.

(3) 不能保证数据的可信传递

在边缘环境下,相比于中心化的云计算模型,边缘服务由众多的边缘节点提供,数据分布在众多的边缘设备上,由此会形成一个信息孤岛.通过安全的访问控制机制可以在保证数据隐私和安全的情况下提供数据的访问策略.但如果要满足更加多样的应用需求,需要多方之间主动共享数据,这需要建



立一个安全可信的数据共享平台,来保证共享数据的安全性和可靠性.另外一方面,边缘环境中的边缘节点可能属于不同的利益相关方,部分节点倾向于拒绝分享数据,而这会导致共享系统的活性大大降低.针对这一点,需要建立正向的激励机制,鼓励边缘节点之间数据共享,形成一个高效可信的数据共享平台.

(4) 缺乏系统可信管理机制

端边云架构系统相对来说是一种开放式的系统,会有各种类型的设备接入系统,尤其是在边缘环境中,各种异构终端设备会连接到边缘服务器上,这些设备的接入给系统带来了不确定性和安全隐患.因此边缘环境下终端设备的管理,比如物联网设备的动态接入与离开、行为记录以及相应的边缘设备身份管理等都需要一个安全的管理和审计手段.在传统的管理系统下,可采用中心化的管理架构来实现边缘环境下的设备管理和系统审计,但中心化的架构存在中心化节点故障和节点作恶的可能性,系统的安全性不能得到保证.另外,分布式的边缘环境

通常会涉及到多方的利益,比如在物联网中,边缘终端设备、边缘计算设备或一些其他的基础设施通常分属于多个不同的利益相关方,多方之间进行协同同时缺乏安全可信的监管和审计机制.

5 端边云架构融合区块链

端边云系统和区块链融合后整体的架构图如图 2 所示:从端边云系统纵向角度来看,整体的架构分为三层:自顶向下依次为云层、边缘层和终端层.云层具有充足的存储和计算资源,负责数据的全量存储,另外采用基于区块链的多副本存储机制保证拜占庭容错下的数据一致性;边缘层负责处理终端采集的数据,由于边缘层设备能力有限,因此仅缓存部分云端数据用来提供低延时的访问服务,同时采用基于区块链的多副本机制保证拜占庭容错下边缘缓存数据多副本之间数据一致性;终端层负责收集环境中的数据并向边缘层请求计算服务.

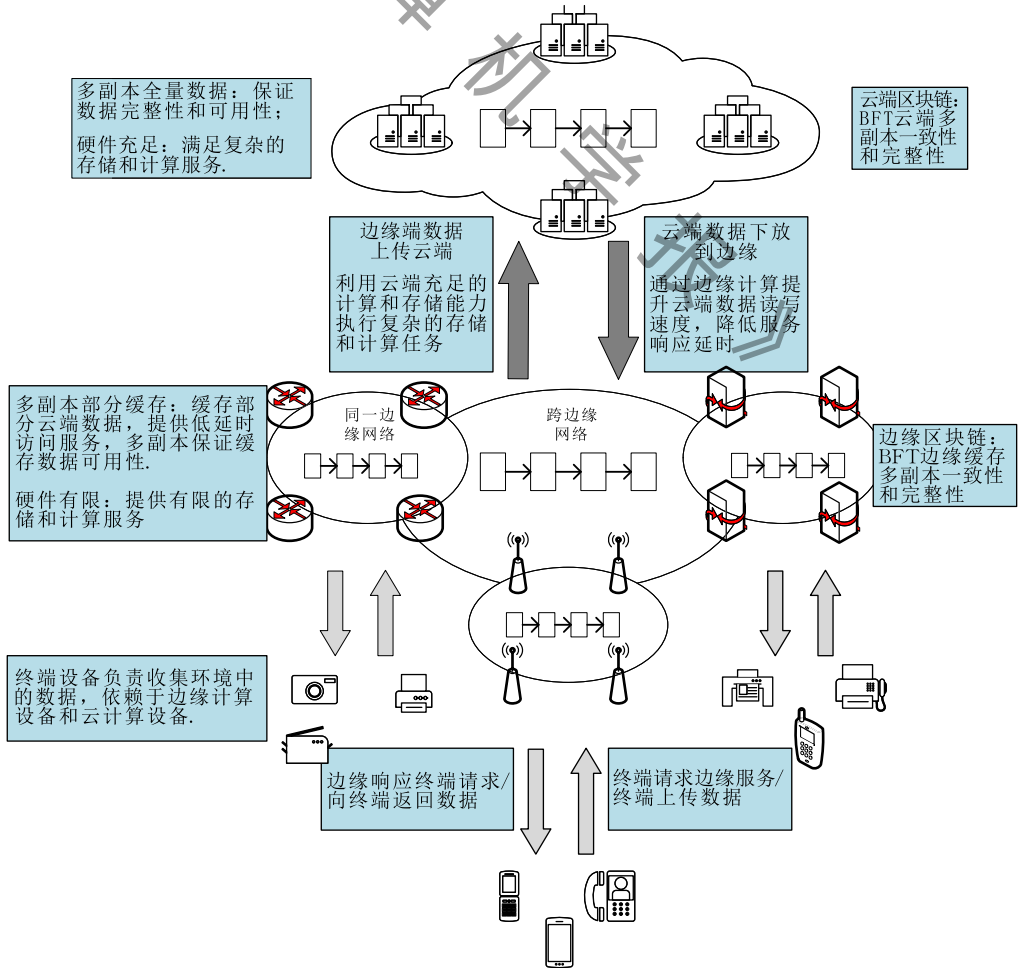


图 2 端边云系统融合区块链架构

从端边云系统横向角度来看,边缘层可以和其他边缘网络节点进行跨边缘网络协作.以道路上的边缘网络为例,车联网中的路边计算单元形成车联网的边缘计算网络;交通管制部门的路边单元形成交通管制的边缘计算网络;环境监测部门部署在环境中的环境监测设备形成环境监测的边缘计算网络.不同边缘网络由于业务场景的特殊性,只会访问和自身业务相关的数据,因此不同的边缘网络会缓存不同的云端数据,访问数据呈现局部性的特点.但当涉及到跨场景数据读写或共享时,需要保证数据读写时边缘缓存多副本之间数据的一致性和数据共享之后的可审计性.

端边云横向协同是指边缘环境下单个场景多节点之间的协同,或者是多个边缘场景下多个节点之间的协同.以文献[49]为例,作者为支持高效的拼车服务,设计了一种车联网拼车系统,其中路边计算单元负责收集道路上车辆和拼车用户信息用以提供拼车服务,多个路边计算单元进行横向协同共享数据,从而提升拼车服务质量.

从端边云系统纵向角度来看,协同过程中会涉及到层次之间数据卸载和计算卸载,数据卸载主要是将不同层次的数据迁移到其他层次,以满足多样的需求.比如边缘节点直接向终端设备提供服务,而边缘节点要访问的数据往往来自于云节点,这个过程中就涉及到将云端数据卸载到边缘侧,这时边缘节点就类似于云端设备的缓存<sup>[50]</sup>.纵向协同其中的关键点在于:(1)通过云层满足终端设备请求的边缘层不能提供的大量存储和计算需求;(2)通过边缘层满足终端设备请求的云层不能提供的低延时的计算服务.以文献[51]为例,作者为满足资源密集型和延迟敏感型任务的需求,设计了一种 IoT-Fog (Edge)-Cloud 端边云融合框架,系统整体的架构分为终端-边缘-云三层,边缘为终端提供低延时服务,云为终端提供大量计算服务,二者纵向的协同融合为终端提供多样的计算需求.

节点间进行横向和纵向协同时,系统会面临诸多挑战:纵向协同过程中,通常会涉及到数据外包存储和卸载的场景,这个过程中数据的完整性和可用性不能得到保证;多方协作过程中,计算过程的透明性和安全性不能保证;横向协同过程中,会涉及到多方之间进行数据共享,但目前缺乏安全的多方交互平台,以及促进多方数据共享的激励机制;另外端边云系统的开放程度较高,节点的移动性较强,节点会不断的进入和退出系统,节点行为不能得到有效监

管和安全审查.

当前针对区块链和端边云架构融合的研究工作大致上可分为如下四类.

(1) 利用区块链实现端边云系统数据可信存储

从微观的数据结构角度来看,区块链是一种链式的数据结构,每个新产生的区块中都会包含前一个区块的摘要(哈希值),当恶意篡改某个历史区块时,会导致区块链链条的“断链”,区块链便会变得无效;从宏观的系统组成来看,区块链是一种全量数据的多副本存储系统,每个节点都会保存完整的区块链数据,节点之间通过拜占庭共识机制保证数据一致性.区块链微观上的链式数据结构和宏观上的全副本分布式存储机制保证了区块链数据的完整性和可用性,因此现有工作主要利用区块链的这些特点保证端边云系统运行过程中数据的完整性和可用性.

文献[52]提出了基于区块链的端边云环境数据完整性验证框架.随着物联网的快速发展,资源受限的终端设备产生的数据需要转发到边缘计算设备或云计算设备,因为数据和数据所有者的分离导致存储在云端和边缘端的数据并不完全安全,针对这个问题,传统的解决方案是通过一个可信的中心化第三方审计者(Third-Party Auditor, TPA)保证数据的完整性,但这种方式存在中心化故障和 TPA 作恶的可能性.针对这个问题,作者利用区块链作为一个可信的验证服务提供方来保证数据的完整性.具体而言,系统整体的物理框架分为三层,终端层,边缘层和云层,终端设备产生的数据会根据数据的特点来决定保存在云层或边缘层(Edge-Cloud Storage, ECS),区块链部署在计算和存储资源较为充足的边缘节点或云端节点.终端设备在将数据转发到云端或边缘端进行数据存储时,会将数据进行划分并利用默克尔树生成摘要(默克尔根),之后将其上链存储.在进行数据验证时,ECS 提供相应的验证信息,通过智能合约结合链上存储的摘要信息提供可信的验证服务.另外,作者提出了取样的验证策略,降低验证过程中的资源消耗和延时.文献[51]设计了一种轻量级的计算框架 FogBus,作者利用雾和云基础设施的不同特点构建应用执行平台来满足不同应用需求.具体而言,作者将资源受限的 IoT 系统结合雾和云端的计算资源构建一个通用的计算平台,充分利用雾计算延时低、云计算计算能力强的特点,根据应用不同的需求提供相应的计算服务.其中的代理节点负责运行区块链实例,通过区块链保证数据完整性,同时利用区块链可追溯的特点追溯历

史数据流监控 FogBus 网络。

(2) 利用区块链智能合约实现端边云可信计算框架

文献[53]将区块链引入到针对端边云系统中,用以解决物联网服务的安全性问题。作者将区块链部署在云端,利用区块链智能合约维护边缘服务提供商的有效性信息;另外通过区块链的激励机制提升边缘服务的积极性和可靠度。系统整体的架构包含云服务器、边缘服务器、轻量级客户端(LWC),云服务器基于智能合约向边缘服务器提供可信服务代码,边缘服务器向 LWC 提供服务。整体上来说,该项工作利用区块链智能合约为端边云系统构建一个可信的计算框架,保证边缘服务器提供的服务的有效性和安全性。文献[54]提出了一种基于区块链的边缘计算分布式控制系统。由终端设备、边缘计算节点和云计算三层形成一个端边云的架构。云端的节点部署为 Hyperledger Fabric 验证节点,在边缘节点上部署 Docker 容器提供边缘计算服务,Kubernetes 用于协调跨边缘资源执行容器。作者通过智能合约来保证边缘执行交易的正确性和安全性。其中,边缘的物理设备和资源(例如控制器、传感器、执行器等)被模拟为执行动作逻辑的元素,众多设备被建模成多个功能组件,从而构建一个大型分布式系统。为了降低管理设备的复杂性,作者对设备和资源进行了抽象化的表达,每个抽象的单元可能包含零个或多个封装独立功能或任务的资源。云端的节点作为整个系统的控制层,功能块以区块链中智能合约的方式实现,保证了控制层的安全性和稳定性。

(3) 利用区块链实现端边云数据可信传递

在文献[55]中,作者提出通过区块链实现联邦计算中模型参数的共享。在端边云架构中,边缘网络包含大量的边缘计算节点,这些节点会收集终端设备采集的环境数据,因此数据会分散在各边缘计算节点上。一些数据挖掘和机器学习算法等任务依赖于各边缘节点收集的数据,当数据分布在各个边缘计算节点上时,各节点独立训练数据模型,再运行融合算法形成全局模型,作者提出通过区块链实现节点之间模型参数的共享,保证模型参数的安全,避免中心化服务器带来的安全问题。同时利用区块链数据可追溯的特点保证联邦计算流程的可审计性。文献[56]提出了一种面向车联网的端边云数据共享架构,利用区块链实现道路上车辆数据安全共享和数据安全存储。整体上为三层的架构:车辆构成系统的

终端层,路边计算单元作为边缘层,云端服务器作为云层。区块链部署在路边计算单元上。通过智能合约实现车辆之间安全高效的数据共享。

(4) 利用区块链实现端边云系统可信管理

端边云系统作为一种开放的系统,在终端层,任意节点均可以接入系统,未知节点的接入对系统的安全性提出了挑战。因此,需要在边缘网络中对边缘设备的行为进行监控和记录,进而保证系统的安全性。

文献[57]提出了一个边缘网络可信编排管理(Trusted Orchestration Management, TOM)架构。端边云系统由终端设备(传感器等),边缘计算设备和云端计算设备组成。其中在边缘环境下包含各种类型的设备,因此边缘网络一般呈现出动态的特点;并且边缘网络经常出现跨组织的情况,即设备可能属于不同的利益相关方,因此存在一定的安全和信任问题,一些设备可能表现出恶意行为。因此边缘环境下所有活动,比如物联网设备的动态变化、边缘计算资源的管理和边缘数据的管理,都需要安全的管理机制。针对这个问题,该文基于区块链实现边缘环境下的安全数据管理,通过区块链管理边缘环境中所有实体的身份信息,记录终端设备数据和网络中终端设备的动态变化情况以及某些具体处理行为的执行情况。从而构建一个安全可靠的边缘网络。

总结来说,区块链作为一种通过密码学和多方共识机制保证数据和系统安全的分布式模型,可以将区块链融入到端边云架构中解决端边云架构的安全性问题。一是利用区块链作为一个安全的分布式存储系统,保证端边云架构下数据的完整性和可用性;二是可以利用区块链作为数据共享平台保证端边云架构下多节点之间数据的安全共享;三是利用区块链智能合约作为端边云系统构造安全的可信计算框架;四是利用区块链作为边缘场景下的监管平台,实现端边云系统整体运行流程可审计,保证系统安全。

以车联网为例描述端边云架构和区块链融合系统的特征。系统整体的架构分为三层:云层、边缘层和终端设备(包括车辆以及其他道路上的终端设备);系统中涉及到的边缘网络包含:车联网中的路边计算单元形成一个车联网的边缘计算网络;交通管制部门的路边单元形成一个交通管制的边缘计算网络;环境监测部门部署在环境中的环境监测设备形成环境监测的边缘计算网络。云层保存三个边缘网络场景完整的数据(包括最新状态数据和历史状

态数据),基于区块链实现拜占庭容错的多副本存储,保证数据的完整性和可用性;为满足延迟敏感型终端设备低延时的访问需求,云层的数据根据不同的应用场景缓存到不同的边缘网络中;为保证每个边缘网络中数据的完整性和可用性,基于区块链实现缓存数据的多副本存储,保证缓存数据的完整性和可用性;当道路上发生突发情况时,一方面需要各方之间快速响应,另一方面会涉及到环境监测边缘节点、交通管制边缘节点和车联网路边边缘节点进行跨场景数据访问,为保证数据访问过程中数据的一致性和访问过后的可审计性,通过区块链来使互不信任的多方对数据的访问过程达成一致,并记录数据共享过程,从而保证跨节点数据访问过程中的一致性以及数据共享之后的可审计性;数据共享过程中,可以通过智能合约实现安全计算,比如车辆运行状态判断等;另外利用区块链记录终端设备的行为记录,对设备的行为进行留痕记录,便于后续设备行为审计,保证端边云系统的安全性.

尽管端边云架构融合区块链能够满足多样的应用需求,然而在架构、隐私保护、节点资源条件和共识等方面面临挑战.

6 端边云架构下区块链面临的挑战

和传统的云计算模型相比,端边云模型在终端层和云服务层之间加入了边缘计算服务层,通过边缘计算服务处理终端产生的数据可以在降低服务响应延迟,减少网络传输负载和隐私保护等方面提供支持. 区块链作为一个去中心化的 P2P 系统,本质上是一种扁平化的系统结构,而端边云则是一种层次型的架构,因此二者在架构上的不统一使得区块链系统和端边云架构融合时面临诸多困难;另外在边缘场景下,边缘节点的安全防护能力有限,容易被网络攻击,区块链作为一种通过签名防篡改,数据以明文方式上链的存储机制,每个节点都可以获取链上数据,节点一旦被攻破,会造成端边云环境中隐私数据的泄露;在端边云计算模型中,原始数据主要由边缘服务层收集,因此区块链一般部署在边缘层,但是边缘层的硬件资源条件相比于云层而言,资源有限并且资源供给受限,部署区块链会给边缘节点带来比较大的存储和计算压力;最后,在边缘场景下,会有大量资源受限的边缘设备接入区块链网络,这些边缘设备由于自身资源受限,无法存储全量数据和参与共识,另外边缘环境下节点之间复杂的信任

关系(属于同一组织的节点互相信任,不同组织的节点互不信任)会导致边缘场景下的安全假设模型变得比较复杂,现有的依赖于单一安全假设模型的共识算法无法适配端边云架构下的区块链系统. 以上这些问题都对端边云架构下的区块链系统提出了新的挑战. 下面我们将详细介绍这些挑战并归纳总结应对这些挑战的可能的解决方案.

6.1 架构融合方面

区块链系统中每个节点地位对等,本质上是一种扁平的 P2P 网络. 相比于区块链系统架构,端边云架构则是一种分层的分布式系统,整体上呈现出层次型结构化的系统模型. 另外在端边云架构中,不同层次间的节点呈现出很强的异构性. 在这种情况下,对区块链在端边云环境下的部署提出了挑战,即如何将非层次型的区块链网络和层次型的端边云系统结合. 目前针对架构方面的融合方案,主要分为三类:第一种是直接将区块链系统部署在云层网络中;第二种是直接在边缘网络中部署区块链系统;第三种是结合端边云系统不同层次设备的特点来部署多重区块链系统或对区块链系统进行层次化设计.

第一种策略是将区块链系统和云端网络(或边缘网络上一层网络)进行结合,充分利用云端网络的硬件优势<sup>[54,58]</sup>. 文献[58]以智慧城市为研究场景,研究如何保证数据的完整性和可用性. 作者提出了一种融合区块链的软件定义网络(Software Defined Network, SDN)智慧城市混合网络架构,整体的架构分为核心网络和边缘网络两个部分,其中边缘网络节点存储和计算能力有限,负责收集和过滤数据;核心网络由具有较高计算和存储资源的节点组成,负责保存和维护数据. 为保证数据的完整性和可用性,作者将区块链融入到核心网络中,由核心网络中的节点充当区块链节点;而边缘节点受限于自身的存储和计算资源,仅充当各个边缘区域的中央服务器,负责汇集、过滤数据,并将数据发往核心网络,同时在靠近服务请求者的位置提供低延时服务,节省核心网络带宽资源.

第二种策略是将区块链系统部署在边缘网络中,在数据产生源头处将数据上链,更能保证数据的完整性和可用性<sup>[49,56,59]</sup>. 其中文献[49]为解决拼车场景下数据云端存储带来的数据被篡改或数据丢失的问题,作者基于端边云架构和区块链系统设计了一种拼车系统. 系统整体的架构包含终端、边缘和云端三层,终端包含拼车用户和车辆信息,边缘设备是路边计算单元,负责车辆和拼车用户匹配,云层负责

存储加密之后的拼车等历史数据. 区块链系统部署在路边计算单元组成的边缘网络中, 通过网络中的区块链系统保证数据的完整性和可用性. 避免数据被篡改的情况, 提高系统的可审计性.

第三种策略是结合端边云系统不同层次设备的特点来部署多重区块链系统或进行层次型设计. 物联网中包含大量的终端设备, 这些设备会收集环境数据, 但物联网设备的安全防护能力有限, 因此数据的完整性和隐私性不能得到保障, 文献[60-61]以智能家居为场景研究如何解决物联网数据完整性和隐私性问题, 设计了一种基于区块链的智能家居环境中的端边云协同架构, 该架构包含智能家居层、覆盖网络层和云层. 其中智能家居层为部署在家庭中的边缘计算设备, 并且该边缘计算设备会部署为一个私有链节点, 负责处理家居环境中产生的各类数据并维护家居环境中的访问控制策略, 保证家居环境中数据的完整性和隐私性; 覆盖网络层是由多个家庭中的边缘计算设备组成的 P2P 网络, 覆盖网络层中的节点分成多个集群, 每个集群中的主节点(Cluster Header, CH)部署为一个公有链节点, 通过公有链实现多方之间的数据共享以及访问控制信息的传递; 云端负责数据的后端存储. 该系统整体的架构是一个多重链的系统. 端边云系统和区块链系统架构融合三种方式比较如表 2 所示.

表 2 端边云系统和区块链系统架构融合方式比较			
架构结合方式	云端部署	边缘部署	多重链和链层次化设计
优点	可以充分利用云端网络的硬件优势, 减轻边缘网络的存储、计算和网络开销	可以充分利用边缘网络的位置优势, 系统响应延时较低	可以结合不同层次的特点进行设计, 从而满足不同应用需求
缺点	系统响应延时较高, 吞吐较低, 不能在数据源头处保证数据的完整性和可用性	存储、计算和网络开销较大, 影响非区块链任务的运行	链间交互和层次化链会增加系统复杂性, 增大开发难度

总结来说, 将区块链部署在云端时, 可以利用云端的存储和计算资源, 但在终端-边缘-云端结合的情况下, 数据主要在边缘端收集、端边云架构和区块链融合的优势并不能充分的体现; 而将区块链部署边缘端时, 区块链会给边缘节点带来比较大的存储和计算开销, 另外数据的隐私安全并不能得到保障; 多重链和层次化链的方式一定程度上可以充分和端边云系统结合, 但是这种方式会使得系统复杂度增高. 具体采用何种方式需要结合不同场景的特点进行具体的设计.

## 6.2 隐私保护方面

在端边云架构下, 边缘环境中节点的硬件基础条件相比于专用服务器安全防护能力有限, 容易受到网络安全攻击, 另外边缘网络中的节点硬件差异较大, 攻击者可以选择性攻击防护能力差的节点, 实现入侵区块链网络的目的; 而区块链全副本存储的特点, 会使得一个节点被攻破, 系统中的全部数据都将被泄露. 即使区块链具有很好的身份匿名性, 避免了攻击者直接通过区块链地址获得隐私数据, 但是交易数据的明文存储使攻击者可以通过交易轨迹分析推测出区块链地址和实际用户身份之间的对应关系, 造成隐私数据的泄漏. 限制区块链节点接入的方式可以保证数据在有限的范围内流转, 但是在存在恶意攻击的情况下, 数据的安全性和隐私性并不能得到保障. 在传统的中心化的网络安全防护中, 可以通过部署高性能的服务器, 部署专属的安全防护硬件和软件保证系统安全性和数据隐私性, 但这种方式主要是通过增强单个服务器的防护能力保证系统的安全性<sup>[62]</sup>, 而端边云架构是分布式架构, 不能直接将该防护措施移植到端边云架构中. 目前在端边云环境下针对区块链数据隐私保护的典型方案包括三类: 数据隔离、数据加密和匿名.

(1) 数据隔离. 数据隔离本质上就是限制节点直接接触数据. 最直接的做法是将涉及隐私的原始数据链下存储, 比如家居环境数据, 个人医疗数据等隐私数据保存在链下, 链上只存储可公开访问的数据, 比如原始数据的哈希摘要, 脱敏之后的元数据等. 这类研究工作的主要思路就是将区块链作为一个访问控制层, 通过区块链实现分布式的访问控制服务器, 避免中心化架构带来的服务宕机和中心化节点作恶的情况<sup>[63-65]</sup>, 其中文献[63]在区块链中设计了两种交易类型: 用于访问控制管理的 T<sub>access</sub> 交易和用于数据存储的 T<sub>data</sub> 交易. 用户首次注册时, 生成一个身份以及关联的用户名并发往链上; 终端收集的数据使用加密密钥进行加密, 通过 T<sub>data</sub> 交易发布到区块链中, 并将其指向区块链外的存储, 在区块链账本上仅保留一个指向数据的指针(该指针可以是数据的哈希值). 服务请求者和数据的所有者都可以使用带有关联的指针的 T<sub>data</sub> 交易查询数据. 数据的所有者通过 T<sub>access</sub> 进行授权. 通过区块链验证数字签名属于服务请求者还是数据的所有者, 对于服务请求者, 还将检查其访问数据的权限. 数据所有者可以通过发出 T<sub>access</sub> 交易更改服务请求者的访问权限. 该工作中, T<sub>data</sub> 交易作为原始数据的元数据链上存储, 原始数据链下存储, 通

过原始数据隔离保证数据的隐私性。

(2) 数据加密. 第二种保护链上数据隐私安全的方式是采用非对称加密或对称加密的方式对链上数据加密, 通过限制解密密钥的分发范围来限制其他节点直接从链上读取原始数据,[66-68]采用加密方式保护隐私数据安全, 文献[66]提出了一种在物联网生态下通过属性加密的隐私保护区块链框架. 参与方主要包括三部分: 集群领导者、区块链矿工和属性授权机构. 其中集群领导者负责收集物联网数据, 将数据加密之后构造成交易发到区块链网络中进行共识; 区块链矿工负责交易验证、全局共识和维护区块链账本数据; 属性授权机构负责为不同属性的矿工或用户验证和发布凭证, 矿工和用户可以通过凭证访问链上隐私数据, 为避免属性授权机构单点故障问题, 采用分布式的属性授权机构实现分布式的凭证分发. 整体的流程为: 集群领导者获取数据之后, 按照访问规则依据属性对数据进行加密, 之后将数据组织成交易的形式发往网络中进行共识, 拥有对该交易访问权限的矿工节点会验证交易的合法性, 合法则将交易打包上链, 之后拥有对数据访问权限的矿工和用户可以通过分发的凭证访问数据. 另外, 为保证系统的安全性, 只有当拥有对某属性具有访问权限的矿工节点数量达到一定阈值时, 属性授权机构才会对相应的属性授权, 否则不予授权.

链上数据加密的方式一定程度上能够保证链上数据的隐私安全, 但是采用简单的加密方式仍存在隐私泄露的风险, 若采用复杂的加密策略可能会给边缘节点或终端设备带来比较大的计算开销, 本策略需要在计算开销和隐私安全二者之间做权衡<sup>[69]</sup>.

(3) 匿名. 第三种方式是通过对链上关键可识别信息的匿名化处理保证隐私数据安全. 文献[70]为解决病历信息传递过程中导致的隐私泄露的问题, 提出了一种基于区块链的保证隐私安全的个人健康信息共享策略, 作者构建了私有链和联盟链两种区块链, 其中私有链负责存储健康信息, 由单一组织进行管理; 联盟链负责维护健康信息的索引记录, 用以定位健康信息. 为了保证隐私数据安全, 健康信息等隐私数据和相应的关键字均被加密, 访问隐私数据需要获得访问权限, 另外作者设计了相应的协议使得医生可以通过访问匿名化处理的数据来获得自己感兴趣的患者信息, 保证隐私数据安全. 文献[71]针对医疗数据链上传递带来的隐私泄露问题进行了研究, 作者使用非对称加密结合双线性配对并基于匿名 ID 的加密来实现分布式密钥管理、身份认证和隐私保护. 另外作者设计了相应策略防止用户之间在通信过程中导致的位置隐私泄露. 端边云环境下区块链常用数据隐私保护方式对比如表 3 所示.

表 3 端边云环境下区块链常用数据隐私保护方式对比

隐私保护方式	原理	隐私性	特点	性能	端边云环境下可行性
数据隔离	隐私数据链下存储, 脱敏元数据链上存储	隐私防护能力较强	实现简单, 但可能导致链下数据不可用	好	不需要额外的安全防护措施, 可行性强
数据加密	对隐私数据加密保证隐私性	隐私性依赖加密函数的安全性	需要设计安全的密钥分发机制	一般	对计算要求高, 需要权衡数据隐私性和共享性
匿名	对链上隐私数据中关键身份信息进行匿名	依赖于匿名策略的设计以及抗链接攻击等安全攻击的能力	匿名策略设计复杂, 需要考虑攻击方式和已公开数据的特征等	较好	对硬件条件要求低, 能较好的应用到端边云环境下, 但匿名策略的设计是难点

数据隔离虽然一定程度上解决了隐私安全的问题, 但是因此也限制了端边云数据的应用价值, 不利于各方之间进行数据共享; 数据加密的方式相比于数据隔离, 数据的安全性主要取决于密码学的安全性, 其主要的問題在于如何安全高效地进行密钥分发来保证多方之间进行高效的协同; 基于匿名的隐私保护方法相比于数据隔离和数据加密, 这种方式的安全性主要依赖于匿名策略的设计, 匿名策略制定过程中, 需要充分考虑可能存在的攻击方式和现有已经公布的数据的特征.

另外基于同态加密和零知识证明的区块链数据隐私保护手段具有很好的研究前景, 可以满足更加

丰富的应用场景需求, 但是在目前阶段下, 同态加密和零知识证明仍处于发展的初级阶段, 应用场景较为有限, 不能支持复杂的验证操作. 同时同态加密和零知识证明是资源密集型的隐私保护机制, 在边缘环境下并不能很好地直接应用<sup>[72]</sup>. 部分工作<sup>[73]</sup>利用 CPU 内的可信硬件构造可信执行环境 (Trusted Execution Environment, TEE), 通过可信硬件保证其内部代码和数据的隐私性和完整性; 也有部分工作利用差分隐私<sup>[74]</sup>来保护链上数据隐私安全, 利用差分扰动策略来避免链上关键隐私数据的泄露.

6.3 边缘参与方资源受限方面

在端边云架构下, 当区块链部署到边缘节点上



时,区块链全副本存储和共识过程等会给节点带来很大的存储和计算开销。

文献[75]提出了一种元数据链上存储,原始数据链下存储的方案。具体而言,作者将原始数据通过一些字段对原始数据的特征进行描述,形成元数据,其中包含数据类型、时间、原始数据存储节点、签名等信息。在原始数据产生过程中生成对应的元数据,并将元数据形成交易广播到网络中,之后区块链节点打包交易形成区块上链存储。数据上链之后,网络中的其他节点通过链上的元数据获得原始数据的特征,并根据链上提供的原始数据存储信息访问原始数据。尽管链上只存储原始数据的元数据,但是在边缘场景下,存储完整的区块链账本仍会给边缘设备带来比较大的存储压力。针对这个问题,作者提出了将账本数据分布式存储的方法,为保证数据的可用性,作者将每个区块都保存多个备份。另外边缘网络中设备之间的存储能力不同,作者设计了相应的区块和分配策略来实现数据划分操作,保证存储方案的合理性。

另外一种减轻边缘节点存储开销的方式是对区块链账本数据进行修剪,但在对账本数据进行修剪时,需要结合区块链账本特点和上层应用的特点设计相应的修剪策略。以基于 UTXO(Unspent Transaction Output)模型的区块链账本为例,账本中每笔交易都引用一个或多个先前的交易作为该笔交易的输入。在输入字段中,交易引用属于一个或多个先前交易的输出列表,并指示它们所属的交易中的输出。在区块链中,全节点需要多个过程来验证交易是否有效。其中最基本的思路是检查用于产生新交易的输入。由于 UTXO 模型中每笔交易不能引用超过一次,因此对于正在验证的交易中的每个输入,全节点将检查引用的其他交易的输出是否存在,不存在或无效的话交易将被拒绝。基于此,文献[76]提出所有输出全部被后一个交易引用的交易是无效的,将无效区块(即仅包含无效交易的区块)发送到云服务提供商中进行备份。然后,这些块将从边缘设备中删除。通过这种方式来降低全节点数据存储量。在这个过程中,一个核心问题是交易的确认策略,只有当交易被明确地确认不会被“推翻”之后才需要考虑是否修剪,否则整体的效率将大大降低。在对区块进行卸载存储时,需要结合区块链的确认策略和应用的特点进行修剪才能真正实现高效的存储优化。

无论是元数据链上存储,原始数据链下存储的方案还是账本修剪的方案,一定程度上解决了区块

链节点的存储压力,但因此也带来了数据存在丢失的可能性,链下数据和被修剪数据的可用性不能得到保证。另外这两种方式会造成数据访问延迟高的问题。

在存储方面,目前也有利用纠删码<sup>[77]</sup>和共识单元<sup>[78]</sup>来解决区块链数据存储的问题。

在计算方面,在边缘网络中,由于边缘设备计算能力有限,本身一些计算需求高的任务就给自身带来了比较大的计算压力,融合区块链之后,区块链运行过程中的签名验证,交易验证或工作量证明等任务进一步加剧了边缘计算节点的计算压力。目前区块链的计算任务主要集中在共识过程中,包含工作量证明等计算过程(主要针对 PoW 类共识算法),另外还有共识过程中交易的验证过程,包括验证签名等。为避免区块链计算任务给边缘计算节点带来比较大的计算压力,可以考虑将区块链的计算任务卸载到其他计算资源充足的节点上,比如云端服务器。

在计算卸载过程中,需要设计一个计算卸载策略,具体涉及何时卸载,卸载给谁,如何卸载几个问题。针对这些问题,需要考虑终端设备自身的计算能力、终端自身的电池能源、未来可能获得的电源、服务器的计算能力、服务器当前的负载、网络带宽、计算卸载时的计算卸载量等因素,并综合考虑这些因素作出合适的计算卸载策略<sup>[79]</sup>。

针对计算卸载的方式,文献[80]提出了一种支持移动边缘计算的区块链框架,移动终端设备通过该框架将复杂的计算任务卸载到边缘节点。考虑到若众多终端设备将计算任务卸载到边缘节点,会导致移动边缘计算服务提供商的过载,因此作者设计了两种卸载模式:一是将计算任务卸载到附近的移动边缘计算服务器,这种方式下用户将全部的计算工作转发到移动边缘计算服务器执行;另一种方式是用户将计算工作进行划分,划分之后通过相应的计算卸载策略将任务转发给附近的其他用户执行。在计算任务卸载过程中,作者将计算任务卸载策略制定为优化问题,其中考虑了延时、任务划分及分配时的能源消耗和挖矿成功概率等因素,并将原始的非凸问题转化为凸问题,提出了一种基于乘数交替方向(ADMM)的算法,以分布式的方式解决计算卸载问题。文献[81]将计算服务提供商和矿工之间的交互建模为 Stackelberg 博弈。计算服务提供商首先设置计算的服务价格,矿工在了解计算服务提供商设定的价格之后,决定自己的计算服务需求。使用反向归纳,作者将领导者和跟随者的优化问题表述为两个子博弈:矿工挖矿策略子博弈;每个矿工针对计

算服务价格,决定最佳的卸载策略;计算服务提供商定价策略子博弈:计算服务提供商获得的利润为矿工支付的计算服务费用减去提供计算时产生的成本,计算服务提供商追求利润最大化.子博弈的两个阶段共同构成了 Stackelberg 博弈.博弈的目的是找到 Stackelberg 平衡,确保计算服务提供商选择的服务价格来使其利润最大化,同时能够及时满足矿工的需求.

针对边缘场景下计算资源受限的问题,目前的工作主要分为两类,一类是降低区块链共识过程给节点带来的计算压力,另一类是卸载节点的计算任务,实现计算任务的合理划分,降低边缘节点的计算压力,这也是区块链和端边云架构融合而非区块链单纯和边缘计算进行融合的重要原因.

端边云场景下区块链计算和存储优化方式如表 4 所示.

表 4 端边云场景下区块链计算和存储优化方式

优化方法		原理	可扩展性	特点	端边云环境下的特点
存储优化	降低账本大小	链上存储元数据,链下存储原始数据	账本容量仍会不断膨胀,本质上并未改善存储的可扩展性	链下数据可能会丢失,无法保证链下数据的可用性,数据访问延迟较高	边缘节点的稳定性较差,链下数据可能会永久丢失
	账本修剪	将部分区块数据卸载到其他节点	一定程度改善账本存储的可扩展性	数据访问延迟高,无法保证数据可用性	需要结合端边云场景特点设计相应的账本修剪规则
计算优化	降低计算量	降低区块链系统运行所需计算量	计算量不能无限降低,不具有扩展性	计算量的降低使得系统容易受到安全攻击,会降低区块链系统的安全性	计算量不能无限降低,仍会给边缘节点带来较大的计算压力
	计算卸载	将区块链计算任务卸载到其他节点	具有一定的扩展性	安全性依赖于计算服务提供者的可靠性	可以与端边云的架构优势充分结合,实现计算任务的合理划分,降低边缘节点的计算压力

6.4 共识方面

在传统的区块链部署环境不同,在端边云架构下,信任模型、区块链节点接入规模和硬件资源条件都不同,因此在端边云架构下的区块链共识算法面临新的挑战.

(1) 混合信任模型

在端边云架构中,尤其在边缘侧,不同的节点往往分属于不同的组织,同一组织下的节点之间互相信任;而属于不同组织的节点之间互不信任,所以在边缘侧,整体呈现出一种“局部信任,全局不信任”的混合信任模型.传统的非拜占庭算法在整体不信任的情况下不能直接应用在边缘侧区块链中,而传统的拜占庭算法则不能充分利用局部信任的特点.

目前基于混合信任模型的分布式复制协议研究工作对于混合信任模型下的端边云区块链具有一定的参考价值:文献[82]提出了一种基于私有云和公有云的分布式复制协议,其中私有云是用户自建的云计算设施,是可以被信任的,而公有云则不被信任,传统的拜占庭容错算法和非拜占庭容错算法都不能很好地适应这种情况,针对这个问题,作者提出了一种基于私有云和公有云混合的状态机复制协议 SeeMoRe,SeeMoRe 以 PBFT 算法为基础,设计了针对私有云不同负载下的三种模式:Lion、Dog 和 Peacock.在私有云负载较轻的情况下,系统采用 Lion 模式,私有云节点作为主节点发起请求,公有云节点收到请求后,对请求进行投票并将结果返回给

私有云主节点,私有云主节点收到投票消息之后根据情况决定是否提交该请求,整个过程由于主节点是可信的,因此不需要额外的多轮投票过程,因此具有较好的性能;当私有云节点负载稍重的情况下,系统采用 Dog 模式,仍由私有云主节点发起请求,但公有云节点对消息进行投票之后并不直接将投票消息返回给私有云主节点,而是公有云节点进行协商(公有云中 2/3 以上的节点为善意节点),并将最终协商的结果发还给私有云主节点,性能相比于 Lion 模式稍差,但相比于 PBFT 性能仍具有明显的优势;当私有云节点负载很重的时候,采用 Peacock 模式,主节点由公有云节点担任,此时整体的流程与 PBFT 类似,性能也与 PBFT 相近.

(2) 边缘和终端节点资源受限

由于边缘节点资源受限,传统的共识算法都不能适用到端边云环境中,在公有链中,节点数量较多,节点可能会随时加入和退出网络,基于投票类的共识算法,如 PBFT 等并不适用,往往是基于计算类的共识算法,如 PoW 等,具有很好的性能和安全性.但是 PoW 类算法计算过程中会浪费大量计算资源.在边缘节点资源受限的情况下,PoW 类共识算法并不适用.目前有很多工作针对这个问题对 PoW 进行了重新设计,其中最常见的就是权益证明(Proof of Stake,PoS)算法.在 PoS 中,拥有更高货币占有率(股权)的节点有更高的概率获得记账权,



不再完全依靠算力获得记账权,减少了对算力的需求.文献[76]中提出的 PoC(Proof of Credit)共识算法是针对边缘场景区块链的共识算法. PoC 算法中,不同节点之间通过一种称为“协作信用(Collaborative Credit,CC)”的代币进行交互.和 PoW 相比, PoC 在计算哈希难题时,加入了 CC 和持久性  $P$  值(持久性  $P$  值定义为节点账户自上次 CC 余额更改以来的时间)的因素,以此来降低工作量证明难度;另外作者限制了挖矿节点持久性  $P$  值的范围:只有挖矿节点账户的持久性  $P$  值在限制的范围之内时,才拥有挖矿的竞争权.这些规则保证了 PoC 算法在单个设备和全网付出的算力两个维度相比于 PoW 付出的算力更少.根据持久性  $P$  值的定义规则:完成挖矿的节点账户得到奖励之后 CC 会变化,持久性  $P$  值就会被清零,而挖矿的节点的持久性  $P$  值需要满足一个范围,所以降低了一个账户节点连续挖矿的概率.但是这种放松计算难度和获得竞争权的方式,降低了网络的安全性,另外节点可以通过更换挖矿账户规避持久性  $P$  值的限制,存在一定女巫攻击风险<sup>[83]</sup>.

Po-X 算法相比于 PoW,对获得记账权的竞争过程进行了改进. Po-X 算法不再依靠解决哈希难题获得记账权或者通过融入其他的一些参数降低哈希难题的难度,减少资源消耗.但是减少资源消耗的同时,一定程度上放松了节点获得记账权的难度,从概率角度来讲,网络被恶意节点控制的概率增加,这就需要通过其他的机制保证系统的安全性.以上面提到的 PoS 为例, PoS 放松了对于算力的要求,将基于算力的证明转化为基于股权的证明,即使有节点在网络中的股权超过了 50%,这些节点也更希望系统的正常运行,而不会去故意破坏系统. PoS 依靠代价和获利博弈的方式来保证系统的安全性.

(3) 大规模接入(Permissionless)

与传统的公有链和联盟链不同,在端边云环境下,系统的主体主要集中在边缘层,这时可能需要边缘节点甚至终端节点加入到区块链网络,并参与系

统的共识过程.当大量的边缘设备节点加入到区块链网络时,终端设备的大规模接入会给区块链共识带来挑战,挑战主要在于如何在保证不会给边缘节点带来很大计算开销的情况下同时支持大规模数量节点共识.

在大量区块链节点存在的情况下,如何选择区块提议者和验证者是共识面临的很大的问题, Algorand 的出现为这个问题的解决提供了解决方案, Algorand 在运行过程中,每一轮都需要在前一个区块的哈希值上通过可验证随机函数(VRF)随机选取区块提议者和验证者,选取过程由节点自身独立完成,从而避免了被攻击的可能性. Algorand 运行过程中不需要协商过程,提议者和验证者只需要单个消息传递就可以证实身份的合法性,因此在大量区块链节点存在的情况下, Algorand 仍具有较好的系统吞吐量.在端边云架构下,边缘节点可能是一些手持终端设备或其他轻型设备, Algorand 运行过程中,每轮都需要节点检查自身是否被选中为区块提议者或验证者,频繁的验证会给设备带来比较大的资源消耗,针对这个问题,文献[84]将在前  $N-1$  区块的基础上计算 VRF 修改为在前  $N-10$  区块的哈希值来进行,避免了每次都需要唤醒设备,从而降低了设备的资源消耗,同时这种方式相比于原来的 Algorand 安全性不会降低.另外,近些年出现了基于 DAG 的新型账本结构, DAG 的结构相比于区块链的链式结构伸缩性较强,可以将交易的同步执行优化为异步执行,该结构支持节点的大规模接入的同时可大幅度的提升网络的吞吐.目前基于 DAG 账本结构的共识算法包括 IOTA<sup>[85]</sup> 的 Tangle,但该算法目前实际运行过程中需要一个中心化的协调节点<sup>[86]</sup>.另外基于 DAG 账本结构的共识算法还包括拜占庭容错的基于状态机复制的异步分布式共识算法 Hashgraph<sup>[87]</sup>.端边云系统融合区块链在共识方面面临的挑战如表 5 所示.

表 5 端边云融合区块链在共识方面面临的挑战

挑战	特点	对共识算法的需求	现有工作分析	面临的挑战
混合信任模型	系统整体上呈现出局部信任,全局不信任的信任模型	适配混合信任模型,保证系统安全性的情况下,充分利用局部信任的特点提升系统性能.	目前在端边云架构下针对混合信任模型的区块链共识算法较为欠缺.	如何充分利用端边云架构下的混合信任模型设计高效且安全的共识机制.
参与节点资源受限	参与节点有限的硬件资源限制共识效率	适配节点资源受限的特点,降低共识过程对节点带来的计算开销.	现有的共识算法降低了共识算法过程中的资源消耗量,但是也一定程度上降低了共识算法的安全性.	如何在保证共识算法安全的前提下降低共识算法带来的计算开销.
参与节点大规模接入	扩展性较差的共识算法限制参与节点大规模接入	适配区块链节点的大规模接入,避免因区块链节点大规模接入导致系统效率降低.	Algorand 类基于 VRF 的算法可以解决大量节点的共识的问题,现有算法不能很好的解决边缘节点动态性较强的问题.	考虑边缘节点动态性强、节点数量大的特点设计高效安全的共识算法.

端边云架构的复杂性也导致了目前已有共识算法并不能直接应用在端边云场景下,目前仍欠缺充分考虑端边云特点(混合信任模型、节点资源受限、大规模接入等)的研究工作。

## 7 端边云融合区块链的研究方向

区块链具有数据不可篡改,历史数据可追溯和由多方共同维护的特点,端边云架构可以融合区块链来保证数据的完整性;另一方面,可以将区块链作为一个激励平台,促进多方的数据共享;区块链作为一个分布式的可信计算平台,可以基于区块链智能合约作为端边云架构构造一个可信计算框架;另外,区块链数据安全透明和可追溯的特点,可以利用区块链实现端边云架构的安全监管和审计。

端边云服务架构可以提供低延时、高计算能力的服务,而区块链的融入可以解决端边云架构中安全、可信和监管的问题。但是二者的融合仍存在诸多问题。文章的最后,我们提出一些未来值得去研究的一些问题,希望能够启发相关的研究者。

(1)端边云协同模式下区块链系统架构设计。区块链作为一种去中心化的架构,整体呈现出一种“扁平化”的结构,而端边云架构作为一种层次型的分布式结构,在与区块链进行融合时会面临架构上不匹配的问题。边缘层作为端边云架构中较为核心的一层,数据周转和计算任务主要是在边缘层完成,若单纯将区块链和云层融合,则不能充分体现出边缘计算的优势;但若将区块链和边缘层融合,区块链全副本存储和共识过程会给边缘层节点带来比较大的存储和计算开销。因此端边云系统和区块链融合时需要考虑二者在系统架构上的不同,并结合场景需求设计相应的融合架构。

(2)端边云场景下区块链的隐私保护策略设计。在端边云系统中,终端收集的数据往往涉及到环境中的隐私数据,并且边缘节点有限的安全防护措施使得节点容易被攻击者攻破。在和区块链进行融合时,区块链传统的隐私保护策略并不能很好地保证数据的隐私性。现有的基于数据隔离和链上数据加密的方式虽然可以保护数据的隐私性,但一定程度上限制了数据共享;另外基于可信硬件的数据隐私保护机制依赖于硬件设计。综上所述,目前在端边云架构下,区块链的隐私保护策略并不完善,仍待进一步研究。

(3)边缘节点资源受限下的存储和计算模式设

计。在一些数据量较大的场景,区块链会给边缘计算设备带来比较大的存储压力,这时可以考虑将数据卸载到其他位置,但这需要设计相应的存储卸载方案,高效合理的存储卸载策略对于卸载过程的高效运行具有重要的意义。在计算方面,在一些计算需求较大的场景下,受限于边缘设备有限的计算能力,运行区块链任务会给边缘设备带来额外的计算开销,会降低端边云协同的效率。为降低边缘设备的计算压力,可考虑将一些计算任务卸载到网络中其他位置,与存储卸载相同,计算卸载同样需要设计卸载策略,高效的计算卸载策略会显著降低对区块链全节点计算能力的需求。综上所述,在边缘节点资源受限的情况下,如何充分利用端边云的架构优势,解决边缘节点资源受限的缺点,是端边云架构和区块链融合的关键点。

(4)混合信任模型下的共识算法设计。区块链可以为网络中互不信任的多方构建一套安全的信任机制,使得互不信任的多方可以在网络中进行有效的价值转移和数据交互。但端边云环境中,不同参与方之间存在不同的信任假设,单纯拜占庭或非拜占庭容错协议不能高效支持参与方之间共识过程。因此需要设计一套面向混合信任模型的共识机制,来适应端边云环境的需求。另外,边缘节点资源受限和节点大规模接入的情况也对区块链共识算法提出较高的要求:一方面,区块链共识过程不能给边缘节点带来比较大的计算压力,另一方面,区块链共识过程不能因为节点数量的增加而导致系统的效率显著降低。

## 8 总 结

本文针对端边云协同架构下区块链系统现状进行了综述。文章首先介绍了端边云协同架构和区块链。之后围绕区块链数据不可篡改、不可否认、多方安全交互等特点,讨论区块链如何解决端边云协同架构在数据可信存储、可信计算、数据可信传递和系统可信管理等方面面临的问题。由于区块链和端边云系统各自特点,使得二者融合时面临多方面的挑战,之后,我们围绕系统架构、隐私保护、资源消耗和共识机制四个方面对二者融合面临的挑战综述了现有的一些研究工作,并进行了总结、对比和分析。最后我们列举了针对未来边缘区块链的发展需要解决的一些问题和研究方向。

致 谢 感谢华东师范大学数据科学与工程学院区块链实验室各位同学的支持!

## 参 考 文 献

- [1] Shi W, Cao J, Zhang Q, et al. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 2016, 3(5): 637-646
- [2] Yu W, Liang F, He X, et al. A survey on the edge computing for the Internet of Things. *IEEE Access*, 2018, 6: 6900-6919
- [3] Mukherjee M, Matam R, Shu L, et al. Security and privacy in fog computing: Challenges. *IEEE Access*, 2017, 5: 19293-19304
- [4] Zhang J, Chen B, Zhao Y, Cheng X, et al. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access*, 2018, 6: 18209-18237
- [5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008
- [6] Jakobsson M, Juels A. Proofs of work and bread pudding protocols//Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks: Communications and Multimedia Security (CMS). Deventer, Netherlands, 1999: 258-272
- [7] Castro M, Liskov B. Practical byzantine fault tolerance//Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI). Berkeley, USA, 1999: 173-186
- [8] Dai H, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, 2019, 6(5): 8076-8094
- [9] Yang R, Yu F R, Si P, et al. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, 2019, 21(2): 1508-1532
- [10] Satyanarayanan M, Bahl P, Caceres R, Davies N. The case for VM-based cloudlets in mobile computing. *IEEE Pervasive Computing*, 2009, 8(4): 14-23
- [11] Bonomi F, Milito R, Natarajan P, Zhu J. Fog computing: A platform for Internet of Things and analytics. *Big Data and Internet of Things: A Roadmap for Smart Environments*, 2014, 546: 169-186
- [12] Dinh H, Lee C, Niyato D, et al. A survey of mobile cloud computing: Architecture, applications, and approaches. *Wireless Communications Mobile Computing*, 2013, 13(18): 1587-1611
- [13] Loghin D, Cai S, Chen G, et al. The disruptions of 5G on data-driven technologies and applications. *arXiv preprint arXiv:1909.08096*, 2019
- [14] Mao Y, Zhang J, Letaief K. Dynamic computation offloading for mobile-edge computing with energy harvesting devices. *IEEE Journal on Selected Areas in Communications*, 2016, 34(12): 3590-3605
- [15] Xu X, He C, Xu Z, et al. Joint optimization of offloading utility and privacy for edge computing enabled IoT. *IEEE Internet of Things Journal*, 2020, 7(4): 2622-2629
- [16] Wang J, et al. Bandwidth-efficient live video analytics for drones via edge computing//Proceedings of the 2018 IEEE/ACM Symposium on Edge Computing (SEC). Seattle, WA, 2018: 159-173
- [17] Liu Y, Yang C, Jiang L, et al. Intelligent edge computing for IoT-based energy management in smart cities. *IEEE Network*, 2019, 33(2): 111-117
- [18] Cao Y, et al. Mobile edge computing for big-data-enabled electric vehicle charging. *IEEE Communications Magazine*, 2018, 56(3): 150-156
- [19] Chen S, et al. Internet of Things based smart grids supported by intelligent edge computing. *IEEE Access*, 2019, 7: 74089-74102
- [20] Taleb T, Dutta S, Ksentini A, et al. Mobile edge computing potential in making cities smarter. *IEEE Communications Magazine*, 2017, 55(3): 38-43
- [21] Chang X, et al. From insight to impact: Building a sustainable edge computing platform for smart homes//Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). Singapore, 2018: 928-936
- [22] Gupta N, Anantharaj K, Subramani K. Containerized architecture for edge computing in smart home: A consistent architecture for model deployment//Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI). Coimbatore, India, 2020: 1-8
- [23] Zhang K, Mao Y, Leng S, et al. Optimal delay constrained offloading for vehicular edge computing networks//Proceedings of the 2017 IEEE International Conference on Communications (ICC). Paris, France, 2017: 1-6
- [24] Chen M, Li W, et al. Edge cognitive computing based smart healthcare system. *Future Generation Computer Systems*, 2018, 86: 403-411
- [25] Peralta G, et al. Fog computing based efficient IoT scheme for the Industry 4.0//Proceedings of the 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM). Donostia-San Sebastian, Spain, 2017: 1-6
- [26] Tong L, Li Y, Gao W. A hierarchical edge cloud architecture for mobile computing//Proceedings of the 35th Annual IEEE International Conference on Computer Communications. CA, USA, 2016: 1-9
- [27] Tan H, Han Z, Li X, et al. Online job dispatching and scheduling in edge-clouds//Proceedings of the IEEE Conference on Computer Communications. Atlanta, USA, 2017: 1-9
- [28] Shah-Mansouri H, et al. Hierarchical fog-cloud computing for IoT systems: A computation offloading game. *IEEE Internet of Things Journal*, 2018, 5(4): 3246-3257
- [29] Zakhary V, Amiri M J, et al. Towards global asset management in blockchain systems. *arXiv preprint arXiv:1905.09359*, 2019

- [30] Berger C, Penzenstadler B, et al. On using blockchains for safety-critical systems//Proceedings of the 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS). New York, USA, 2018: 30-36
- [31] Wu S, Du J. Electronic medical record security sharing model based on blockchain//Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSPP). New York, USA, 2019: 13-17
- [32] Underwood S. Blockchain beyond bitcoin. Communications of the ACM, 2016, 59(11): 15-17
- [33] Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese)  
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481-494)
- [34] Lamport L, Shostak R, Pease M. The Byzantine generals problem. Transactions on Programming Languages and Systems, 1982, 4(3): 382-401
- [35] Merkle R. A certified digital signature//Proceedings of the Conference on the Theory and Application of Cryptology (CRYPTO). New York, USA, 1989: 218-238
- [36] Lamport L. The part-time parliament. ACM Transactions on Computer Systems, 1998, 16(2): 133-169
- [37] Lamport L. Fast Paxos. Distributed Computing, 2016, 19: 79-103
- [38] Moraru I, Andersen D G, Kaminsky M. There is more consensus in Egalitarian parliaments//Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles (SOSP). New York, USA, 2013: 358-372
- [39] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm//Proceedings of the 2014 USENIX Annual Technical Conference (ATC). Philadelphia, PA, 2014: 305-319
- [40] Miller A, Juels A, Shi E, et al. Permacoin: Repurposing bitcoin work for data preservation//Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP). CA, USA, 2014: 475-490
- [41] Luu L, Narayanan V, Zheng C, et al. A secure sharding protocol for open blockchains//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS). New York, USA, 2016: 17-30
- [42] Kokoris-Kogias E, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding//Proceedings of the IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2018: 583-598
- [43] Zamani M, et al. Scaling blockchain via full sharding//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS). New York, USA, 2018: 931-948
- [44] Al-Bassam M, et al. Chainspace: A sharded smart contracts platform//Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS). San Diego, USA, 2018: 18-21
- [45] Wang J, Wang H. Monoxide: Scale out blockchain with asynchronous consensus zones//Proceedings of the 16th USENIX Conference on Networked Systems Design and Implementation (NSDI). Berkeley, USA, 2019: 95-112
- [46] Szabo N. Formalizing and securing relationships on public networks. First Monday, 1997, 2(9)
- [47] Fan Ji-Li, Li Xiao-Hua, Nie Tie-Zheng, Yu Ge. Survey on smart contract based on blockchain system. Computer Science, 2019, 46(11): 1-10(in Chinese)  
(范吉立, 李晓华, 聂铁铮, 于戈. 区块链系统中智能合约技术综述. 计算机科学, 2019, 46(11): 1-10)
- [48] Ferrag M A, Derdour M, Mukherjee M, et al. Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 2018, 6(2): 2188-2204
- [49] Li M, Zhu L, Lin X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. IEEE Internet of Things Journal, 2019, 6(3): 4573-4584
- [50] Zeng Y, Huang Y, Liu Z, et al. Joint online edge caching and load balancing for mobile data offloading in 5G networks//Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Dallas, USA, 2019: 923-933
- [51] Tuli S, Mahmud R, et al. FogBus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, 2019, 154: 22-36
- [52] Yue D, Li R, Zhang Y, et al. Blockchain-based verification framework for data integrity in edge-cloud storage. Journal of Parallel and Distributed Computing, 2020, 146: 1-14
- [53] Rehman M, Javaid N, Awais M, et al. Cloud based secure service providing for IoTs using blockchain//Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM). Waikoloa, USA, 2019: 1-7
- [54] Stanciu A. Blockchain based distributed control system for edge computing//Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS). Bucharest, 2017: 667-671
- [55] Dillenberger D, et al. Blockchain analytics and artificial intelligence. IBM Journal of Research and Development, 2019, 63: 1-14
- [56] Kang J, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670
- [57] Pahl C, Ioini N, Helmer S, et al. An architecture pattern for trusted orchestration in IoT edge clouds//Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC). Barcelona, Spain, 2018: 63-70
- [58] Sharma P K, Park J H. Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 2018, 86: 650-655
- [59] Pan J, Wang J, Hester A, et al. EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet of Things Journal, 2019, 6(3): 4719-4732

- [60] Dorri A, Kanhere S, Jurdak R, et al. Blockchain for IoT security and privacy: The case study of a smart home//Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Kona, USA, 2017: 618-623
- [61] Dorri A, Kanhere S, Jurdak R. Blockchain in Internet of Things: Challenges and Solutions. arXiv preprint arXiv: 1608.05187, 2016
- [62] Zhu Lie-Huang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186(in Chinese)  
(祝烈煌, 高峰, 沈蒙等. 区块链隐私保护研究综述. 计算机研究与发展, 2017, 54(10): 2170-2186)
- [63] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data//Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW). San Jose, CA, 2015: 180-184
- [64] Guo H, Li W, Nejad M, et al. Access control for electronic health records with hybrid blockchain-edge architecture//Proceedings of the IEEE International Conference on Blockchain. Atlanta, USA, 2019: 44-51
- [65] Ren Y, Zhu F, Qi J, et al. Identity management and access control based on blockchain under edge computing for the industrial Internet of Things. Applied Sciences, 2019, 9(10): 2058
- [66] Rahulamathavan Y, et al. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption//Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). Bhubaneswar, India, 2017: 1-6
- [67] Zhao H, et al. Lightweight backup and efficient recovery scheme for health blockchain keys//Proceedings of the IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). Bangkok, Thailand, 2017: 229-234
- [68] Yang Z, Yang K, et al. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 2019, 6(2): 1495-1505
- [69] Hassan M, et al. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 2019, 97: 512-529
- [70] Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of Medical Systems, 2018, 42: 140
- [71] Wu H, Tsai C. Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing. IEEE Consumer Electronics Magazine, 2018, 7(4): 65-71
- [72] Christidis K, et al. Blockchains and smart contracts for the Internet of Things. IEEE Access, 2016, 4: 2292-2303
- [73] Yan Y, Wei C, et al. Confidentiality support over financial grade consortium blockchain//Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data. New York, USA, 2020: 2227-2240
- [74] Hassan M, Rehmani M, Chen J. Differential privacy in blockchain technology: A futuristic approach. Journal of Parallel and Distributed Computing, 2020, 145: 50-74
- [75] Huang Y, et al. Resource allocation and consensus on edge blockchain in pervasive edge computing environments//Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Dallas, USA, 2019: 1476-1486
- [76] Xu C, et al. Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(4): 870-882
- [77] Qi X, Zhang Z, Jin C, et al. BFT-store: Storage partition for permissioned blockchain via erasure coding//Proceedings of the 2020 IEEE 36th International Conference on Data Engineering (ICDE). Dallas, USA, 2020: 1926-1929
- [78] Xu Z, Han S, Chen L. CUB, a consensus unit-based storage scheme for blockchain system//Proceedings of the 2018 IEEE 34th International Conference on Data Engineering (ICDE). Paris, France, 2018: 173-184
- [79] Kumar K, Liu J, Lu Y, et al. A survey of computation offloading for mobile systems. Mobile Networks and Applications, 2013, 18: 129-140
- [80] Liu M, Yu F, et al. Computation offloading and content caching in wireless blockchain networks with mobile edge computing. IEEE Transactions on Vehicular Technology, 2018, 67(11): 11008-11021
- [81] Xiong Z, Zhang Y, et al. When mobile blockchain meets edge computing. IEEE Communications Magazine, 2018, 56(8): 33-39
- [82] Amiri M, Maiyya S, et al. SeeMoRe: A fault-tolerant protocol for hybrid cloud environments//Proceedings of the 2020 IEEE 36th International Conference on Data Engineering (ICDE). Dallas, USA, 2020: 1345-1356
- [83] Douceur J R. The sybil attack//Proceeding of the First International Workshop on Peer-to-Peer Systems. London, UK, 2002: 251-260
- [84] Satija S, et al. Blockene: A high-throughput blockchain over mobile devices//Proceedings of the 14th Symposium on Operating Systems Design and Implementation. Virtual Event, 2020: 567-582
- [85] Serguei Popov. The tangle. White Paper, 2016
- [86] Gao Zheng-Feng, Zheng Ji-Lai, Tang Shu-Yang, et al. State-of-the-art survey of consensus mechanisms on DAG-based distributed ledger. Journal of Software, 2019, 31(4): 1124-1142(in Chinese)  
(高政风, 郑继来, 汤舒扬等. 基于 DAG 的分布式账本共识机制研究. 软件学报, 2019, 31(4): 1124-1142)
- [87] Baird L. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. White Paper, 2016



**TONG Xing**, Ph. D. candidate. His research interests include blockchain and edge computing.

**ZHANG Zhao**, Ph. D. , professor. Her research interests include blockchain, massive data management and data mining.

**JIN Che-Qing**, Ph. D. , professor. His research interests include blockchain and massive data mining.

**ZHOU Ao-Ying**, Ph. D. , professor. His research interests include data management and applications, inclusive of Web data management, data intensive computing, in-memory cluster computing, big data benchmarking and performance optimization.

Background

This article summarizes the problems of the integration of blockchain and end-edge-cloud systems from the perspective of blockchain and this article belongs to the category of blockchain. As a decentralized ledger technology, blockchain is essentially a distributed computing model that can build a secure interactive platform for multiple parties who do not trust each other.

With the advent of edge computing, it is possible to provide services close to service requesters, which reduces the response time compared to cloud computing. Although edge computing can provide low-latency services compared to cloud computing, the end-edge-cloud architecture formed by the fusion of edge computing and cloud computing can meet diverse application needs. Existing works only consider the fusion of edge computing and blockchain, which limit the effect of blockchain in edge scenarios.

This article focuses on the integration of the blockchain

and the end-edge-cloud cloud system, the integration of blockchain and end-edge-cloud architecture can ensure the safe transmission, safe storage and safe computing in end-edge-cloud system, and guarantee the safety of the end-edge-cloud system. However, because of the blockchain’s consensus mechanism and full copy storage mechanism, blockchain nodes need to perform strong storage and computing capabilities, which poses challenges for the deployment of blockchain in edge scenarios. From the perspective of blockchain, this article considers how to integrate the blockchain and the end-edge-cloud system based on the blockchain’s storage, computing, privacy and scalability characteristics and proposes some possible solutions and future research directions.

This work is supported by the National Natural Science Foundation of China (61972152, U1911203) and the Guangxi Key Laboratory of Trusted Software (No. kx202005).