区块链赋能 6G

代玥玥[1]，张科[1]，张彦[2]
（1. 电子科技大学信息与通信工程学院，四川 成都 611731；2. 挪威奥斯陆大学，挪威 奥斯陆 0316）

摘　要：6G 网络在探索更高通信速率的同时，将结合云计算、边缘计算、人工智能、大数据等新兴技术，以全新的网络架构实现跨网跨域间更广泛的互联互通，为工业物联网、智慧城市和智能交通提供智能、安全、高效的技术支持。区块链技术作为一种去中心化、公开透明的分布式账本技术，将为 6G 提供强有力的安全保障。针对区块链技术与 6G 的融合展开了研究，首先给出了 5G 网络与 6G 网络的区别以及 6G 网络所面临的挑战，并对区块链技术在频谱管理、移动边缘计算与 D2D 通信方面的研究现状进行了总结。然后对区块链与 6G 新兴技术的融合进行了探索，分别提出了区块链与云边端协同、区块链与联邦学习、基于区块链的资源交易以及针对边缘网络的轻量级区块链所面临的技术挑战，并给出了对应的解决方案。

关键词：区块链；6G；数据共享；资源分配
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2020.00154

Blockchain empowered 6G

DAI Yueyue[1], ZHANG Ke[1], ZHANG Yan[2]
1. School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
2. University of Oslo, Oslo 0316, Norway

Abstract: 6G network not only explore higher communication rates but also combine with the emerging technologies such as cloud computing, edge computing, artificial intelligence, and big data, and use a new network architecture to achieve wider interconnection and interoperability across network and domains, and provide an intelligent, safe and efficient technical support for industrial Internet of things, smart cities, and intelligent transportation. Blockchain technology as a decentralized, open and transparent distributed ledger technology can provide strong security for 6G. The integration of blockchain technology and 6G network was studied. Firstly, the difference between 5G and 6G network and the challenges of 6G faced were given, and the research of blockchain technology in spectrum management, mobile edge computing and D2D communication was reviewed. Then, the integration of blockchain technology and 6G emerging network was explored. Thus, the technical challenges in terms of blockchain and the cloud-edge-device network, blockchain and federal learning, blockchain-based resource transactions, and lightweight blockchain for edge network were presented. The corresponding solutions were also given.

Key words: blockchain, 6G, data sharing, resource allocation

1　引言

据 Gartner 预测，移动终端数量在 2020 年将达 250 亿台，思科云指数则预测这个数量将达 750 亿台，百亿级的终端设备将导致数据的爆发式增长。据互联网数据中心（IDC, international data corporation）预测，全球数据总量将从 2018 年的 33 ZB 增至 2025 年的 175 ZB。移动互联网的快速迭代和更新，使得虚拟现实（VR, virtual reality）、超高清视频流（UHD, ultra-high-definition）及智能驾驶等具有超低时延、高可靠性和低功耗需求的新应用逐渐兴起。为了应对海量终端、海量数据、新兴应用的性能需

收稿日期：2020−02−05；修回日期：2020−03−03

求，6G 将作为新型通信技术，从线上到线下、从消费到生产、从平台到生态，为众多诸如智能交通、数字化办公、智慧城市等新型服务和工业生产提供强有力的技术支持，并通过数以百万计的人与物、物与物、物与网之间的互联来促进跨网跨域的通信、计算、存储以及供能等方面的无缝协作。

5G 已经成熟且即将商业化，学术界、工业界以及政府现已启动 6G 研究计划。芬兰政府于 2019 年率先在世界范围内发布了首份 6G 白皮书[1]，并且给出了若干衡量 6G 技术的关键指标，分别为峰值速率达到 100 Gbit/s～1 Tbit/s，而 5G 仅为 10 Gbit/s；室内定位精度为 10 cm，室外定位精度为 1 m，相比 5G 提高了 10 倍；通信时延为 0.1 ms，是 5G 的 1/10；超高可靠性，中断概率小于百万分之一；超高密度，连接设备密度达每立方米过百个。此外，文献[1]重点强调了安全和隐私保护在 6G 网络中的重要性。一方面，全球化部署使得 6G 网络中存在海量数据与信息，数据和信息的泄露将给个人和企业造成严重的经济损失。另一方面，6G 无线网络将实现地面、卫星和空中网络的全面连接，以最大限度支持信息的互通。复杂多变的网络连接和更频繁的通信将增加信息泄露发生的概率，而信息的泄露可能造成通信网络瘫痪，从而影响商业合作、交通出行、工业生产等方面的正常运行。因此，安全和隐私保护是 6G 网络的研究重点之一。

区块链技术是一种基于分布式对等网络的去中心化分布式账本技术[2]。在区块链中，对等实体间可自由进行交易，交易的信息由所有网络参与者共同管理。区块链技术具有去中心化、不可篡改、可追溯、匿名性和透明性五大特征，这些特征为构建安全可信的分布式交易环境提供了良好的契机。我国于 2019 年 10 月提出把区块链技术与现有应用进行集成，使得区块链技术在新的技术革新和产业变革中具有重要作用[3]。目前，区块链技术已经被集成于金融、医疗、数字政务、物流、工业生产以及智慧城市等领域中。

为了获得更优的性能，区块链技术可以与 6G 网络进行集成，以构建安全可信的移动网络和服务。美国联邦通信委员会（FCC, the Federal Communications Commission）在 2018 美国移动世界大会上首次展望了 6G 技术[4]，强调 6G 将迈入太赫兹频谱时代，并提出可将区块链技术引入频谱管理中，设计更安全、灵活的频谱共享机制，在提升频谱利用率的同时，提高频谱交易的安全性。中国联合网络通信集团有限公司提出将区块链技术引入 6G 网络中，并利用区块链的分布式协作机制来支持通信服务节点间更安全、更稳健和更扁平化的交互，进一步提升通信网络的覆盖、通信和服务。因此，区块链技术可与无线通信技术结合，在频谱、带宽、信道的管理与调度方面提供安全性保障。

区块链与 6G 的融合还有望为新兴技术提供安全、可靠的部署环境[5]。在下一代网络中，为了充分实现万物互联，云计算、边缘计算、人工智能和大数据等先进技术将发挥重要的作用[6]。云计算为 6G 网络提供强劲的数据处理和信息存储能力，边缘计算为计算密集和时延敏感性应用提供就近的计算服务，以提升用户体验，人工智能和大数据为实现智慧网络、智能管控提供技术支持。但是，这些新兴技术的引入也带来了新的信任和安全问题。目前，云计算主要采用集中式架构，这种架构虽然便于管理数据和服务，但是易受单点故障的影响。另外，由于用户对存储在云服务器上的数据失去了控制权，因此，数据和隐私存在泄露的风险。边缘计算虽然采用分布式架构，但是计算任务的迁移仍然可能受到恶意节点的干扰攻击或拒绝服务式攻击。基于人工智能的 6G 应用则可能面临训练数据和模型被窃取等安全问题。当前的 6G 新兴技术需要一个安全、公开、透明的系统，区块链具有去中心化、不可篡改、可追溯的特征，可以提升 6G 网络的稳健性、数据隐私性和安全透明性。因此，区块链将会是保障 6G 网络安全和隐私最有潜力的技术。

本文围绕如何将区块链技术与 6G 网络融合展开研究。首先给出了 5G 网络与 6G 网络的区别以及 6G 网络所面临的挑战，并分析了区块链技术与 6G 网络融合在频谱管理、边缘计算与端到端（D2D, device-to-device）通信等方面的研究。然后分别从网络架构、与人工智能结合的数据共享、资源交易以及针对边缘网络的轻量级区块链 4 个方面提出了区块链技术与 6G 网络进一步深入融合的技术挑战和解决方案，最后总结全文。

2 区块链赋能的 6G

5G 网络主要利用毫米波通信、大规模 MIMO 等通信技术以及软件定义网络（SDN, software defined networking）、网络功能虚拟（NFV, network

functions virtualization）等技术提升通信速率，降低通信时延和能耗，从而支持增强移动带宽业务（eMBB, enchanced mobile broadband）、超高可靠超低时延通信（uRLLC, ultra-reliable low latency communication）、大规模机器类通信（mMTC, massive machine type of communication）。然而，随着 5G 网络部署的展开，网络规模越来越大、设备间交互的数据越来越多、网络连接也更复杂。如果基于现有的 5G 网络，万物互联这一目标将难以达成。6G 网络将结合具体场景，在现有网络上做进一步的提升和扩展，以实现移动带宽高可靠超低时延通信（MBRLLC, mobile broadband reliable low latency communication）、大连接高可靠超低时延通信（mURLLC, massive ultra-reliable low latency communication）和以人为中心的服务（HCS, human-centric service）[7]。另外，虚拟现实/增强现实、无人驾驶、智能交通等应用的普及，使得用户对网络的通信速率、时延、移动性支持和可靠性等有了更高的要求。5G 网络与 6G 网络的性能指标对比如表 1 所示，表 1 展示了 5G 网络与 6G 网络在性能指标和应用类型方面的区别[1]。

表 1　5G 网络与 6G 网络的性能指标对比

	5G	6G
应用类型	eMBB	MBRLLC
	uRLLC	mURLLC
	mMTC	HCS
峰值速率	10 Gbit/s	100 Gbit/s～1 Tbit/s
端到端时延	1 ms	0.1 ms
设备密集度	$10/m^3$	$100/m^3$
移动性支持	500 km/h	1 000 km/h
可靠性	$<10^{-5}$	$<10^{-9}$
流量情况	10 MB/(s·m^2)	<10 GB/(s·m^2)

根据表 1 可知，6G 网络的性能将得到大幅度提升。然而，6G 网络的具体实现将面临以下挑战。

1) 更广泛的万物互联：万物互联使得移动终端规模呈爆发式增长，未来网络的连接数量将达百亿级，超大规模连接对 6G 网络的可扩展性和可靠性提出了巨大挑战。另一方面，为了保证 D2D 通信和机器到机器通信的超低时延，6G 网络需要考虑如何将资源尽可能地向终端设备和用户倾向，同时满足多个用户的服务质量需求，以支持分布式节点间更安全、更稳健和更扁平化地交互。

2) 安全的通信生态：物联网的广泛部署，使得 6G 网络中来自手机、传感器和可穿戴设备等底层终端的数据量剧增。相比于 5G 网络，6G 网络中设备间的数据传输更频繁。由于 6G 网络趋向于扁平化，传统的集中式安全认证和接入控制机制将不再适用。6G 网络需要建立安全可信的分布式数据交互与通信机制。

3) 可追溯的资源管理：5G 网络和 5G Beyond 网络利用边缘计算和人工智能设计高效的资源管理机制，以支持具有超低时延和超高计算资源需求的应用。然而，目前的资源管理机制几乎不考虑资源使用的可追溯性，因此，可能存在恶意用户非法占用资源的现象。6G 网络不仅需要考虑未来网络拓扑结构的复杂性以及高度动态性，还需要考虑资源使用的可追溯性，以保证资源得到安全且合理的利用。

区块链作为一种分布式的数据结构，无任何第三方参与，可用于构建安全可信的网络交互环境。首先，由于无第三方权威机构介入，区块链可避免由第三方引起的数据泄露隐患，同时可消除用户与第三方机构之间在数据共享和资源交易期间的通信开销。其次，由于用户之间的所有交易均被永久完整地记录在区块链账本中，因此，区块链可为 6G 网络提供具有可追溯性的通信，这不仅便于网络管理者随时查询历史资源情况，还可以降低恶意用户杜撰资源使用情况的行为。此外，区块链采用多方共识机制记录用户间的交互，从而保证所有交互的公正、公开。

6G 网络一方面将利用太赫兹、空天地一体化通信等提升网络带宽和频谱利用率，另一方面将结合云计算、边缘计算、人工智能、大数据等新兴技术，实现跨网跨域间更广泛的互联互通。区块链与 6G 的结合将为构建安全可信的通信生态提供强有力的安全保障，目前，关于区块链与 6G 融合的研究主要涉及基于区块链的频谱管理、区块链与移动边缘计算的融合以及区块链与 D2D 通信等方面。

2.1　基于区块链的 6G 频谱管理

在基于区块链的频谱管理研究中，文献[8]提出了基于区块链校验和接入控制机制，以完成主用户与次用户之间的频谱共享。首先，引入了虚拟货币 Specoins，并基于拍卖理论建立了主用户与次用户之间的频谱共享。其次，采用了区块链校验和记录主用户与次用户之间的频谱交易信息。最后，证明

了基于区块链的频谱管理具有良好的可扩展性，并且可保证系统免受 DoS 攻击。文献[9]基于联盟区块链，设计了无人机与地面通信系统之间安全的频谱交易和共享方案。首先，为了避免频谱交易过程中恶意用户引起的安全和隐私问题，提出了基于区块链的分布式频谱共享架构。然后，基于 Stackelberg 博弈模型设计了无人机与地面通信系统之间的最优频谱竞价方案。文献[10]将频谱感知作为一种服务，提出了基于区块链的频谱感知即服务（Spass, spectrum sensing as a service）方案。其中，智能合约作为核心组件，主要负责完成：1) 调度用户与 Helper 之间频谱分配，最大化系统收益；2) 识别 Helper 是否为恶意节点，保证频谱交易和共享的安全性。

区块链技术能够为 6G 网络提供一个安全、智能、高效的动态频谱共享环境，利用区块链技术，用户之间可进行安全的频谱共享，进一步提升系统的频谱利用率。目前，国内外已经开始研究区块链与频谱管理的结合，但是关于区块链在 6G 网络中如何部署、区块链本身的开销对系统成本的影响以及针对具体应用场景的共识机制设计等诸多关键问题还有待解决。

2.2 区块链与移动边缘计算的融合

边缘计算的动态网络环境使得缓存的内容和所迁移的数据容易受到恶意节点的干扰攻击或拒绝服务式攻击，区块链可应用于移动边缘计算中解决上述问题。文献[11]将区块链应用于边缘计算中，建立了一套安全的分布式能源交易系统。在该系统中，边缘节点间进行能量交易以便完成自身的计算任务，区块链通过智能合约获取向边缘节点分发任务并负责维护边缘节点的身份信息，以保证能量交易的安全和用户隐私。文献[12]将区块链应用于车载边缘计算网络中，提出了安全的车载数据存储与共享机制。

另一方面，移动边缘计算可以为区块链提供分布式的计算资源，以保证边缘节点能正常运行区块链。文献[13]提出了区块链可采用边缘节点的计算资源运行区块链的共识算法。首先，分析了基于工作量证明（PoW, proof-of-work）的区块链技术需消耗大量的 CPU 时间和能量资源，不适用于资源受限的移动设备。其次，利用经济学模型设计了针对区块链的计算资源管理策略。最后，提供了具有移动边缘计算功能的区块链系统的演示原型，并给出了实验结果以证明所提概念的合理性。文献[14]考虑分布式网络的多跳协作性，提出将计算密集型区块链挖掘任务卸载到边缘服务器，以保证区块链的正常运行。利用博弈论提出了针对数据处理和区块链挖矿任务的多跳式计算迁移问题，以尽可能降低物联网区块链的运行成本。

此外，区块链与移动边缘计算的结合，还可应用于视频共享、工业物联网等方面。文献[15]针对移动边缘计算网络，设计了基于区块链的分布式安全视频传输和共享机制。在所提机制中，基站负责提供用于视频共享的计算和通信资源，智能合约自动执行视频转码和共享流程。基于所提机制，基站、用户和视频提供者 3 方共同参与区块链的构建和维护，以保证安全的视频传输和共享。文献[16]将区块链、人工智能与边缘计算 3 者结合，提出了针对工业物联网的安全智能的区块链架构，以实现安全的跨域资源调度。

下一代网络为了同时满足超大规模计算的应用和时延敏感性应用，将会同时存在云服务器和边缘服务器，并通过云边端的协同，保证所有应用的服务质量。目前，关于区块链和移动边缘计算的研究主要涉及用户和边缘节点，而针对区块链与云边端网络结合的问题尚未涉及。

2.3 基于区块链的 D2D 通信

随着智能通信终端的普及和移动通信技术的更新迭代，用户对近距离通信的需求日渐增强。D2D 通信作为一种最直接的近距离通信技术，可以提高频谱利用率，因此，被广泛认为是下一代移动通信的关键技术之一。然而，在不可信的 D2D 环境中进行设备间的数据共享，可能会造成数据泄露。另外，由于没有身份和权限认证，恶意节点可随时进行非法访问。因此，如何在确保低时延的同时进行安全的 D2D 数据共享是值得研究的问题。现有的解决方案需要依赖外部权威机构进行设备身份验证和数据访问授权，但是外部机构的引入不仅会增加不必要的通信开销，还会降低整体的网络性能。

区块链不需要依赖外部权威机构为 D2D 通信提供安全方面的保障。文献[17]利用区块链设计了一种分布式 D2D 数据共享架构，其中，Access Point 负责校验设备间的交易。为了使终端用户能及时收集 D2D 区块链的数据，采用轻量级区块校验方案，委托权益证明（DPoS, delegated proof-of-stake）作为一致性共识算法。为了衡量交易和区块的质量，

分别制定了交易中继的价值函数和区块验证的价值函数两个模型，并基于合同理论提出了适用于 D2D 区块链的激励机制，从而实现用户间的高效安全数据共享。文献[18]提出了基于区块链和 D2D 通信的任务迁移策略。主要利用区块链的可追溯和去中心化的特性，记录 D2D 网络中的任务迁移和内容缓存行为，以保证边缘服务器之间安全的信息交互。目前，大部分工作主要借助 D2D 网络进行区块链的信息传递，而关于信息传递过程中涉及的带宽、时延以及能耗方面的研究尚不明确。未来工作应研究区块链在信息传递过程中的开销，设计更合理的区块链应用方案。

上述工作主要介绍了区块链在频谱管理、移动边缘计算与 D2D 通信方面的国内外研究现状。近年来，云计算与边缘计算的协同、联邦学习、大数据等新兴技术备受关注，6G 网络将利用这些技术实现跨网跨域的网络互联。然而，目前关于区块链与这些新兴技术融合的工作相对较少。接下来，本文将重点针对区块链与云边端协同、区块链与联邦学习、基于区块链的资源交易以及针对边缘网络的轻量级区块链进行分析，并给出相应的解决思路，为未来相关问题的研究提供参考。

3　区块链与新兴技术融合的挑战与解决思路

本节将对区块链与 6G 网络中新兴技术的融合做进一步的探索，将分别从网络架构、应用、资源管控和轻量级区块链 4 个角度进行分析，并给出相应的解决思路，以期更全面地理解区块链与 6G 网络的融合。

3.1　基于区块链的云边端协同网络架构

移动边缘计算将计算和存储资源分布式部署在基站、路边单元或接入点等无线通信基础设施上[19-20]。然而，出于成本考虑，部署在无线通信基础设施上的计算和存储资源通常有限。当多个用户或多个计算密集型任务同时运行时，有限的计算和存储资源将无法支撑所有用户的应用需求。另一方面，云服务器可以为用户提供强大的计算和存储功能，如果在下一代网络架构中仅考虑边缘而不考虑云端的资源和能力，则会造成资源的巨大浪费并且严重影响网络的可扩展性。因此，下一代网络需考虑云边端的协同。云边端协同可支持灵活的资源调度和计算迁移，也使得用户、边缘服务器以及云服务器 3 者之间的交互异常频繁。然而，如果不在设计网络架构时考虑数据安全和用户隐私，频繁的网络交互将进一步增加数据泄露等恶意攻击发生的概率。因此，本文提出了区块链赋能的云边端协同网络架构，基于区块链的云边端协同网络架构如图 1 所示。该架构由 3 个平面构成，即终端层、边缘层和中心云层[2]。

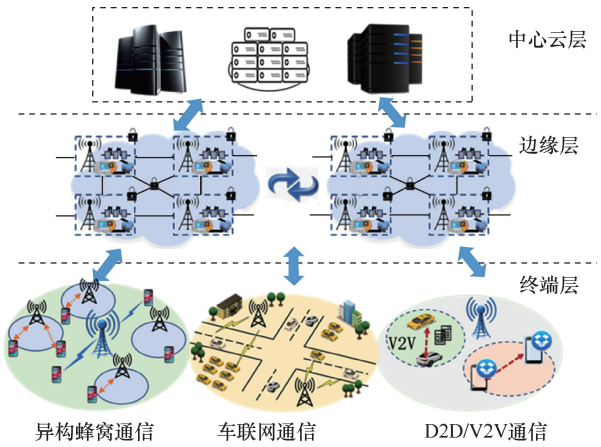


图 1　基于区块链的云边端协同网络架构

终端设备具有多种不同功能的应用程序，如短视频、导航地图、在线游戏等，这些应用程序对计算资源和存储资源要求较高。最新的终端设备均具有一定的计算和存储能力，可支持部分计算密集和时延敏感型应用。然而由于终端设备的电池容量有限，仍需借助边缘服务器或云服务器处理部分应用。终端设备主要通过无线通信接入边缘服务器或云服务器的计算和存储资源，然而，由于无线通信的接入是多样的，因此，所提架构按照无线网络拓扑和通信模式将终端层进一步细分为大小蜂窝并存的异构蜂窝通信、面向车载应用的车联网通信以及 D2D/V2V 通信。

边缘层位于网络的边缘，由多个分布式部署的边缘服务器构成。边缘服务器通常分布于如咖啡馆、购物中心、公交、街道、公园等位置的基站、路边单元、接入点，利用部署在边缘服务器中的计算和存储资源，用户可运行具有低时延需求的应用。所提架构中的边缘服务器除了部署计算和存储资源以外，还部署了区块链。区块链的引入一方面可以激励边缘服务器分享自身闲置的资源，提升系统整体的资源利用率；另一方面可以追踪和记录网络中的各个实体间数据共享、内容投递、任务迁移等行为，以维护一个安全、可信的网络生态。

中心云层由多个具有高性能计算能力和超强

存储能力的服务器组成。由于具有全局视图，该层可利用数据挖掘和大数据等先进技术，通过预测某些事件或预先分配一些资源，将被动式响应网络转变为主动式感知网络，从而加快业务处理速度，提升网络吞吐量。其次，充足的计算资源和缓存资源使得云服务器可处理高度复杂或具有时延容忍特征的应用程序，并存储大容量或不太流行的内容，以缓解边缘服务器的压力。

值得注意的是，由于终端设备的应用时延敏感且边缘网络的资源相对有限，因此，在设计区块链的共识机制时，应尽可能避免选择如 PoW 或者 Proof-of-Stake 等需耗费大量计算资源和能量的一致性算法。

3.2　基于区块链和联邦学习的数据共享

欧洲联盟于 2018 年颁布了《通用数据保护条例》以保护用户隐私，防止个人敏感数据被滥用。该条例规定，在没有获得原始数据拥有者授权的情况下，不允许企业之间直接交换数据。因此，许多传统的数据交换和共享方式面临失效。另一方面，数据在各个用户中独立存储、独立维护，彼此间互不沟通，形成了一座座无法联通的数据“孤岛”。然而 6G 时代的到来，必将大幅度提升数据的量级，万物互联也将带来海量的数据信息。如果这些数据依然彼此独立、无法联通，那么数据本身的价值将得不到体现，也会严重影响企业效益甚至社会发展。因此，6G 时代，需要考虑如何在满足数据隐私、安全和监管要求的前提下，设计合理的数据共享和交互方案。

近年来，联邦学习作为一个满足隐私保护和数据安全的可行方案，受到了广泛关注。联邦学习是 Google AI 提出的一种分布式机器学习方案，它允许多个参与者协作共同建立数据模型，同时保证各方原始训练数据始终保留在本地，从而起到保护数据安全和用户隐私的作用。具体而言，联邦学习利用终端设备的数据处理能力，分布式地执行本地模型的训练，然后终端设备再将本地训练的模型上传到中心节点执行全局模型聚合[21]。由于联邦学习需要一个中心节点完成全局模型更新，如果恶意节点对其发起单点攻击，则会造成整个平台的失效。区块链可以很好地解决集中式应用平台的单点故障失效问题，为此，本文提出了一种基于区块链和联邦学习的数据共享架构[22]，基于区块链和联邦学习的数据共享如图 2 所示。

基于区块链和联邦学习的数据共享主要分为以下 3 步。

1) 本地模型训练：首先，车辆、传感器、手机等终端从就近的边缘服务器下载最新的全局训练模型，然后基于自身的数据和计算能力进行本地模型训练。当训练完成时，终端将所学的模型上传至边缘服务器。

2) 区块链的构建与维护：基站或路边单元等边缘服务器首先对所收集的本地模型进行校验，并将其记录在区块中进行全局广播。只有通过一致性校验的区块才能上链被永久记录。因此，边缘服务器基于一致性算法校验新生成区块的正确性。当新生成的区块通过 2/3 及以上的边缘服务器的校验时，该区块及其所包含的训练模型被添加在区块链上。

3) 全局模型聚合与更新：边缘服务器基于区块

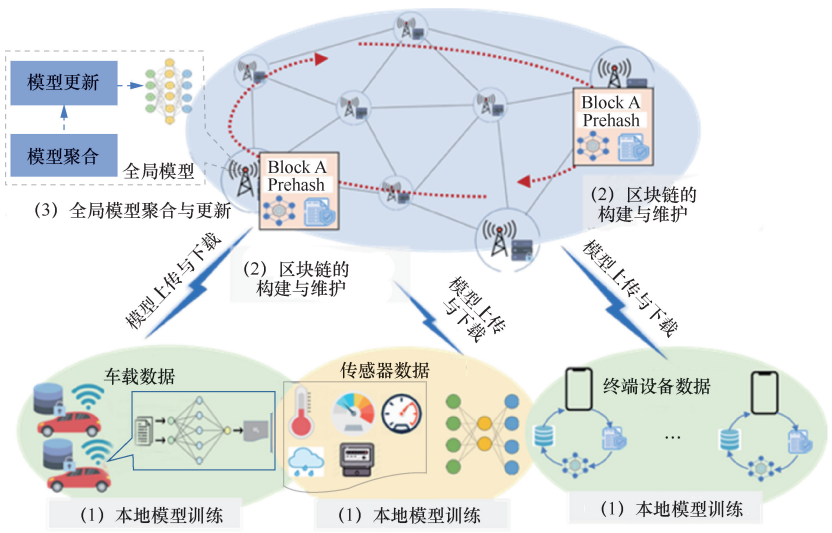


图 2　基于区块链和联邦学习的数据共享

链的记录和更新执行模型聚合。所聚合的模型为最新的全局模型，当终端设备需要再次执行本地更新时，可下载该模型。

基于区块链和联邦学习的数据共享架构主要具有 3 方面好处。首先，在所提架构中车辆和终端设备仅上传训练后的模型，原始数据始终保留在本地，防止数据和用户敏感信息泄露；另一方面，由于仅在通信链路上传输模型，因此，大幅度降低了信道的传输压力，避免了网络拥塞。其次，将区块链引入联邦学习中，规避了集中式全局更新的单点故障问题。同时，区块链作为分布式账本，可完整地记录系统中所有的模型更新，保证所有行为有据可查，从而降低了恶意节点发起篡改攻击的概率。此外，联邦学习充分利用设备和车辆的分布式计算资源进行模型训练，避免了碎片资源的浪费，大幅度提高了系统的资源利用率。综上所述，区块链和联邦学习的融合为应对 6G 海量数据的增加提供了一个很好的解决方案，能够在保证数据安全和用户隐私的前提下，充分挖掘数据本身的价值，实现网络实体间的数据共享。

3.3　基于区块链的安全资源交易机制

物联网技术的蓬勃发展催生了众多新兴应用和服务，同时也赋予了物联网设备通信、计算、存储、能量等资源。其中，通信资源主要包括频谱、带宽、信道、传输功率等无线链路资源，计算资源主要是指 CPU、硬盘容量，存储资源主要是指内存容量，能量资源主要涉及太阳能、风能等绿色资源。为了激励物联网设备分享自身闲置的资源，可采用资源货币化的策略进行资源交易，并通过分布式节点间的灵活组网，实现对等实体间资源的直接交换。目前，由于资源货币化策略涉及货币交易，因此，必须依赖于一个受信的集中化应用平台负责交易的安全性。然而，这种模式存在交易不透明和单点故障等安全问题。此外，目前的资源交易机制几乎不考虑资源使用的可追溯性，这使得恶意用户可非法占用资源，造成资源的大量浪费。为此，本文提出了基于区块链的安全资源交易机制，以保证物联网设备间资源交易的安全以及资源使用的可溯源。基于区块链的资源交易过程如图 3 所示。

从资源供需的角度考虑，本文将物联网设备分为资源的供给方与使用方。基于区块链，物联网设备间的交互主要分为以下 4 步[2]。

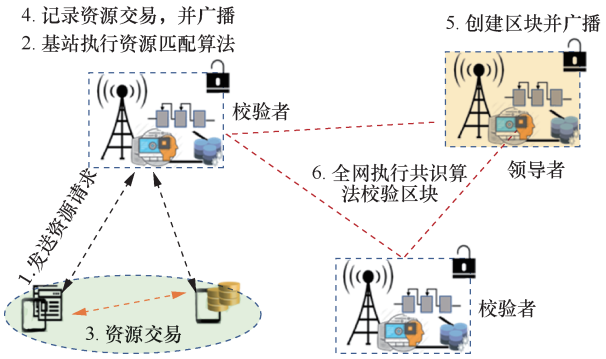


图 3　基于区块链的资源交易过程

1) 身份构建与系统初始化：采用椭圆曲线数字签名算法和非对称加密建立物联网设备和基站的身份信息。这里的身份信息主要包括公钥、私钥以及数字证书。其中，公钥可作为交易的发起方，用于验证交易的真实性；私钥可用于交易的数字签名。在系统初始化时，每个设备设有一个数字钱包的账户，该账户的地址可由公钥生成，可通过账户信息实现设备间的转账功能。

2) 针对资源交易的智能合约：基站收集其覆盖范围内所有设备的资源请求以及设备所拥有的闲置资源总量。具体地，资源使用方向邻近的基站发出资源请求，其中，包括物联网设备的位置信息、数字签名以及证书，以保证请求来源的可靠性。资源供给方向基站发送自身的资源闲置情况，其中，包括闲置的资源总量、位置信息、数字签名与证书。基站接收到资源使用方的请求后，验证资源使用方的请求和身份信息，确认其合法性。然后，基站执行资源匹配算法，匹配供给方与使用方，并向使用方提供资源供给方的信息。基于智能合约，资源供给方和使用方完成资源交易。

3) 记录交易：资源使用方向供给方付费并将交易记录发送到最近的基站。基站首先验证交易的正确性，然后向全网广播。经过一段时间后，基站将所收集的交易封装成区块，该区块采用防篡改的数据结构存储交易。多个区块通过哈希值按线性时间顺序链接，形成区块链。

4) 执行共识算法，构建区块链：区块的创建和共识主要由基站完成。负责创建区块的基站称为领导者，每一个区块可能由不同基站执行。新创建的区块需向全网广播，以触发共识算法，共识算法主要进行区块的审计和校验。

基于以上步骤，资源供给方与使用方不需要依

赖集中化平台，可直接进行资源交易。物联网设备和基站采用公钥并以匿名方式进行资源交易，真实身份未被暴露，从而保护了身份隐私并确保账户安全。此外，设备间所有的资源交易被记录在区块链上且所记录的交易带有时间戳，用户可以很方便地通过区块链追踪历史信息。因此，恶意用户对资源的不合理使用很容易被检测出来。

3.4　针对边缘网络的轻量级区块链

区块链通过维护不可篡改的分布式账本实现用户间的安全交易。按照接入许可划分，区块链可分为公有链和许可链两种类型。其中，公有链没有权限限制，任何用户均可以参与区块创建与校验，具有代表性的公有链如“比特币”和以太坊。在公有链中，参与共识算法的用户数量庞大，达成共识的时间开销很长。许可链由于只允许具有许可证书的节点参与区块创建与校验，因此，达成共识的时间被大幅度缩短。另一方面，“比特币”所采用的 PoW 共识算法对计算资源的要求很高且非常耗能。许可链的共识算法不涉及求解 PoW，可用较少的能耗与计算资源构建分布式账本。

许可链具有低能耗和低时延的优点，更适用于能量受限、时延敏感的网络。然而，目前一般将许可链应用于边缘网络的工作仅是一种简单的结合，尚未将边缘节点的计算资源限制和应用的时延约束与共识机制很好地结合起来。为此，本文针对边缘网络提出了一种基于效用证明（PoU, proof-of-utility）的共识机制，该机制选取网络中通信、计算存储能力较强的节点，对网络中的交易进行校验，从而有效解决了边缘节点因计算、存储能力不足导致的系统性能下降问题。同时还可更高效地部署针对边缘网络场景下的共识算法，使其更具针对性[23]。

基于 PoU 的共识机制主要分为代表选举和区块验证两个阶段，基于 PoU 的共识机制如图 4 所示。在代表选举阶段，用户评估基站的效用值，并基于效用值选择一定数目的基站组成代表委员会。在每次选举中，每辆车和每个设备每轮仅投一票，投票权重与其所持代币的数量成正比，最终排名由票数与权重的加权值决定。投票完成后，排名前 K 的基站被选为代表，构成代表委员会，执行区块生成和校验。在区块校验阶段，所选代表分为两个角色：领导者和验证者。领导者负责交易收集和区块生成，验证者负责区块校验。领导者的角色由所选代表轮流担任，即在每轮校验中，K 个基站中仅有一个担任领导者，其余担任验证者。具体而言，领导者首先收集一定数量的交易，然后封装成区块进行广播，当验证者收到新生成的区块时启动交叉验证。如果新生成的区块成功通过校验，则该区块被

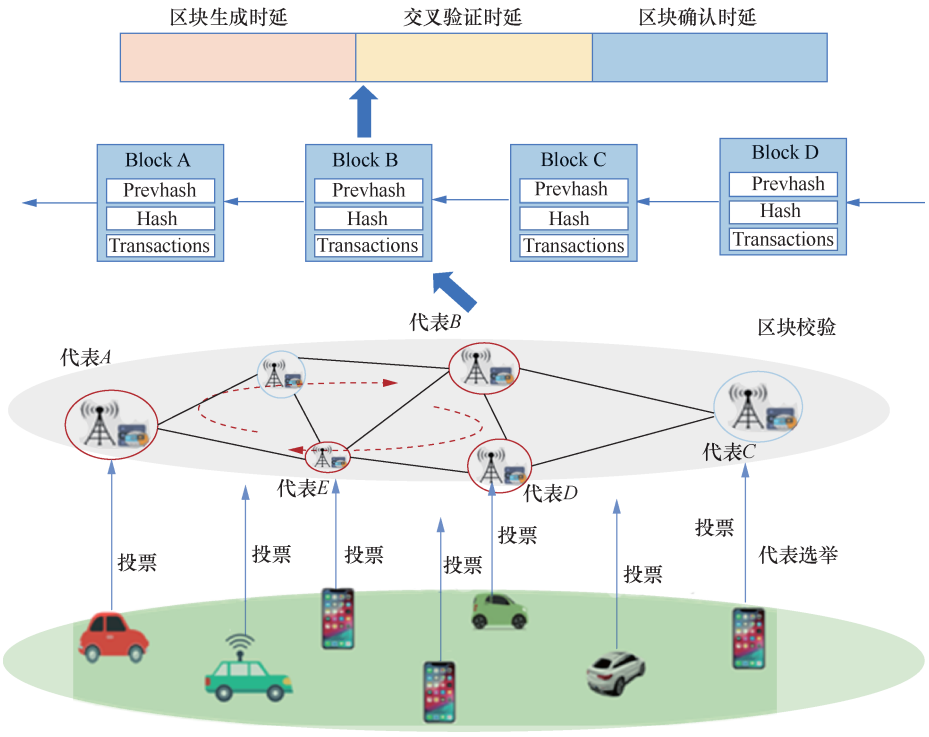


图 4　基于 PoU 的共识机制

添加在区块链中永久保存。如果新生成的区块被成功添加到区块链上，参与区块生成和校验的基站将获得一定的奖励以补偿其资源消耗。当所有代表轮流担任领导者之后，代表它们的排序被重新洗牌，然后再次以轮询的方式生成新的区块。

从用户的角度来看，区块验证时间越短，则用户体验越好。这里的区块验证时间主要由区块生成时间、交叉验证时间和区块校验确认时间组成，其时间开销与无线链路的通信质量和基站的计算资源有关。通常链路的通信质量越好、计算资源越充足，则区块验证时间越短。综合用户的时延约束，本文提出了针对边缘网络的基站效用评估函数即

$$U=\left[e^{1-\frac{T_m}{\tau_i}}-1\right]^{+} \tag{1}$$

其中，T_m 由区块生成时延、交叉验证时延、区块确认时延以及用户间的交易传输时延构成，τ_i 表示用户的时延约束，该函数主要用于指导用户的投票。

本文提出的基于 PoU 的共识机制选择网络中通信质量好、计算资源充足的节点进行区块校验，能加快共识进程，最大限度地提升网络性能，避免因资源不足或故障而导致的系统问题。另外，代表选举机制筛选出一定数目的优质基站，可更进一步地缩减参与共识的基站数目，实现更轻量级的区块链。

4　结束语

6G 将利用云计算、边缘计算、人工智能等新兴技术，实现跨网跨域智能高效的互联互通。区块链技术作为一种去中心化、公开透明的分布式账本技术，将为 6G 提供强有力的安全保障。本文针对区块链技术与 6G 网络的融合展开研究，首先给出了 5G 网络与 6G 网络的区别以及 6G 网络所面临的挑战，总结了区块链技术在频谱管理、移动边缘计算以及 D2D 通信方面的研究现状。然后给出了区块链与 6G 融合在网络架构、数据共享与资源交易方面面临的技术挑战和解决思路，同时，提出了从通信质量和计算能力等网络特征角度出发的区块链共识机制。

参考文献：

[1] LATVA-AHO M, LEPPANEN K. Key drivers and research challenges for 6G ubiquitous wireless intelligence[M]. Oulu: Oulun Yliopisto, 2019.

[2] DAI Y Y, XU D, MAHARJAN S, et al. Blockchain and deep reinforcement learning empowered intelligent 5G beyond[J]. IEEE Network, 2019, 33(3): 10-17.

[3] 中共中央网络安全和信息化委员会. 把区块链作为核心技术自主创新重要突破口[R]. 2019.
The Central Cyberspace Affairs Commission. Take blockchain as an important breakthrough for independent innovation of core technology[R]. 2019.

[4] JOHN E. FCC’s rosenworcel talks up 6G[S]. 2018.

[5] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for Internet of things: a survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[6] DAI Y Y, XU D, MAHARJAN S, et al. Artificial intelligence empowered edge computing and caching for Internet of vehicles[J]. IEEE Wireless Communications, 2019, 26(3): 12-18.

[7] SAAD W, BENNIS M, CHEN M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems[J]. arXiv: 1902.10265, 2019.

[8] KOTOBI K, BILEN S G. Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access[J]. IEEE Vehicular Technology Magazine, 2018, 13(1): 32-39.

[9] QIU J, GRACE D, DING G, et al. Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: an operator’s perspective[J]. IEEE Internet of Things Journal, 2020, 7(1): 451-466.

[10] BAYHAN S, ZUBOW A, GAWŁOWICZ P, et al. Smart contracts for spectrum sensing as a service[J]. IEEE Transactions on Cognitive Communications and Networking, 2019, 5(3): 648-660.

[11] GAI K K, WU Y L, ZHU L H, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. 2019, 3(6): 4660-4670.

[12] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks IEEE Internet of things journal[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[13] XIONG Z H, ZHANG Y, NIYATO D, et al. When mobile blockchain meets edge computing[J]. IEEE Communications Magazine, 2018, 56(8): 33-39.

[14] CHEN W H, ZHANG Z, HONG Z C, et al. Cooperative and distributed computation offloading for blockchain-empowered industrial Internet of things[J]. IEEE Internet of Things Journal, 2019, 6(5): 8433-8446.

[15] LIU Y M, YU R F, 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.

[16] ZHANG K, ZHU Y X, MAHARJAN S, et al. Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of things[J]. IEEE Network, 2019, 33(5): 12-19.

[17] JIANG L, XIE S L, MAHARJAN S, et al. Joint transaction relaying

and block verification optimization for blockchain empowered D2D communication[J]. IEEE Transactions on Vehicular Technology, 2020, 69(1): 828-841.

[18] LIU M T, YU F R, TENG Y L, et al. Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing[J]. IEEE Transactions on Wireless Communications, 2018, 18(1): 695-708.

[19] DAI Y Y, XU D, MAHARJAN S, et al. Joint computation offloading and user association in multi-task mobile edge computing[J]. IEEE Transactions on Vehicular Technology, 2018, 67(12): 12313-12325.

[20] DAI Y Y, XU D, MAHARJAN S, et al. Joint load balancing and offloading in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4377-4387.

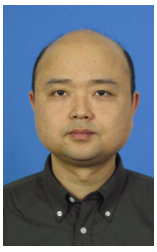
[21] LU Y L, HUANG X H, DAI Y Y, et al. Differentially private asynchronous federated learning for mobile edge computing in urban informatics[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2134-2143.

[22] LU Y L, HUANG X H, DAI Y Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2019.

[23] DAI Y Y, XU D, ZHANG K, et al. Permissioned blockchain and deep reinforcement learning for content caching in vehicular edge computing and networks[C]//2019 11th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2019: 1-6.

[作者简介]

代玥玥，电子科技大学博士，主要研究方向为区块链和移动边缘计算。



张科，博士，电子科技大学讲师，主要研究方向为物联网、车联边缘计算与存储。

张彦，挪威奥斯陆大学教授，IEEE Fellow，挪威工程院院士，全球“高被引科学家”，主要研究方向为物联网、区块链和边缘智能网络。