紫金山实验室
Purple Mountain Laboratories

区块链赋能 6G 移动通信白皮书

体系架构与技术原理

第五届未来网络发展大会组委会

2021 年 6 月

编写说明

编写作者：
王家恒 [1,2]，凌昕彤 [1,2]，乐煜炜 [1,2]，黄永明 [1,2]，尤肖虎 [1,2,*]

参与单位：
[1] 网络通信与安全紫金山实验室，南京 211111 中国
[2] 东南大学 信息科学与工程学院 移动通信国家重点实验室，南京 210096 中国
[*] 通信作者 E-mail：xhyu@seu.edu.cn

编者注：

本文主体内容源于 Jiaheng Wang, Xintong Ling, Yuwei Le, Yongming Huang, Xiaohu You, **Blockchain enabled wireless communications: a new paradigm towards 6G**, *National Science Review*, 2021. nwab069, https://doi.org/10.1093/nsr/nwab069

摘要

当前，5G 网络已开始商业化部署，6G 移动通信研究全面启动，6G 无线网络将容纳海量异构设备和基础设施，全面提升频谱、计算、存储等各类资源的利用效率和安全性。然而，移动通信系统的持续演进面临一系列信任危机与挑战，诸多信任相关问题在当前无线网络设计中被忽视。区块链作为近十年来兴起的一项创新技术，为解决此类问题提供了极具前景的思路与方案。区块链具有分布式、透明性、匿名性、不可篡改性、可追溯性、可扩展性等特点，能够在不同网络实体间建立协作信任，促进无线网络高效资源共享、可信数据交互、安全接入控制、隐私保护、数据追踪、身份认证和信息监管，为 6G 移动通信提供了全新演进方向。本文主要研究区块链赋能 6G 移动通信技术，首先简要介绍了区块链基本原理，并全面调研了目前区块链在无线通信领域应用情况。本文提出了面向 6G 可信移动通信新型网络体系架构——区块链无线接入网（B-RAN），旨在实现区块链与无线通信深度融合，打破“人-机-物-网”之间的信任壁垒，提升无线网络效率与安全性。本文阐述了 B-RAN 框架的关键要素，如共识机制、智能合约、可信接入、数学模型、跨网络协作及共享、数据追踪及审查、人工智能等，并展示了 B-RAN 原型设计与初步实验结果。

目录

一、简介

过去数十年中，随着无线设备数量迅速增加，无线数据流量的指数级增长[1]，第四代（4G）移动通信系统容量逐渐趋于饱和，也加速了第五代（5G）移动通信网络的全球研发[2]。5G 采用了超密集网络（UDN）[3, 4]、大规模多输入多输出（MIMO）[5]、毫米波（mmWave）通信[6, 7]等多项关键技术以实现高达 20Gbps 的数据速率、百万设备每平方千米的连接密度和毫秒级的端到端时延。从 2020 年起，5G 网络业已在全球范围内开始商业化部署以提供增强型移动宽带（eMBB）、大规模机器类通信（mMTC）和超可靠低时延通信（uRLLC）服务，相关技术已经标准化通用化。目前，第六代（6G）无线通信的研究已正式启动，旨在满足 2030 年及未来的无线通信需求。有关 6G 愿景的初步研究已基本达成共识[8-10]，6G 将通过地面、卫星、海上和无人机（UAV）通信提供全球信号覆盖，充分利用 6GHz 以下、毫米波、太赫兹（THz）和光频段的全波段频谱，并支持包括虚拟现实和增强现实（VR 和 AR）、全息通信、超高分辨率多媒体流等在内的海量应用，大数据及人工智能（AI）也将充分助力 6G 性能提升。6G 在关键性能指标上（如频谱效率、连接性、可靠性和时延等方面）将全面超越 5G。

6G 网络将包括大量基础设施和异构设备，提供超高速率、超可靠和超低时延泛在无线连接，进一步促进物联网（IoT）发展及未来的万物互联（IoE）。未来网络规模化、致密化及多样化的持续加剧将给移动通信系统带来诸多重大挑战。网络中频谱、计算、存储、能源、设备、基础设施等资源的高效、安全及可信管理是 6G 网络发展的首要问题，如何促进多维度大规模资源共享是未来网络进一步提高资源利用效率的关键。尽管当前已有诸多资源管理技术方案，但现实应用中由于缺乏激励措施及资本和运营投入，包括移动网络运营商（MNO）、移动虚拟网络运营商（MVNO）、云/边缘服务提供商、资源代理甚至个人用户等在内的资源主体之间通常存在资源共享及数据交互壁垒。此外，6G 网络还面临包括接入控制、数据交互、隐私保护、身份认证等在内的多项安全问题。鉴于 6G 网络的开放性和异构性不断提升，此类问题相较于 5G 将更具挑战性且将进一步加剧网络和资源主体之间的分隔，使得高效、安全及可信的资源共享变得愈加困难。虽然网络资源高效共享技术方面已有大量相关研究，但却极少有实际投入应用的研究成果，最为典型的是认知无线电技术（CR）[11, 12]，它考虑了让次级网络共享未充分利用的主网络频谱，但却忽略了网络及其资源实体之间缺乏互信的核心问题。为应对这些挑战，近年来兴起的区块链技术可为解决当前 5G 和未来 6G 移动通信网络中的信任问题提供极具前景的方案。

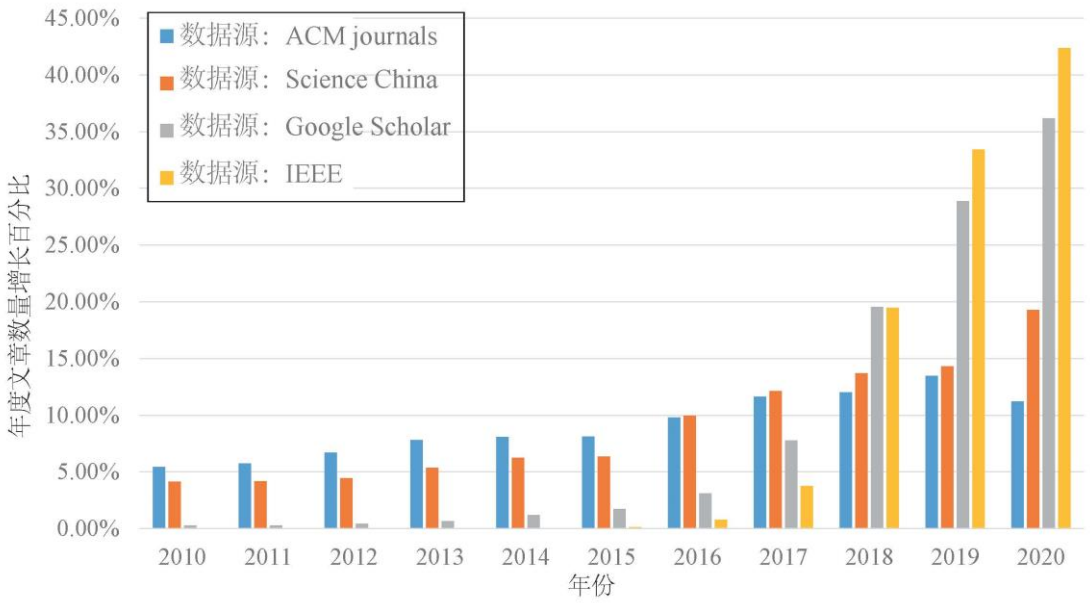

图 1　学术数据库中区块链领域学术论文的年增长率（2010-2020 年）

区块链是一种通用的分布式账本（DLT）技术，近年来作为加密货币的底层技术受到全球研究者和大众的高度关注。2008 年，中本聪（化名）结合多类密码学算法的技术，提出了全球首个强安全、分布式的匿名支付方式，即比特币（Bitcoin）[13]，在短短十年内，比特币作为一种实用的加密货币取得了令人瞩目的成功[14,15]。区块链作为比特币的核心使能技术，在机制上是一个不断增长的数据记录列表，这些数据记录使用加密机制依序连接，构造了一个公开透明、不可篡改的序列化账本。区块链以分布式方式存储、保护和操作数据，同时在匿名保护、数据安全、交易跟踪等方面具有极高可信度，近年来已从以比特币为代表的初代系统发展出诸多增强版本及应用，如支持图灵完备计算及复杂程序执行的以太坊（Ethereum）[16]和超级账本（Hyperledger）[17]。区块链凭借其公开透明、不可篡改、全程留痕、历史可溯、集体维护等特性，能够以低成本、分布式的方式创建安全可信的交互环境，并支持加密货币以外的海量创新应用及服务。如今，区块链的广泛应用已从金融领域扩展到物流、数字政投、税收监管、版权保护、医疗保健等诸多领域。

5G 网络的商业化部署和 6G 移动通信研究的启动，促使更多科研工作者将区块链应用于无线通信[8,10]。在 2018 年移动世界大会（MWC）上，美国联邦通信委员会（FCC）展望了结合区块链技术的 6G 移动通信网络[18]，并强调区块链将在移动通信网络中发挥重要作用。自此，区块链在电信行业蓬勃发展。同年，AT&T 推出了边缘到边缘的区块链解决方案，旨在帮助企业以数字方式跟踪整个供应链的业务流程[19]。自 2019 年以来，德国电信子公司 T-Mobile 一直与标准机构和开源社区合作，开发基于区块链的自主身份认证和接入管理解决方案[20]。在

中国，阿里巴巴于 2015 年启动了蚂蚁链项目，为通信、数据存储和计算提供基础区块链服务[21]。2016 年，腾讯发布了第一个区块链白皮书，旨在建立一个区块链即服务的平台 TBaaS，为用户提供一站式区块链解决方案[22]。最近，中国联通研究院和中兴通讯公司提出了几种移动通信系统与区块链集成的建设性方法。2018 年，中国信息通信技术研究院（CAICT）和可信区块链计划（TBI）共同提出了区块链技术与数据安全白皮书，以期将区块链与未来电信业融合。

近十年来，在区块链学术研究领域，多个学术数据库中区块链的相关研究工作数量呈现迅猛增长态势（如图 1 所示）。目前已有若干研究将区块链应用于无线网络中。在文献[23]中，作者对区块链在 5G 网络及服务中的潜在应用场景进行了广泛讨论；文献[24]调研了区块链在 5G 智慧城市中的信息通信应用。在文献[25]中，作者提出了一种面向未来无线通信的区块链无线接入网架构，并研究了区块链在资源管理和网络接入中的潜在融合应用；文献[26]调研了将区块链和机器学习结合并应用于移动通信网络系统的一些研究成果并讨论了潜在问题及挑战；文献[27]展望了区块链在 6G 中实现资源共享的潜力并介绍了多类应用场景。到目前为止，已有研究大多集中在将区块链应用于一种或几种特定的通信场景，如频谱共享及设备管理，将区块链技术与无线网络进行深度融合的相关研究数量仍较少。同时，区块链在解决无线网络中的安全性、时延、容量、可扩展性、成本和功耗等关键问题的研究也亟待进一步推进，以提升区块链在 5G 及未来 6G 移动通信网络中的适用性。

本文调研了区块链与无线通信融合的最新进展和挑战，并开拓性地提出了面向 6G 移动通信的区块链无线接入网（Blockchain Radio Access Network, B-RAN）框架。本文将首先介绍区块链基本原理、共识协议、智能合约以及潜在安全风险，并从资源共享、数据交互、接入控制、隐私保护、数据追踪、身份认证、信息监管等多个方面调研区块链在无线通信领域的应用情况，总结区块链在移动通信中的主要技术领域及应用场景。本文提出了面向 6G 可信移动通信新型网络体系架构——区块链无线接入网（B-RAN），旨在实现区块链与无线通信深度融合，打破“人-机-物-网”之间的信任壁垒，提升无线网络效率与安全性。B-RAN 构建了一个开放式多边平台（MSP），可支持物联网、移动边缘计算（MEC）、分布式机器学习、车联网和能源互联网等网络中海量多维服务及应用，通过可信聚合、调配与共享多域资源，最大化利用资源池化与网络效应以提升网络整体效能。本文阐述了 B-RAN 框架的关键要素，如共识机制、智能合约、可信接入、数学模型、跨网络协作及共享、数据追踪及审查、人工智能等，并展示了 B-RAN 原型设计与初步实验结果。

全文共分为五个章节。第一章主要介绍了无线通信发展现状与区块链技术应用前景；第二章介绍了区块链基本原理及结构；第三章调研了区块链在移动通信领域的应用情况；第四章提出了面向 6G 移动通信的区块链无线接入网框架及一系列相关技术与应用场景；第五章总结了全文。

二、区块链原理

本章将介绍区块链的基本原理，包括其基本概念与结构、共识协议以及智能合约，并探讨多项区块链应用实践中的潜在风险。

2.1 基本概念

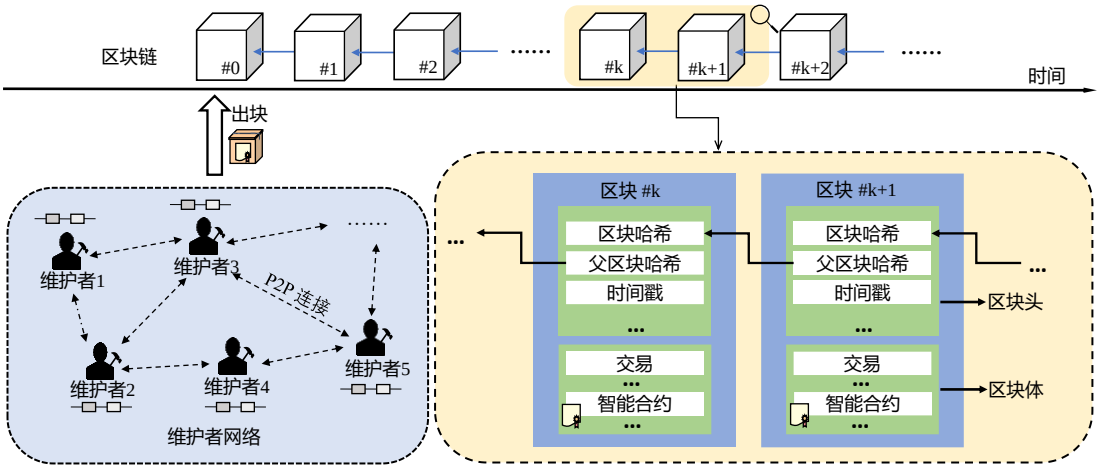

图 2　区块链通用结构

区块链是由对等（P2P）网络中所有活动节点维护的公共数据库，也称为分布式帐本[13]。如图 2 所示，区块链是由多个区块按时间顺序串联起来的账本，其中每一个区块都是一组聚合数据，记录了一段时间内的一系列数字操作（例如交易或智能合约）。每个区块由一个哈希值标识，并通过哈希指针连接起来，即每个区块都包含前一个区块的哈希值（哈希值是由该块的数据生成的数据摘要，该数据摘要会随区块的数据变化而变化）。由于哈希函数的数学特性，篡改区块中的任何信息都会破坏由哈希指针建立的区块间的连接，因此，每个新生成的区块都是对其先前区块有效性的确认。一般来说，篡改区块数据的难度会随其确认区块的数量增加而急剧上升。区块链维护者对需要记录的数字操作进行验证并将其分组打包至区块中，然后通过共识算法将新的区块连接至区块链尾部，以保持区块链的一致性和不可篡改性，这通常称为出块。

根据区块链数据管理策略的不同，可以从两个角度将区块链进行分类：公有区块链和私有区块链，以及免许可区块链和许可式区块链[14]。公有区块链和私有区块链的主要区别在于身份验证，即限定接入区块链的对象。一般来说，在公有链中，任何人都可以加入区块链，而在私有链中，只有区块链所有者能控制对区块链的访问。另一方面，免许可区块链和许可式区块链的主要区别在于授权，即限定区块链的操作权。通常，在免许可的区块链中，任何人都可以更新区块链中的数据，而在许可式区块链中，只有授权实体才被允许参与区块链操作。当前，最适合孵化落地应用的联盟链就是许可式和半私有的区块链。与通常由单个所有

者控制的私有链相比，联盟链由来自多个组织或个人的受控节点共同维护，它可以以部分分布式的方式在保证全局安全的前提下实现自主和可控，对于协同多边事务、建立多方信任有重大的参考价值。

2.2 共识机制

共识机制是用于在多个区块链维护者间对区块链状态达成统一共识的一类协议，是区块链的核心组成部分之一[28]。本节调研了现有的各种共识机制，并将它们分为两类，如表 1 所示。

表 1 共识机制总结

基于证明的共识机制	proof of work 类	proof of work[13] cuckoo cycle[29] useful proof of work[30] proof of learning [31]
	proof of stake 类	proof of stake[32] delegated proof of stake[34] ouroboros[35] proof of luck[33]
	其它类	proof of device[25] proof of human [36] proof of negotiation[37] bitcoin-NG[38]
基于投票的共识机制	crash fault tolerance 类	paxos[39] raft[40]
	byzantine fault tolerance 类	practical byzantine fault tolerance[41] proof of authority [42] redundant byzantine fault tolerance[45] tendermint[47]

2.2.1 基于证明的共识机制

基于证明的共识机制要求区块链维护者证明其相比于其他维护者更有资格产生新区块。工作量证明（PoW）是目前最著名的区块链共识机制[43]，其设计初衷是应对垃圾邮件泛滥问题，它要求所有邮件发送者必须完成一些计算工作才能

成功发送电子邮件，比特币[13]的广泛应用使 PoW 在学术及工业界广为人知。基于 PoW 的共识机制要求区块链维护者们进行大量运算来竞争产生新区块的资格。由于 PoW 资源消耗巨大，许多基于 PoW 共识机制的研究[29-31]尝试将 PoW 中的哈希运算替换成具备实际价值的任务，从而避免算力资源浪费。此外，也有研究者设计了另一类基于证明的共识机制——权益证明（PoS）[32]，该机制以区块链维护者的代币数量[33]锚定区块链维护者产生区块的能力，代币数量越多，产生新区块的难度越低。在 PoS 的基础上，代理权益证明（DPoS）[34]将 PoS 中代币持有权益转化为投票选举权，由持币人选出多个代理节点代为管理区块链网络，而无须消耗大量算力求解数学难题，进一步降低了区块链共识能耗。

上述共识机制都可以归纳为证明类（PoX）共识[14]，这类共识的特点是要求区块链网络中的所有维护者都以可验证的方式来证明自身对某些可量化资源（不仅是哈希运算）的持有权。在 PoX 类共识机制中，PoW 的替代机制层出不穷，它们在原有 PoW 共识上将经济成本[25]，环境友好[36]，公平性[37]或者性能[38]作为考虑因素。对于无线通信这类应用环境，需要统筹考虑产生区块所要消耗的资源与无线设备功率限制来选择或设计合适的共识机制。更多相关的讨论，请参见本文 4.2 共识机制部分。

2.2.2 基于投票的共识机制

基于投票的共识机制广泛应用于联盟链中，此类共识根据多数维护者的决策来生成区块[28]。与 PoX 类共识相比，基于投票的共识机制要求区块链维护者之间具有完全连接的网络拓扑结构，以便于区块链维护者验证区块并最终达成共识。

在基于投票的共识机制中，崩溃容错（CFT）类共识机制可在某些维护者因软硬件故障、网络连接断开而无法响应消息等情况下最终达成共识。常用的 Paxos 共识[39]和 Raft 共识[40]就是 CFT 类共识的典例。此外，对于区块链中某些维护者出现行为异常的情况，文献[44]的作者指出，只有当区块链维护者总数严格大于行为异常维护者数的三倍时，所有区块链维护者才能达成共识并做出最终决定。由于存在行为异常维护者（拜占庭节点）而无法最终达成共识的情况被称为拜占庭将军问题，应对此类问题的共识机制则称为拜占庭容错（BFT）机制。著名的实用拜占庭容错机制（PBFT）由 BFT 改进而来[41]，该机制依赖于一种“领导-服从”的对等层次结构，并利用三阶段交互使所有节点达成最终共识。PBFT 具有低时延、高吞吐和低能耗等优势，但也因较高的通信复杂度导致其可扩展性较差。冗余拜占庭容错共识（RBFT）[45]是 PBFT 共识的改进型，它利用多线程模型并发执行多个冗余 PBFT 共识实例，并在 PBFT 共识中额外增加了传播阶段以确保非拜占庭节点工作稳定性与共识安全性。著名开源区块链平台以太坊所采用的共

识机制之一，权威证明（PoA）[42]，也是 BFT 的一种基于网络身份声誉的改进共识。与 PBFT 相比，PoA 显著减少了通信开销并提高了共识达成效率[45]。Cosmos[47]区块链中所采用的 tendermint 共识是 PBFT 的一类改进型，支持在全网超过 1/3 节点为拜占庭节点时有效阻止区块提交，可显著增强区块链维护安全性。

2.3 智能合约

智能合约作为区块链中的程序脚本，通常负责区块链中数字操作的执行，并实现多步骤流程的自动化。以太坊[48]将智能合约描述为一个加密的盒子，只有在满足某些条件时才能解锁。一旦激活了，合约条款便会在网络参与者之间自动执行，无需依赖第三方或中心节点。相较于比特币的未花费交易输出（UTXO）[13]，智能合约的灵活性和多样性使区块链不再仅仅局限于一个简单的加密货币交易系统，而是让区块链形成一个分布式虚拟机。数字资产（例如存储、传输和计算）和操作（例如交易、收费和利息）都可以通过智能合约中的数字签名和密钥对轻松地进行授权和认证。随着以太坊的逐渐普及，智能合约也已成为各种新兴区块链应用必不可少的组成部分，并且智能合约的功能也得到了极大扩展[49]。

虽然智能合约的应用带来了诸多好处，但仍存在一些安全性和实现问题。文献[50]研究了实现智能合约的几类风险，提出了安全的智能合约必备的三个关键属性：确定性、隔离性和可终止性。文献[51]分析了针对智能合约的七种攻击，并推荐了几种保障智能合约安全的解决方案。验证智能合约的标准对于保护智能合约中的数字资产和操作至关重要，但是当前仍然缺少成熟的验证智能合约的标准[52]。文献[53]提出了几种嵌入式分析方法和基准，以识别智能合约中的漏洞（例如，重入和代码克隆）。在智能合约的实现方面，文献[54]的作者针对研究人员使用的面向特定领域的智能合约编程语言进行了全面评估，文献[55]总结了一些衡量智能合约属性（如规模和复杂性）的指标。

2.4 潜在风险

与传统的分布式系统相同，区块链也会存在某些分布式安全问题。本节总结了区块链中的一些潜在风险，并简要讨论这些风险的特征和对策。

2.4.1 替代历史攻击

攻击者可以通过私下产生区块形成一条替代主链的欺诈链来发动替代历史攻击，从而实现双花攻击[14]。如果攻击者能够创建比主链更长的欺诈链，则其可以用欺诈链替代已被区块链维护者而接受的主链。在 PoW 中，如果攻击者拥有整个区块链网络 50%以上的算力资源，那么他就可以更改区块链中已确认的区

块，这被称为 51%攻击[14]或者 Goldfinger 攻击[56]。这种攻击中，攻击者的欺诈行为会促使区块链网络中诚实的区块链维护者离开网络，从而扩大攻击者自身的算力优势。与 51%攻击相似，PoS 中的长程攻击[57]可以改变区块链的历史记录，导致区块链数据不一致。长程攻击的发动者通过收集过去拥有多数代币的老帐户的私钥，可以构建一个分叉链来覆盖当前的主链。为了抵御这种攻击，文献[32]的作者建议使用检查点（指某类特定的区块，这类区块上链时，区块链被视为“最终化”且不可再被篡改）来限制长程攻击。

2.4.2 自私出块攻击

自私出块攻击的关键是通过让诚实的区块链维护者在主链上浪费算力来提高攻击者的攻击成功概率[58]。攻击者计算出新的有效区块但不立即发布，而是继续计算下一个区块，直到其他区块链维护者也找到主链中当前区块高度下的另一个有效区块，攻击者就会将之前私下产生的所有有效区块发布到区块链网络中。（当然，攻击者还承担着公共链可能超越其私有链的巨大风险。）Bahack[59]分析了一系列自私出块策略，并提出了缓解自私出块危害的解决方案。在文献[60]中，作者使用马尔可夫链模型描述了公有链和私有链中的自私出块的状态转变，并分析了存在多个自私矿池时的自私出块的获利能力。

2.4.3 密码分析攻击

区块链中的密码分析攻击，如密钥攻击和量子攻击，旨在破解密码算法获得密钥。区块链与密码算法紧密结合，例如 Hyperledger Fabric 依靠椭圆曲线数字签名算法（ECDSA）生成私钥，而椭圆曲线数字签名算法时常会遭受密钥攻击[61]。私钥泄漏和密钥生成的弱随机性是密钥攻击发生的常见原因。在文献[62, 63]中，作者指出私钥应通过密钥生成的强随机性来防止密钥攻击。另一方面，量子计算的发展对传统的密码算法以及区块链产生了巨大冲击。文献[64]研究了区块链中潜在的量子攻击，并提出了一个反量子攻击的交易认证方案。

2.4.4 无利害攻击

使用低能耗共识协议的区块链容易受到无利害攻击，其本质原因是攻击者可以以极低的作恶成本换取可观的经济收益。这类攻击中，通过制造多个分叉链，攻击者以一种无风险方式对区块链发起攻击。Buterin[48]针对该攻击提出了一种 Slasher 算法，该算法要求区块产生者缴纳一定押金并存放一定时间，通过提高作恶成本防范无利害攻击。PoS 共识中所采用的币龄机制也易遭受无利害攻击，攻击者可以通过囤积硬币来积累币龄，从而增加他在区块链中的影响力。Li 等人[65]建议为币龄设置上限来抵御这种攻击。

2.4.5 传统网络攻击

区块链网络中仍然存在传统的网络攻击，例如分布式拒绝服务（DDoS）攻击，重放攻击，中间人攻击，女巫攻击和日蚀攻击。区块链中的 DDoS 攻击会导致多个区块链节点被无效请求淹没，从而使得这些节点无法正常工作。重放攻击会拦截通信方的数据包并将其不经修改地转发到目的地，而中间人攻击则可以拦截这些数据包并向数据包添加信息。在文献[66]中，作者展示了如何利用中间人攻击在以太坊私有链中进行双花攻击。此外，某些恶意实体可能会伪造多个身份来发起女巫攻击[67]，该攻击会将大量错误信息注入到区块链网络。与针对整个区块链网络的女巫攻击不同，日蚀攻击则只会欺骗单个网络目标，并制造出扭曲的区块链视图来控制被攻击节点。

三、区块链赋能移动通信

区块链作为一项开创性技术，能够为无线网络中诸多信任危机和安全挑战提供解决方案。区块链赋能移动通信技术领域与应用场景如图 3 所示。区块链有望进一步促进通信网络中的资源共享、可信数据交互、安全接入控制与隐私保护，并为 5G 及 6G 移动通信提供数据溯源、身份认证和信息监管等功能。本节将全面调研区块链技术在无线网络中的应用情况。

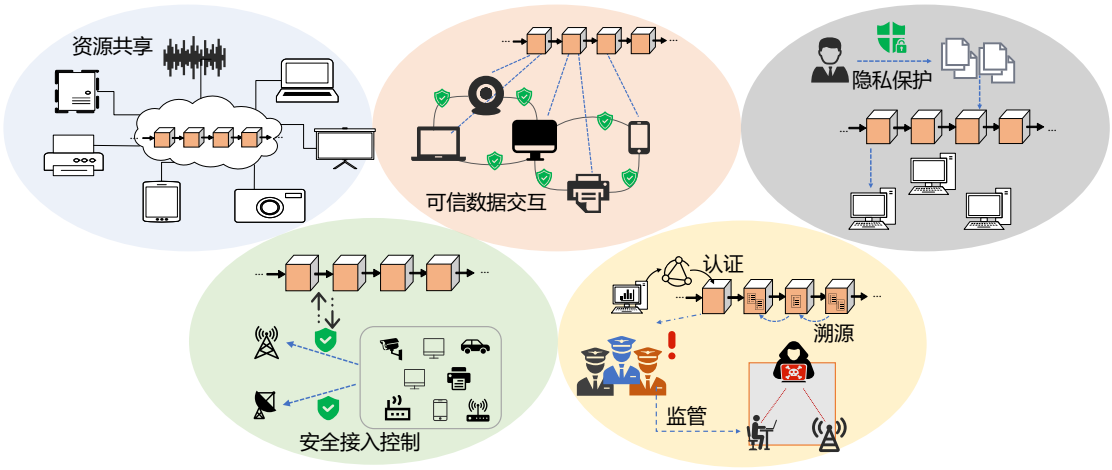

图 3 区块链赋能移动通信技术领域与应用场景

3.1 资源共享

频谱和基础设施等无线网络资源难以匹配各种移动业务爆炸式增长的需求，这对网络资源的共享机制提出了更高要求[68]。然而，无线资源拥有者出于对激励机制、成本和安全性等因素的顾虑，常常不愿意共享彼此之间的资源，因此网络实体之间的协调与合作变得异常困难。另一方面，随着云计算、移动边缘计算（MEC）、软件定义网络（SDN）和网络功能虚拟化（NFV）等新应用加入到 5G 中，5G 所汇聚的计算资源、存储资源和网络切片资源等网络资源的类型和数量也在增加，这使得资源管理与共享变得异常复杂。区块链因其固有特性可以有效地缓解网络实体之间的信任和安全问题，促进多方协作，从而实现更高效的资源共享。

3.1.1 频谱共享

频谱是无线网络中最重要的资源之一，目前已有许多研究将区块链应用于频谱共享。如在文献[69]中，作者探讨了结合区块链进行频谱管理的应用方案，并总结了不同频谱共享机制的优缺点。文献[70]提出了基于联盟链的运营商之间的频谱共享系统，该系统可以提供可靠的隐私与安全保障。文献[71]设计了一种区

块链验证协议，该协议可以在移动认知无线电网络中，以不连续频谱感知的方式实现安全的频谱共享。文献[72]提出了区块链赋能的频谱共享架构，可以有效地激励主用户共享其闲置频谱，实现低复杂度、高效的频谱分配。文献[73]利用区块链构建了一个半分布式的无线网络非授权频谱管理架构，解决了频谱竞争问题。文献[74]引入了一种智能网络架构，通过智能合约处理运营商和用户之间的非授权频谱共享。此外，文献[75]引入了一种新型的区块链结构与共识算法以自主管理未授权频谱，减少了网络部署和运营的成本。

3.1.2 计算与存储

云计算与边缘计算的广泛应用使人们意识到了计算和存储资源的价值，相关研究也试图通过引入区块链来更为有效地管理这类资源[76, 77]。文献[78]提出了基于区块链的计算卸载架构来促进实体之间的计算资源共享。Liu 等人[52]设计的基于区块链的 MEC 架构使用三阶段的 Stackelberg 博弈来对不同参与者之间的服务出价、协商和交易进行建模。文献[79]的作者设计了两种双重拍卖机制来激励区块链网络中的参与者共享其计算资源。文献[80]提出了一种用于防范车辆边缘计算（VEC）资源交易中出现恶意行为的联盟链。Sun 等人[81]借助区块链设计的一种基于属性的加密方案可以有效用于安全存储与共享病历之类的应用场景。文献[82]提出了一种基于区块链的可仲裁远程数据审查方案，以提供可靠的网络存储服务。

3.1.3 基础设施和设备

区块链技术提供了一种安全有效地管理 5G 和 IoT 中的异构设备与基础设施的方法。文献[83]研究了利用区块链实现 5G 小型蜂窝网络中独立、自治、可信的基础设施共享的方案。文献[84]考虑将区块链作为分布式网络的基础设施以保障未来电网的安全，并基于此提出了优化能源基础设施分配和提高能源利用效率的原型。文献[85]提出使用区块链来控制和配置物联网设备，并探索了互连设备的身份管理问题。Novo 等人[86]提出了多种基于区块链的解决方案来缓解受限设备管理的相关问题。在文献[87]中，作者介绍了一种基于私有链的 IoT 体系架构，用于对 IoT 设备进行有效的监管。文献[88]构建了用于组织和共享 IoT 数据和设备的 IoT 区块链架构。

3.1.4 网络切片

5G 系统中软件定义网络和网络功能虚拟化的发展让网络切片技术逐渐受到学术界和工业界的关注。作为各种物理网络资源的逻辑组合，网络切片天生具有可被共享的属性[89]。在文献[90]中，作者就切片租赁问题提出了区块链网络切片

代理商的概念，随后文献[91]分析了在工业自动化场景中区块链网络切片代理商的可行性。文献[92]提出了一种名为 NSBchain 的新型网络切片代理解决方案，使得基础设施提供商可以通过智能合约将网络资源分配给中间代理。同样，文献[93]设计了一种基于信令的区块链使能的网络切片分布式架构，以促进不同服务提供商之间的动态资源租赁，支持高性能的端到端服务。

3.2 可信数据交互

无线业务种类和网络连接密度的日益增加，某些特定服务对各方数据交互和协作提出了新需求[94]。但是，移动网络中的数据所有者之间缺乏互信关系，这导致了数据的真实性、可靠性以及交互过程的安全性难以保障[95]。目前，已有不少研究致力于使用区块链在各种设备之间建立相互信任，为安全的数据交互创建可信通道[95,96]。其中，使用区块链技术支持无线网络中可信数据交互的研究工作可划分为两个方向：一是确保每个网络实体身份的可信度，二是提高所传输数据的真实性。

3.2.1 身份可信度

为了确定网络实体身份的可信度，区块链参与者可以在每个实体进入网络之前分析其历史行为等指标，获取其可信度值，然后以此为依据向该实体授予相应权限。文献[97]提出了一种基于区块链的信任管理机制，该机制规定只有具有特定可信度的节点才能与其他节点进行交互，而恶意节点将被检测并驱逐。文献[98]针对基于区块链的车联网设计了一种新型共识机制，该机制基于车辆的可信度对数据交互进行验证。文献[95]通过将分布式身份与区块链的底层技术结合，增强了对个人隐私和数字身份的控制。文献[99]提出了一种在车辆自组织网络中使用区块链和认证中心的智能车辆可信系统模型。

3.2.2 数据真实性

为保证无线网络中数据的真实性和准确性，不少研究考虑将群体智能感知和共识机制相结合。文献[100]利用双向认证协议和用户自定义敏感数据加密技术，构建了一种基于区块链的边缘计算可信数据管理方案。文献[101]提出了一种基于区块链的车载网络分布式信任管理系统，通过贝叶斯推理模型对交通信息的可信度进行评估。类似地，文献[102]针对车载网络提出了一种名为事件证明的共识机制，通过过往车辆来验证路侧单元所收集的交通数据的真实性。

3.3 安全接入控制

无线网络的不断致密化和海量设备的持续异构化给移动通信系统的接入控制带来了诸多安全风险。具体安全风险主要分为三类：恶意设备入侵造成的设备安全风险，单点故障导致的系统安全风险以及数据泄漏导致的数据安全风险。区块链具有防篡改、分布式和细粒度审核等优良特性，有望为无线网络中的诸多安全风险提供可行的解决方案。

3.3.1 设备接入

移动通信网络为海量异构设备提供服务，且必须阻止恶意设备损害系统安全。目前，一些研究已经考虑使用区块链来抵御恶意设备的入侵[103-105]。在文献[103]中，作者采用了定制的智能合约来抵御DDoS攻击和恶意设备攻击。文献[104]设计了一种名为ControlChain的区块链接入控制体系结构，提供了一种安全的方法为网络实体创建关系并为其分配属性。文献[105]提出了一种区块链接入控制框架，该框架包含三种智能合约，分别用于安全添加、更新和删除网络实体身份。

3.3.2 系统接入

除需阻止恶意设备入侵之外，传统的接入控制机制大多基于集中化架构，因此也存在单点故障的隐患。区块链具有分布式与协作维护等特点，对于防范单点故障有着天然的优势。目前，已有研究尝试将区块链技术与接入机制相结合来应对单点故障[85, 86, 106, 107]。文献[106]提出了一种面向IoT的基于属性的接入控制方案，该方案利用区块链分布式地记录设备属性，以避免单点故障和数据篡改。文献[107]设计了一种基于身份的令牌管理策略，通过使用智能合约来完成接入授权的注册、分发与撤销。

3.3.3 数据接入

用户对移动网络中数据安全性的关注度极高，而在传统的集中式接入控制机制中，数据的恶意操纵与泄漏时有发生。许多研究工作已经尝试将区块链技术引入数据接入过程，以解决数据安全问题[108-111]。文献[108]的作者通过在UTXO模型中设计公平接入机制实现了基于区块链的安全接入，并保障了IoT数据的安全性和匿名性。此外，文献[109]的作者提出了一种名为CapChain的接入方案，该方案利用区块链的匿名性隐藏数据共享和委托中的关键信息，从而保障数据安全。在文献[110]中，作者设计了一种新型的区块链赋能网关，该网关作为用户和IoT设备之间的中介，增强了IoT接入中的数据安全性。

3.4 隐私保护

当不同实体通过无线链路彼此通信时，无线传输的开放性和无线设备的移动性可能会带来许多隐私问题。例如，恶意实体可能会拦截、转发甚至篡改包含实体身份隐私或机密数据的传输信息。因此，移动通信网络中的隐私保护越来越受到重视。区块链通过内生的非对称加密等密码学机制，有望同时为实体身份隐私与机密数据提供保护。

3.4.1 身份隐私

假名机制在区块链中十分常见，它通过隐藏用户的身份来保护身份隐私。文献[96, 112]的作者们提供一种使用区块链为节点提供隐私保护的方案，其中每个节点都拥有唯一的公钥，节点可通过从区块链中检索公钥来与其他节点通信。文献[113]利用私有区块链中的假名来隐藏用户的身份，其中每个用户可以使用与这些假名相关的数据创建多个假名。文献[114]设计了车载通信系统中的动态密钥管理体系，在该体系中，用户必须定期联系区块链维护者来更改他们的假名集，以及与此假名相关的所有密码信息。在文献[115]中，证书颁发机构的所有活动都会被公开透明地记录在区块链中，防止其泄露车辆的敏感身份信息，从而车辆可以将公共密钥作为通信过程的认证假名，而不会在通信中泄露自身隐私。此外，文献[116]提出的基于区块链的智能电网，通过使用群签名技术来保护用户的身份隐私。

3.4.2 数据隐私

除身份隐私外，也有一些研究关注无线网络中用户机密数据的隐私保护。文献[112, 117]使用非对称加密算法对记录在区块链交易中的用户数据进行加密，从而为机密数据提供隐私保护。文献[118]将工业物联网中数据提供者的原始数据保存于本地，仅通过许可链实现相关数据的检索与管理，以此来保障数据的隐私。文献[113]的作者提出了一种根据平均用电量选择区块链维护节点的方案，该方案可以在不泄露个人隐私数据前提下进行电网通信。不同于上述机制，文献[110]的作者提出了一种区块链赋能的物联网网关，以增强数据隐私和安全性。用户可以通过该网关管理他们的隐私偏好，并决定个人数据是否可以转发到物联网设备中。

3.5 溯源、认证与监管

随着移动网络规模的不断扩张和业务的多样化，如何满足网络使用者对数据

溯源、设备认证和信息监管的需求，并杜绝关键网络信息被非法访问、随意操纵与虚假传播变得十分关键。目前使用受信第三方服务器提供数据存储、设备认证和追踪服务的方法普遍存在隐私和安全问题。区块链因其具有不可篡改、公开透明等特点，可以为这些问题的解决提供突破性方案。

3.5.1 溯源

通过共识机制和智能合约的自动化执行，区块链可为网络实体溯源提供全方位的可信记录和安全保障，从而确保区块链中数据和交易的完整性与安全性。在文献[119, 120]中，作者们利用区块链来增强IoT设备可追溯性。而文献[121]的作者则是采用混合区块链结构的资产跟踪方法实现溯源功能。文献[122]设计了一种新的令牌，以增强区块链数据的可追溯性。文献[123]的作者使用智能合约来跟踪与管理制造业中的工业交易。在文献[124]中，作者提出了一种基于区块链秘密共享和动态代理的身份认证方案，并将其应用于跟踪协同认证过程。

3.5.2 认证

通过区块链技术，移动服务提供商可以透明、可靠地认证设备和保存数据。文献[125]提出了一种基于区块链的认证服务，该服务使用智能合约来保存生物医学数据库的查询操作和查询结果。文献[126]构建了基于许可区块链的公钥基础设施证书系统，并解决了多证书颁发机构中的互信问题。此外，在文献[127, 128]中，作者都提出了使用区块链来增强公钥基础设施系统中设备证书安全性的方案。文献[129]提出了一种基于区块链的数字证书系统，赋予了数字证书防伪和可验证的功能。文献[130]设计了一个区块链驱动的认证系统，实现了高效、安全的证书查询和验证。

3.5.3 监管

区块链具有保护监管数据和提高监管效率的能力，天然迎合了信息监管的需要。在文献[131]中，作者提出了一种基于阈值环签名算法的区块链电子政务监管模型。文献[132]提出了一种基于双层区块链的疫苗生产监管机制。文献[133]使用区块链为政府招标中的工作流程监管创建了边缘计算基础架构，并保证了政府计划和政策的安全性。此外，在文献[134]中，作者设计了一个基于区块链的IoT自主交易结算系统，允许所有网络参与者共同监督结算过程。

四、6G 区块链无线接入网（B-RAN）

本节提出了面向 6G 可信移动通信的区块链无线接入网（B-RAN）架构，并对 B-RAN 中的共识机制、智能合约、可信接入、数学建模、跨网络协作及共享、数据追踪及审查，以及智能组网等多项关键要素进行了深入讨论，最后展示了 B-RAN 的原型设计与初步实验结果。

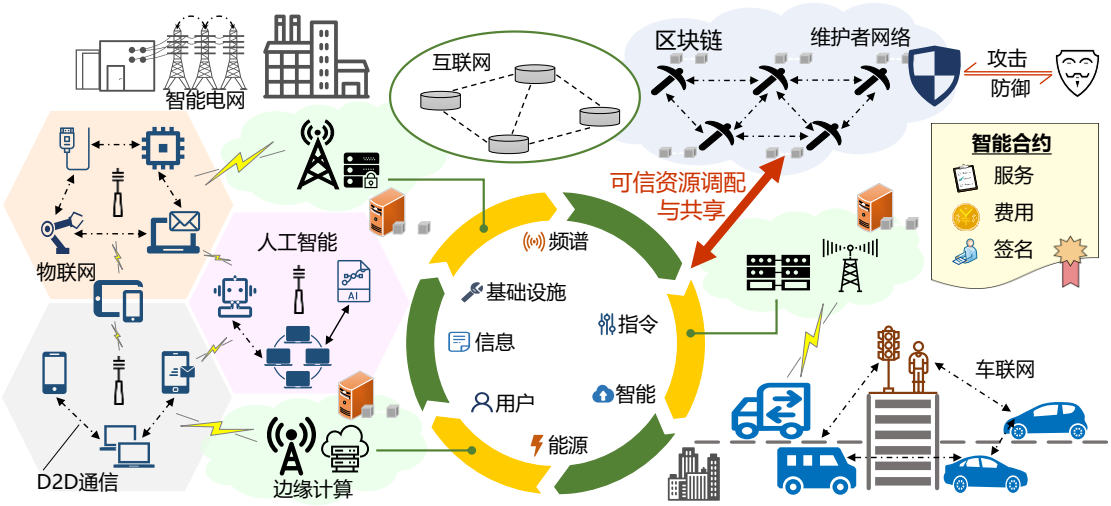

图 4　区块链无线接入网(B-RAN)概览图

4.1 B-RAN 简介

近十年来，区块链技术发展迅猛，许多研究工作已经从区块链底层技术延伸到在无线网络中的前沿应用。然而，现有的研究工作大多将区块链应用到独立且具体的小规模场景，而未考虑将区块链与无线通信深度融合。并且，诸多研究将区块链简单地套用于无线网络中实质上无法完全解决其中的信任问题，应当在充分考量网络内及网络间复杂不信任特性的基础上，使用区块链构建未来无线网络的协作信任。现有的研究并没有对无线环境中区块链的安全性、时延、可扩展性、成本、功耗等关键问题展开研究，缺乏描述基于区块链的无线网络的数学模型和相应的参考实验结果。因此，探究并解决前述问题是将区块链深入融合至未来 6G 移动通信架构中的关键。

B-RAN 的出现为大规模、异构、可信的无线网络提供了一种新范式[25]。如图 4 所示，B-RAN 为海量应用提供了一个开放与统一的架构，实现了多网络资源池化与共享，并为未来 6G 网络提供了一个极具前景的解决方案。B-RAN 在无任何第三方或中心代理的情况下将互不信任的网络实体连接起来，构建了多个网络中及网络间的协作信任，通过可信交互来管理网络接入、身份验证、授权和记账等操作。B-RAN 建立了连接多方网络及实体的多边平台（MSP），并以灵活、

安全与可信协作的方式促进了资源及数据共享，不仅可以动态共享计算、存储及通信能力，还可在网络间共享与散播智能模型及操作（联邦学习可进一步优化 B-RAN 中的资源及网络服务利用率）。此外，B-RAN 作为一个区块链即服务（BaaS）平台，具有诸多增强安全属性，有望为未来网络用户提供数据交换、隐私保护、跟踪及监管等多项关键功能。

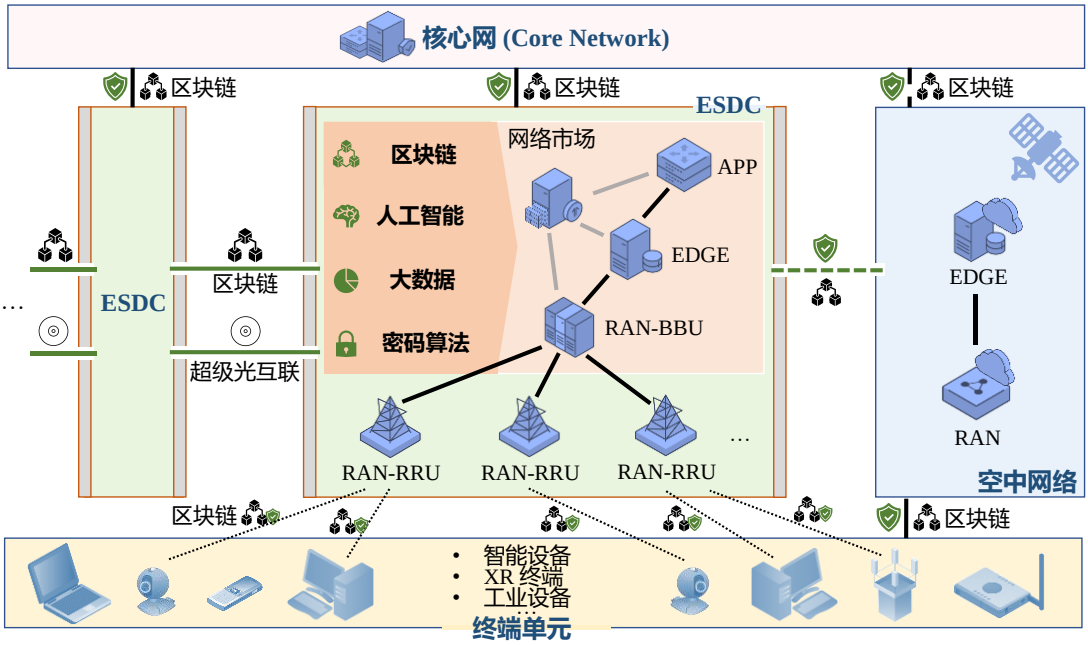

图 5　基于区块链的 6G 体系架构设想示意图

图 5 展示了基于区块链的 6G 体系架构设想示意图。边缘超级数据中心（ESDC）由功能强大的基带单元（BBU）和边缘服务器组成。边缘超级数据中心采用区块链、人工智能和大数据等技术构建，与诸多远程无线单元（RRU）共同组成了超级基站，也即 5G 移动通信中 eNode B 的增强版本。超级基站不仅支持无线服务，还可支持各类本地应用及网络市场。在边缘超级数据中心内，区块链以其密码学特性保证了内生安全，在人工智能和大数据技术的辅助下，增强了移动终端安全接入控制、跟踪及监管等众多关键功能。不同边缘超级数据中心之间可通过超级光缆互连以进行高速数据交换，并通过区块链保障了可信数据交互及业务协作。区块链还可通过远程无线单元将海量的各类终端单元、边缘节点与核心网络进行可信互联，通过链上/链下智能合约实现分布式可信网络管理。

此外，在物联网场景中，即便缺乏互信基础，B-RAN 也可借助于区块链为物联网设备和接入点（AP）建立协作信任，这也将为未来多运营商网络中的物联网/万物互联网提供新的解决思路[135]。B-RAN 所建立的协作信任可有效规避互不信任设备间可能作出的自私行为，并促进各物联网网络之间的合作。B-RAN 将多个独立网络重组成基于区块链的联合多运营商网络，可有效整合、调配和共享

频谱、接入点、物联网设备和用户数据等多维度跨网络资源。因此，在 B-RAN 中，物联网设备不再局限于其订阅的服务提供商服务，而可以通过 B-RAN 提供的有效激励机制及协作机制获取海量跨网络资源及服务。

B-RAN 的另一项重要应用是区块链赋能的移动边缘计算，它可以实现开放分布式网络的多方资源调度，同时为用户提供隐私保护并保障数据安全。B-RAN 可建立网络用户和来自不同运营商的移动边缘计算服务器之间不依赖中间代理的可信直连通信，同时还可充分利用移动边缘计算参与者的存储及计算资源，提升网络管理资源利用率并降低冗余，实现资源共享和调度的高效配置。

4.2 共识机制

虽然 PoW 具有较强的鲁棒性，但该类共识机制会消耗大量的资源。而移动设备资源往往有限，达成 PoW 共识或其多种变体类共识所带来的显著时延无法满足时延敏感型无线服务的需求，因此资源消耗大和时延性能差的传统共识机制并不适用于移动通信环境。

除了考虑使用权益证明（PoS）和行动证明（PoA）等低成本共识协议外，B-RAN 还设计了基于身份的共识机制 PoD[25]。B-RAN 由海量的设备构成，因此 PoD 使用了用于区分不同设备的唯一硬件标识符（ID）来作为共识核心。根据设备的唯一硬件标识符，每个设备只需在每个时隙中执行一次哈希运算，如果获得的运算结果小于目标阈值，那么该设备获得当前时隙的传输权利。PoD 通过限制哈希运算的次数来减少资源消耗，但在这种情况下，硬件标识符的唯一性对于 PoD 的安全性和有效性至关重要。为保证标识符的安全性与有效性，应考虑使用位置信息、射频指纹（RF）和硬件安全模块（HSM）等更为安全的特性作为标识符。例如，射频指纹识别是根据发射器硬件的制造缺陷来生成识别设备的唯一指纹。此外，可以将硬件安全模块嵌入 B-RAN 的设备中，以防止硬件标识符被伪造和篡改。由于设备的硬件标识符和其他必要的信息存储在设备的硬件安全模块中，因此用户只能验证而无法随意篡改其中的信息数据。攻击者也无法以物理方式或数字方式篡改硬件安全模块所存储的硬件标识符等数据。一旦硬件安全模块检测到入侵行为，它将抹除设备中的关键信息，危急情况下硬件安全模块甚至会触发设备自毁。

此外，文献[134]设计了一种新颖的卫星辅助区块链共识协议。它充分利用了卫星广域覆盖和泛在互联的优势来设计共识协议，并构建了具有高可扩展性的空地区块链结构。在这一共识协议的每一轮中，卫星负责定期生成 oracle，oracle 是用于选定本轮中唯一获胜的区块链维护者的随机数，该区块链维护者有权生成当前轮次唯一有效的新区块，并利用区块链网络将新区块广播给其他区块链维护者。

随后，卫星将 oracle 多播到地面的区块链网络。这种选择获胜者的方法不需要大量的哈希运算，从而极大地减少了共识过程中的资源消耗。文献[134]中的仿真结果表明，该文献所提出的共识协议在保持与 PoW 相同的安全性的同时，可以获得比 PoW 更高的吞吐量。此外，由于地面 P2P 网络跳数较多，其时延通常是长尾分布的[135]，而卫星通信的传播时延几乎是固定的，更具可控性[133, 134]。因此，对于地面 6G 网络中的 B-RAN，此共识协议也可以作为一种重要的参考选择。

在共识机制中，节点还可以基于有实际意义的任务设计共识算法，而不是执行无意义的哈希运算。例如，B-RAN 中的大规模资源分配和调度就是一种合适的共识任务。借鉴学习证明（PoL）原理[30]，B-RAN 的参与者可以部署多样化的智能算法，为机器学习竞赛中的这些任务提供解决方案，提供最佳解决策略的维护者将被选为下一轮出块权利的获胜者。在 B-RAN 中，这种机器学习竞争可以用来为多种复杂任务提供解决方案及提供优化思路。

4.3 智能合约

B-RAN 的底层区块链技术和机制保证了资源共享、数据交互和用户接入的系统安全和效率。智能合约中的可验证软件代码确保了这些服务在 B-RAN 网络中的一致性和自动执行，并防止后门病毒植入到 B-RAN 中。接下来，本节将介绍两种基于智能合约的机制来增强 B-RAN 的安全性及效率。

快速智能合约部署（FSCD）是 B-RAN 中为加速执行和保护服务而提出的一种先进的机制[138]。通过在智能合约中实现填充模板的概念，FSCD 的根合约详细定义了服务条款，该条款随后会自动应用于所有服务。快速智能合约部署可以有效地验证和跟踪服务请求，可避免伪造与恶意请求被区块链接受，从而降低了服务请求过程中的潜在风险。

此外，可以在 B-RAN 中使用哈希时间锁定合约（HTLC）机制[139]，以加强服务提供商和用户之间资源交换的安全性和公正性。哈希时间锁定合约通过在两个交易方之间形成“约束”，允许用户以“链外”支付渠道进行无信任环境支付。在这种“约束”的作用下，违约方在基于哈希时间锁定合约的资源交换中注定无法获利。通过这种方式，哈希时间锁定合约有效地降低了服务提供商和用户之间的风险（如身份欺骗风险），并增强了资源交易的安全性。

尽管 B-RAN 证明了其安全性和高效性，但仍有一些问题尚未解决。B-RAN 是一种协调多个网络及其子网的管理服务提供商，但如何安全隔离各网络之间的私有信息仍有待研究。同样，在 PoD 中很难避免预计算攻击，攻击者可以通过未来的时间戳预先计算出有效的区块。此外，如何设计出稳健高效的智能合约来自动惩罚违规行为也是未来 B-RAN 持续发展所面临的重大挑战。

4.4 可信接入

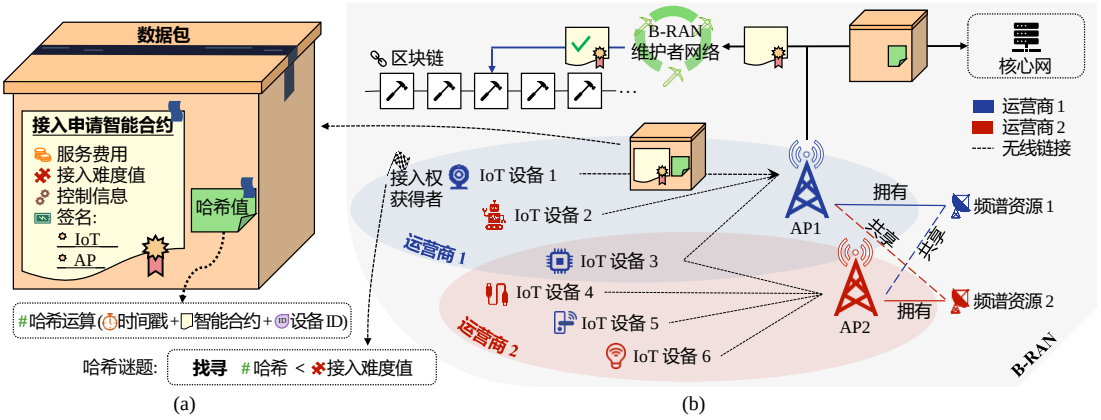

图 6　哈希接入机制示意图

未来 6G 网络将包含属于多个互不信任参与方的海量异构设备，这些设备可能会忽略了预先设定的协议，为了自身利益而竞争有限的资源，而导致公共资源的浪费。尤其是对于共享链路（例如物联网上行链路）的免授权接入，大量设备共享一个公共接入链路，而无需请求权限或专用资源。由于缺乏信任，自私的设备可能会故意缩短随机接入中的退避时间，以减少接入时延。伴随此类自私设备的数量和比例的持续增加，网络中将会出现灾难性的拥塞，这种情况称为开放接入困境[133]。

为了消除用户终端设备之间的不信任并解决免授权情形下的开放接入困境，文献[133]中提出了一种可信接入方案——哈希接入，并在 B-RAN 架构内对其进行了数学模型分析和评估[140]。如图 6 所示，每个设备都需要在发送数据包之前计算出低于给定阈值的哈希值来解决哈希难题。否则，设备将被拒绝接入当前时隙。哈希难题由当前时间戳，其唯一标识符（ID）和接入合约共同决定。由于哈希函数具有不可逆性，哈希难题的结果很容易验证，但很难伪造。自私设备几乎不可能生成伪造的哈希值。因此，哈希接入相当于变相地引入了一种强制的随机退避机制来避免冲突，任何设备都无法跳过该机制的约束。通过这种方式，哈希接入强制设备遵守接入规则，在用户终端设备之间建立信任，从而防止自私设备的欺诈行为。另外，哈希难题中的阈值确定了每个设备的接入难度，可以根据 B-RAN 中的流量相应地对其进行调整。此外，哈希接入保证了上行链路资源的公平共享，从而促进了多方协作，有助于跨网资源的整合和负载均衡。

除了上面讨论的物联网自私设备的不当行为外，“3.3 安全接入控制”部分中还研究了无线网络不同层中的设备接入的其他安全风险，6G 网络中安全、可靠的设备接入控制方法还有待开发。B-RAN 提供了一个理想的平台，在具有潜

在安全风险的异构网络及实体间建立起协作信任，可从系统级层面将多种接入方法及协议集成于未来 6G 体系架构中。

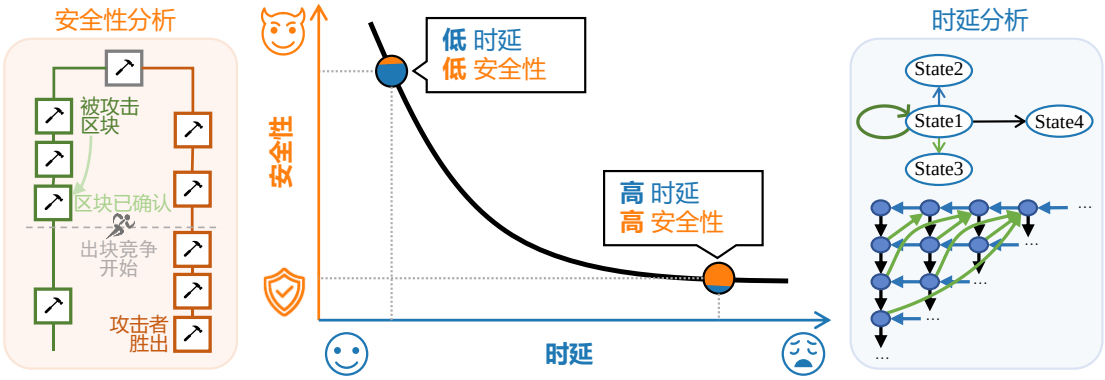

图 7　B-RAN 数学模型及时延与安全性指标的权衡示意图

4.5 数学模型与表征

尽管基于区块链的无线网络已逐渐成为学术界关注焦点，但关于其数学表征和基础分析的研究工作却相当有限，许多问题仍未得到解决。在引入区块链后，现有的研究工作暂未评估分布式特性对 B-RAN 的影响，但是对其进行表征分析和精准量化的工作对实际系统的研发及部署却十分重要。目前，鲜有工作注意到服务时延对于 B-RAN 来说是一个十分重要的问题。作为 B-RAN 的另一个关键方面，其安全性也尚未得到充分研究。因此，迫切需要一个分析模型来深入分析 B-RAN 的特性（例如时延和安全性），并为其落地提供进一步的指导。

在文献[143]中，作者对 B-RAN 进行了初步的数学建模，并分析了 B-RAN 的特性和性能。具体来说，文章根据泊松（Poisson）过程对区块生成进行了建模，并通过实际数据对其进行了验证，然后为 B-RAN 建立了一个基于连续齐次马尔科夫过程的排队模型。在排队模型的基础上，作者进一步提供了状态转换分析及示意图，从时间平均维度评估了服务时延，并通过进一步推导时延的上下限揭示了诸多 B-RAN 系统关键参数对服务时延的影响。此外，文章还通过考虑攻击者侧策略来评估及量化 B-RAN 的安全性能。

该文在对 B-RAN 时延和安全性进行分析时发现了它们之间的内在关系，如图 7 中所示的时延-安全权衡曲线。一方面，B-RAN 的请求等待时间与区块生成时间呈近似线性关系，并且随着区块验证确认次数或区块生成时间的增加而增加。另一方面，B-RAN 需要更多的区块确认数来降低攻击成功概率。确认数是权衡 B-RAN 中的服务等待时间和系统安全的关键因素，应谨慎选择。这种权衡特征能够综合地体现出 B-RAN 所能达到的性能。文献[143]中的分析模型为设计基于

区块链的无线网络提供了重要的启发，基于区块链的网络不仅在抵御恶意区块链维护者的攻击方面具有足够的安全性，同时还拥有较低的接入时延。

4.6 跨网络协作及共享

B-RAN 能够吸引大量服务提供商和用户，从而实现跨网海量资源共享。随着用户数量的增加，更多的服务提供商会出于经济动机而加入 B-RAN。随着服务提供商的增加，服务质量（QoS）的提升又将进一步提升 B-RAN 的吸引力，从而形成正反馈网络效应。此外，B-RAN 还担任了管理服务提供商的角色。B-RAN 是一个允许多边团体（不限于服务提供商与用户）加入的平台，它们之间能够直接交互，这种多边性使得 B-RAN 的构成趋于多样化。这些来自多个不同参与方的资源或服务在 B-RAN 中会被商品化，通过智能合约进行虚拟化后放入资源池，这将促使多维资源及服务更进一步的深度共享。以下总结了 B-RAN 中几种重要的资源类型：

1. 频谱：B-RAN 中的频谱被虚拟化为数字化频谱资源。频谱资源可以定义为在指定的时间内，在指定覆盖区域及频段上进行数据传输的有限权利。相比单运营商网络，多运营商场景中的频谱资源利用将更加高效和灵活。
2. 基础设施：B-RAN 中的基础设施包括接入点、基站（BS）、移动边缘计算设备、云服务器和骨干传输网等，属于不同网络的基础设施可以通过计算能力授权、数据交叉存储或网络接入等 B-RAN 服务在不同的服务提供商及用户间进行共享，可显著提升设施利用率并提高网络整体效率。
3. 设备：得益于不同的物联网互联设备的群体感知能力，海量用户设备可以协同为服务提供商或其他应用程序的大规模服务收集数据并提取信息。用户终端数量的增长将会吸引更多的服务提供商加入 B-RAN，并进一步取得规模效益，激励 B-RAN 持续发展。
4. 内容：B-RAN 中的内容可以是媒体文件、软件、文件、应用程序、实时流媒体等。服务提供商不仅可以提供内容交付服务，还可鼓励用户参与创建或提供内容。在 B-RAN 的安全和隐私保护策略下，内容不可篡改且仅在服务过程中由受信用户接入。
5. 控制：在 B-RAN 中，多个设备的控制能力也是一类资源，B-RAN 中具有数据包转发功能的网络设施或智能设备均可在共享密钥授权的控制命令下运行。通过区块链技术，B-RAN 可实现更加可信及可靠的控制。
6. 能源：B-RAN 中的能源通常是来源于化石资源或可再生能源的电能。闲置能源充足的装置可对其他设备进行能源对点供给，并获得相应报酬，B-RAN 中能源生产者和消费者可以安全、公平地进行交互。

7. 智能：B-RAN 中的智能是可信的机器学习模型及相应功能，如计算、缓存和通信等，并以此来执行学习、分类、优化等一系列智能算法。在 B-RAN 中，可以在异构设备上以协作联合的方式调度智能资源并保证协同过程中的数据隐私及安全。

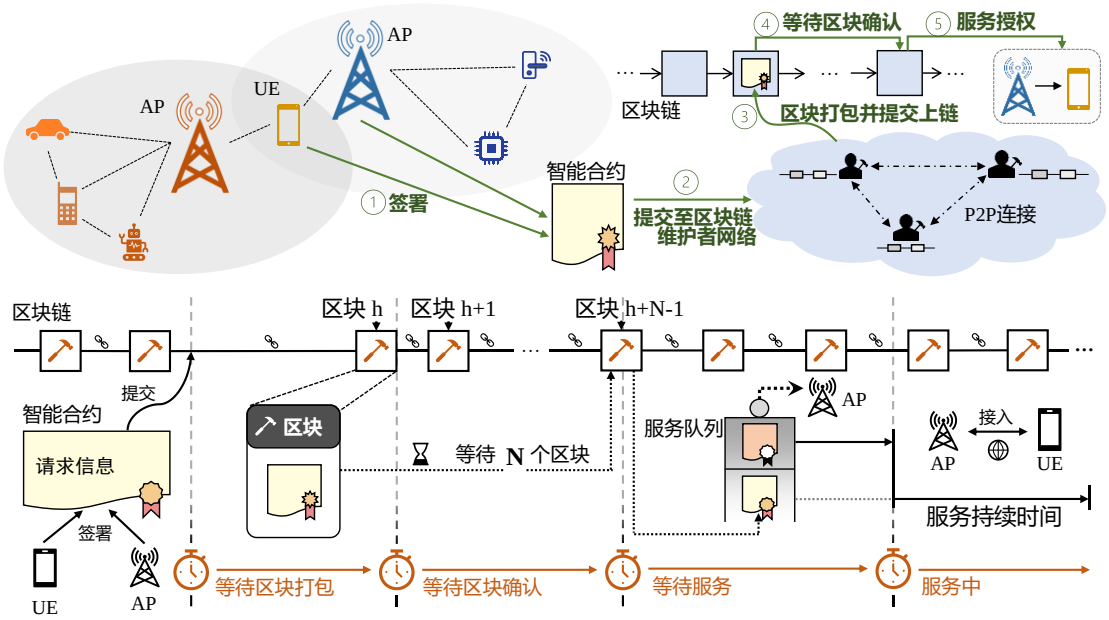

图 8　B-RAN 基本工作流程示意图

图 8 中展示了一个 B-RAN 服务流程的示例步骤，以下介绍了 B-RAN 用户设备向服务提供商请求服务的基本流程。

1. 在准备接入时，用户设备和服务提供商首先应该签订服务协定（SLA），其中包含各项服务详细信息、服务类型和服务费用等申请细节。服务条款和费用将明确记录在经过双方数字签名确认的一份智能合约中。
2. 步骤 1：用户与服务提供商共同将智能合约提交至区块链网络，等待区块链网络维护者验证其有效性。
3. 步骤 2：区块链网络维护者完成对智能合约的验证，待本轮共识达成后，将其记录在新的区块中。
4. 步骤 3：新区块封装好后上传至主链，智能合约在得到足够数量后续区块的安全确认后，所记录的服务正式进入至服务提供商的服务等待队列。
5. 步骤 4：服务提供商完成先前请求的服务后，将根据智能合约中的请求信息向用户设备提供接入服务。

B-RAN 在效率方面的优势来源于网络池化效应，B-RAN 中各子网间可灵活地共享资源和服务。在上述示例中，用户设备已通过图 8 中所示过程与服务提供商建立了信任，因此用户设备可以接入和使用 B-RAN 中其他服务提供商共享的资源，其中涉及的交易和漫游费用将由智能合约定期清算。在这种情况下，B-

RAN 的维护者可以使用一些智能算法来分配汇聚的资源，以提高网络效率。因此，移动设备可以接入隶属于不同子网的优选服务提供商，以获得更高质量的资源和服务。

4.7 数据追踪及审查

在大数据时代，数据量的快速增长给企业、社会和政府带来了诸多挑战。数据泄露事件频繁发生，为数据安全带来了紧迫风险[144]。无线网络开放性和移动性的特点使其更容易面临数据泄露和恶意入侵。从数据安全和保护用户隐私的角度出发，需要对数据进行追踪和审查，以检测数据泄漏，并防止对敏感数据未经授权的接入和使用。一些国家和组织已经发布了关于数据使用的相关法规，从而遏制数据泄漏的现象并加强了数据追踪和审查的可信度。例如，欧盟在 2018 年发布了《General Data Protection Regulation (GDPR)》[145]，美国发布了《National Security and Personal Data Protection Act of 2019 (NSPDPA)》[146]。

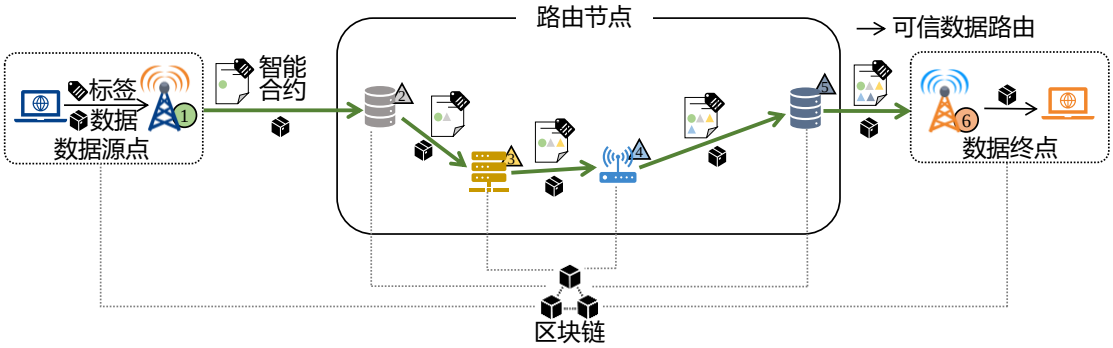

图 9　B-RAN 中数据追踪和审查机制示意图

目前，网络数据追踪和审查方法主要有两种，基于深度数据包检查（DPI，deep packet inspection）[147]以及流量分析[148]。基于深度数据包检查的方案通常需要进行大量的数据处理并手动发现流量特征；流量分析可能遭受实时性能和部署效率的困扰，这使其难以随着大数据的快速增长而扩展。除此之外，数据标记技术也可以用于追踪网络流量，例如文献[146,147]设计了两种水印方案，用于移动网络中的数据追踪和分析。文献[148,149]展示了使用区块链技术来实现或增强数据追踪和审查的可行性技术方案，目前区块链已经广泛应用在加密货币、医疗保健和食品供应链等领域。但是，区块链赋能的无线网络数据追踪和审查方法仍有待进一步研究。

在 B-RAN 中，数据通过多个中继路径在设备和基础设施间传递。由网络中多源实体组成的区块链网络能够以可靠且透明的方式记录数据的路由路径，因此适用于数据追踪和审查。通过与数据标记技术的结合，所设计的 B-RAN 数据追踪和审查方案如图 9 所示。该方案使来自不同制造商和运营商的路由节点加入

B-RAN，并通过智能合约将路由数据报告给区块链。为了保护数据及数据源的真实性，数据源必须使用设备内部的可信平台模块（TPM）为其传输数据生成一个难以伪造及篡改的数字标签，智能合约则用以记录数据标签和数据源的信息。此外，每个中继节点必须在接收到路由数据后添加自身的数字签名，并将最新合约提交给区块链，从而形成由智能合约组成的可信路由路径。因此，数据的中继路径由 B-RAN 中的多方共同审查并被区块链保护，难以被伪造或篡改，该方案可有利于监管机构进行数据审查和违规行为监控。

4.8 人工智能

B-RAN 可以提供一种智能资源供给机制，以分布式学习的方式管理网络资源。B-RAN 中的网络维护者可以通过机器学习技术监控资源状况并优化资源分配策略。正如“2.2 共识机制”部分所述，B-RAN 的智能合约为频谱和基础设施共享提供了可靠技术支撑，这有助于网络运营商更好地为用户服务。此外，还可以在 B-RAN 中实现资源交易、计算迁移和存储共享等功能。

B-RAN 的分布式特性能够较好地辅助并增强联邦式学习模式及效率。在 B-RAN 中，不同实体可以交换可信的机器学习模型并共享机器学习所需的算力，从而提高了联邦式学习的效率。区块链为 B-RAN 建立了多方信任关系，从而网络实体能够以开放包容的方式共享智能。B-RAN 可以追踪数据处理的全过程，从而增强机器学习的可解释性和可信度。

B-RAN 还可提高网络质量并提供智能服务。在用户发送请求后，B-RAN 网络维护者可以通过分布式学习的计划和分配服务，从而形成自适应智能服务网络。B-RAN 可以收集用户反馈的数据以调整实时服务质量，而服务调度则可作为不同网络实体之间的联合学习任务来执行。用户还可根据具体情况选择和使用适当的信号传输介质，例如毫米波、可见光、红外探测和太赫兹波等。

此外，B-RAN 可以监控网络状态，利用分布式学习，避免流量拥塞，实现快速差错定位。通过对历史数据进行深度学习，B-RAN 可以预测流量趋势并防止流量拥塞。为了在有限的网络资源和服务质量之间取得平衡，B-RAN 可以通过 AI 技术对数据包进行优先级排序，从而为网络运营商和用户带来最佳体验。但伴随着设备和用户数量的激增，由于预警信息的空间相关性以及基于机器学习的算法（例如学习向量量化神经网络（LVQNN）[153]和深度神经进化网络（DNEN）[154]）累积差错等原因，差错定位仍面临着诸多挑战。

4.9 原型设计

为验证 B-RAN 框架及一系列技术方案的性能，本节首先评估了 B-RAN 基本功能需求并构建了相应的原型架构。功能需求主要涵盖六个方面，包括物理存储、数据结构、安全链接、网络、区块链共识、资源和资源交易以及用户应用程序。根据评估需求，本节进一步设计了相应的原型架构，将接入控制层、通道层、共识层和交易层等引入架构中并使用多个传统的网络系统层（即存储层、结构层、网络层和应用层）来保障 B-RAN 原型的基本功能。考虑到 B-RAN 独特的应用场景，本节将包括快速智能合约部署（FSCD）、哈希时间锁定合约（HTLC）和哈希接入的机制整合到架构中。前述基本功能需求和架构设计如图 10 所示。

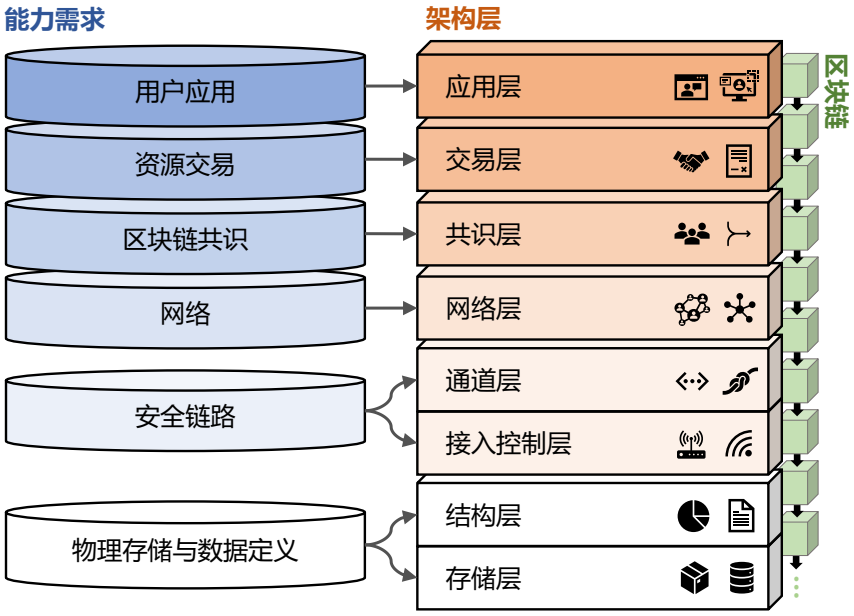

图 10　B-RAN 基本功能需求和体系结构设计示意图

1. 物理存储和数据：与 B-RAN 相关的所有区块链数据及信息组成了存储层，包括交易信息、多类别数字操作和加密密钥等。数据由服务器或任何有源电子设备在存储层中持久化，移动设备可仅存储部分信息构成轻量级节点，并非所有设备都需要存储区块链的完整副本。
2. 安全链接：B-RAN 中可建立节点间安全链接，通过在通道层中利用哈希时间锁定合约机制，用户终端和接入点之间可建立可信支付通道。通过接入控制层中的数据流控制和差错检测，B-RAN 可确保传输可靠性，利用智能合约保障链路数据交互安全。
3. 网络：B-RAN 中的海量异构子网构成了网络层基础，网络层主要负责各子网及其实体相互连接、新入节点发现、通信及同步，组构并维护分布式网络。

4. 区块链共识：B-RAN 中的共识层负责生成和验证区块，并确保参与者就 B-RAN 相关交易达成共识。B-RAN 中的所有维护者都遵循共识层中的机制及规则，通过可信协作明确区块生成与区块链维护决策。
5. 资源交易：B-RAN 基于确定性链上规则执行资源交易，保障服务提供商与用户之间的交易公平，在交易层中使用基于智能合约的服务协议（SLAs）可有效地确保此类公平性。
6. 用户应用程序：用户应用程序是架构的顶层设计，旨在让用户与区块链和智能合约进行交互。除接入服务外，B-RAN 还将为开发人员提供应用层中的应用程序接口（API），方便开发其他所需功能。

4.10 实验结果

本节将开展数项实验来评估 B-RAN 在不同运行参数设置下的实际性能，使用 Python 搭建了 B-RAN 原型，并在单局域网中运行的计算机集群上测试了该原型，通过预先设计的脚本自动收集相关实验数据。为验证 B-RAN 性能，本文将收集的数据与现有方案的实验数据进行了比较，在下文中主要介绍和分析有关服务时延、资源利用率和请求处理等方面的实验结果。

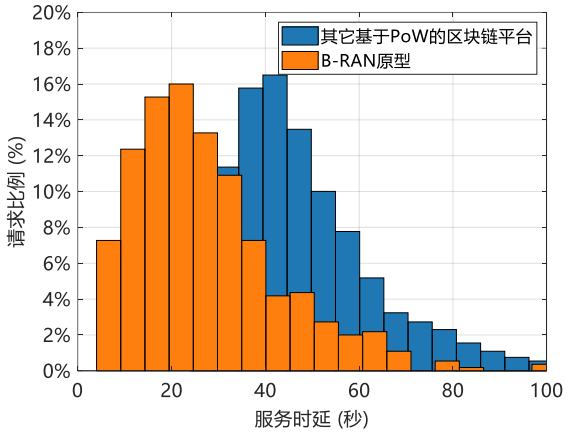

图 11　B-RAN 及其它基于 PoW 的区块链服务延迟分布对比

图 11 将基于 PoW 的 B-RAN 原型与其他基于 PoW 的区块链（例如，比特币和以太坊）的服务等待时间分布进行了比较。在实验中，将出块时间设置为 10 秒，并且设置了两个区块确认数以确保区块数据安全。如图所示，B-RAN 的服务等待时间显著低于其他基于 PoW 的区块链。通过配置快速部署智能合约机制，B-RAN 极大地减少了所需的服务等待周期，将服务等待时间缩短至几秒钟，而一般区块链平台中的服务时延通常会持续数分钟。缩短的服务等待时间会对 B-RAN 的用户满意度产生积极影响，并为系统安全性提升留出更大的改善空间（具体可参考“4.6 跨网络协作及共享”部分）。

图 12（a）展示了平均请求间隔时间对 B-RAN 的资源利用率的影响，并指出了链路资源的利用效率与服务请求密度之间的关系，其中资源利用率是根据链路的繁忙时间与总运行时长的比值来衡量的。在不同的服务时间下，平均请求间隔时间的减少会显著提升资源利用率。通过比较三种不同服务时间所对应的资源利用率变化趋势可发现：与较短的服务时间场景相比，当某段时间内平均服务时间很高或呈现上升趋势时，更高的请求密度（或更多活动用户）将使得 B-RAN 获得更高的资源利用率。可以看出，资源利用率的增长与网络规模的持续扩张及 B-RAN 用户参与度的提高密切相关。

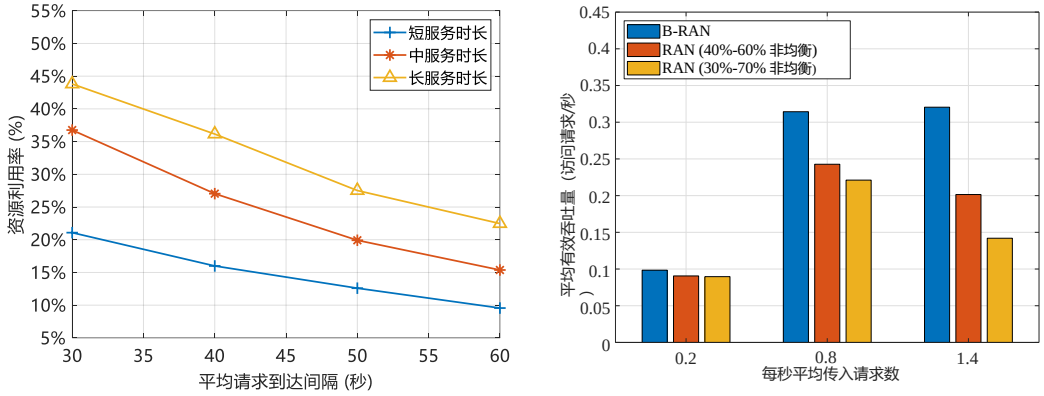

图 12　B-RAN 资源利用率及吞吐量性能评估。（a）平均请求到达时间在不同服务时间下对资源利用率的影响；（b）B-RAN 和两类流量非均衡 RAN 在不同请求强度下的有效吞吐量。

图 12（b）比较了 B-RAN 和其他两个“非均衡”接入网（RAN）在不同服务请求强度下的各子网平均有效吞吐量。在该实验中，B-RAN 和 RAN 都由两个子网组成，但不同的是，RAN 通常由两个具有不同流量负载且彼此隔离的子网组成。如图 12（b）所示，实验中测试的 RAN 与 B-RAN 预设了相同的流量负载，用户请求分别以 40%-60%和 30%-70%的比例不均等地分配给它们的子网。实验结果表明，B-RAN 的平均有效吞吐量在各种强度参数设置下均表现优异。由于 B-RAN 具有可信子网融合和平衡流量负载的功能，其不会受到子网流量不均的影响，当用户请求强度提升时，B-RAN 的有效吞吐量也始终显著高于其他两个“非均衡”RAN。

该实验演示了 B-RAN 在低服务时延、高资源利用率和突出的负载平衡方面的优势。服务等待时间的显著减少归功于快速智能合约部署机制，该机制有效提高了合约部署效率，并确保将合约和交易记录以强安全、高可靠的方式记录在区块链中，该机制还可减少合约部署时延，提升 B-RAN 网络的资源利用率。此外，由于 B-RAN 由多个子网融合组成，其请求处理效率远高于单个或多个独立网络，因此增加 B-RAN 容纳的子网数量也可显著提高网络的整体吞吐性能。

五、结论

本文针对移动通信演进中面临的一系列信任危机与安全挑战，深入调研了区块链赋能移动通信的前沿研究成果，并提出了面向 6G 可信移动通信的新型网络体系架构，旨在推动当前无线网络向更高效、更安全、更可信的方向发展。本文简要介绍了区块链基础技术及相关机制，并从资源共享、可信数据交互、安全接入控制、隐私保护、数据追踪、身份认证、信息监管等多个方面调研了区块链在无线通信领域的应用情况。本文提出了面向 6G 可信移动通信的区块链无线接入网（B-RAN）体系架构，旨在实现区块链与无线通信深度融合，打破“人-机-物-网”之间的信任壁垒，提升无线网络效率与安全性。本文详细介绍了 B-RAN 中共识机制、智能合约、可信接入、数学建模、跨网络协作及共享、数据追踪和审查、人工智能等多项关键要素，并展示了 B-RAN 原型设计与初步实验结果。

致谢

特别感谢张博文、高征、郭瑞伟、王子悦、王炎、李洋、杨兹博、陈鹏程、谢辉、王茂山、曹苇杭和杨雅萱在本文档编制工作中提供的无私帮助和宝贵建议。

参考文献

[1] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 2017–2022. https://www.davidellis.ca/wp-content/uploads/2019/12/cisco-vni-mobile-data-traffic-feb-2019.pdf (24 March 2021, date last accessed).

[2] Wang C, Haider F and Gao X et al. Cellular architecture and key technologies for 5G wireless communication networks. IEEE Commun Mag 2014; 52: 122–30.

[3] Andrews J G, Claussen H and DohlerM et al. Femtocells: Past, present, and future. IEEE J Sel Areas Commun 2012; 30: 497–508.

[4] Wang J, Guan W and Huang Y et al. Distributed optimization of hierarchical small cell networks: A GNEP framework. IEEE J Sel Areas Commun 2017; 35: 249–64.

[5] Marzetta T L. Noncooperative cellular wireless with unlimited numbers of base station antennas. IEEE Trans Wireless Commun 2010; 9: 3590–600.

[6] Heath R W, Gonzalez-Prelcic N and Rangan S et al. An overview of signal processing techniques for millimeter wave MIMO systems. IEEE J Sel Top Signal Process 2016; 10: 436–53.

[7] He S, Wang J and Huang Y et al. Codebook-based hybrid precoding for millimeter wave multiuser systems. IEEE Trans Signal Process 2017; 65: 5289–304.

[8] 6G FLAGSHIP. Key drivers and research challenges for 6G ubiquitous wireless intelligence. http://www.cbdio.com/image/site2/20191022/ f42853157e261f18f92561.pdf (10 December 2020, date last accessed).

[9] Saad W, Bennis M and Chen M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network 2019; 34: 134–42.

[10] You X H, Wang C X and Huang J et al. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci 2020, 64. doi: 10.1007/ s11432-020-2955-6.

[11] Mitola J and Maguire G Q. Cognitive radio: Making software radios more personal. IEEE Pers Commun 1999; 6: 13–8.

[12] Haykin S. Cognitive radio: Brain-empowered wireless communications. IEEE J Sel Areas Commun 2005; 23: 201–20.

[13] BTC Papers. Bitcoin: A Peer-to-Peer Electronic Cash System. https:// btcpapers.com/bitcoin.pdf (10 December 2020, date last accessed).

[14] Tschorsch F and Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun Surv Tutorials 2016; 18: 2084–123.

[15] Tapscott D and Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York, USA: Portfolio, 1 st ed ed., 2016.

[16] Ethereum. Ethereum white paper. https://ethereum.org/en/whitepaper/ (10 December 2020, date last accessed).

[17] Cachin C. Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, 4. Chicago,USA, 2016.

[18] Federal Communications Commission. Remarks of commissioner jessica rosenworcel mobile world congress americas. https://docs.fcc.gov/public/attachments/DOC-354091A1.pdf (10 December 2020, date last accessed).

[19] AT&T. AT&T suite of blockchain solutions. https://www.business.att.com/learn/att-solutions-for-b lockchain.html (10 December 2020, date last accessed).
[20] Fobes. How telecom giants AT&T and T-Mobile are using blockchain. https://www.forbes.com/sites/benjaminpirus/2019/06/13/how-telecom-giants-att-and-t-mobile-are -using-blockchain/ (10 December 2020, date last accessed).
[21] ANTCHAIN. Antchain. https://antchain.antgroup.com/ (10 December 2020, date last accessed).
[22] TrustSQL. TrustSQL. https://trustsql.qq.com/ (10 December 2020, date last accessed).
[23] Nguyen D C, Pathirana P N and Ding M et al. Blockchain for 5G and beyond networks: A state of the art survey. J Network Comput Appl 2020; 166: 102693.
[24] Xie J, Tang H and Huang T et al. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun Surv Tutorials 2019; 21: 2794–830.
[25] Ling X, Wang J and Bouchoucha T et al. Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. IEEE Access 2019; 7: 9714–23.
[26] Liu Y, Yu F R and Li X et al. Blockchain and machine learning for communications and networking systems. IEEE Commun Surv Tutorials 2020; 22: 1392–431.
[27] Xu H, Klaine P V and Onireti O et al. Blockchain-enabled resource management and sharing for 6G communications. Digital Commun Networks 6: 261–9.
[28] Nguyen G T and Kim K. A survey about consensus algorithms used in blockchain. J Inf Process Syst 2018; 14: 101–28.
[29] Tromp J. Cuckoo cycle: A memory bound graph-theoretic proof-of-work. In: International Conference on Financial Cryptography and Data Security. San Juan, PR, 2015. 49–62.
[30] Ball M, Rosen A and Sabin M et al. Proofs of useful work. IACR Cryptology ePrint Arch 2017; 2017: 203.
[31] Bravo-Marquez F, Reeves S and Ugarte M. Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions. In: 2019 IEEE International Conference on Decentralized Applications and Infrastructures. San Francisco, CA, USA, 2019. 119–24.
[32] Peercoin. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. https://docs.peercoin.net/#/proof-of-stake (10 December 2020, date last accessed).
[33] Milutinovic M, He W and Wu H et al. Proof of luck: An efficient blockchain consensus protocol. In: 1st Workshop System Software Trusted Execution. Trento, IT, 2016. 1–6.
[34] Larimer D. Delegated proof-of-stake (DPoS). Bitshare white paper, 2014.
[35] Kiayias A, Russell A and David B et al. Ouroboros: A provably secure proof-ofstake blockchain protocol. In: 7th Annual International Cryptology Conference. Santa Barbara, US, 2017. 357–388.
[36] Blocki J and Zhou H S. Designing proof of human-work puzzles for cryptocurrency and beyond. In: Theory of Cryptography : 14th International Conference. Beijing, CN, 2016. 517–46.
[37] Jingyu F, Xinyu Z and Kexuan C et al. Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks. Future Gener Comput Syst 2020; 105: 248–58.
[38] Eyal I, Gencer A E and Sirer E G et al. Bitcoin-NG: A scalable blockchain protocol. In: 13th USENIX symposium on networked systems design and implementation. Santa Clara, CA, USA, 2016. 45–59.

[39] Lamport L et al. Paxos made simple. ACM Sigact News 2001; 32: 18–25.
[40] Ongaro D and Ousterhout J. In search of an understandable consensus algorithm. In: 2014 USENIX Annual Technical Conference. Philadelphia, PA, US, 2014. 305–19.
[41] Castro M, Liskov B et al. Practical byzantine fault tolerance. In: 3rd Symposium on Operating Systems Design and Implementation, vol. 99. New Orleans, LA, US, 1999. 173–86.
[42] OpenEthereum. Proof of authority. https://github.com/openeth ereum/parity-ethereum/ (7 February 2021, date last accessed).
[43] Dwork C and Naor M. Pricing via processing or combatting junk mail. In: International Cryptology Conference on Advances in Cryptology. Santa Barbara, CA, USA, 1992. 139–47.
[44] Lamport L, Shostak R and Pease M. The Byzantine generals problem. ACM Trans Program Lang Syst 1982; 4: 382– 401.
[45] Aublin P L, Mokhtar S B and Quéma V. RBFT: Redundant byzantine fault tolerance. In: 2013 IEEE 33rd International Conference on Distributed Computing Systems, Philadelphia, PA, USA, 2013. 297-306.
[46] Dinh T T A, Wang J and Chen G et al. Blockbench: A framework for analyzing private blockchains. In: 2017 ACM International Conference on Management of Data. New York, NY, USA, 2017. 1085–100.
[47] Kwon J. Tendermint: Consensus without mining. https://tendermint.com/static/docs/tendermint.pdf (21 August 2021, date last accessed).
[48] Ethereum Blog. Slasher: A punitive proof-of-stake algorithm. https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/ (10 December 2020, date last accessed).
[49] Zou W, Lo D and Kochhar P S et al. Smart contract development: Challenges and opportunities. IEEE Trans Software Eng 2019. doi: 10.1109/TSE. 2019.2942301.
[50] Harris C G. The risks and challenges of implementing ethereum smart contracts. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency. Seoul, KOR, 2019. 104–10.
[51] Sayeed S, Marco-Gisbert H and Caira T. Smart contract: Attacks and protections. IEEE Access 2020; 8: 24416–27.
[52] Liu Y, Yu F R and Li X et al. Decentralized resource allocation for video transcoding and delivery in blockchainbased system with mobile edge computing. IEEE Trans Veh Technol 2019; 68: 11169–85.
[53] Qian P, Liu Z and He Q et al. Towards automated reentrancy detection for smart contracts based on sequential models. IEEE Access 2020; 8: 19685–95. data security. Christ Church, BB, 2014. 157–75.
[54] Parizi R M, Amritraj and Dehghantanha A. Smart contract programming languages on blockchains: An empirical evaluation of usability and security. In: 2018 International Conference on Blockchain. Cham,CHE, 2018. 75–91.
[55] Pinna A, Ibba S and Baralla G et al. A massive analysis of ethereum smart contracts empirical study and code metrics. IEEE Access 2019; 7: 78194– 213.
[56] Kroll J A, Davey I C and Felten E W. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: 12th Workshop on the Economics of Information Security. Washington D.C., US, 2013. 11.

[57] Ethereum Blog. Long-range attacks: The serious problem with adaptive proof of work. https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work/ (10 December 2020, date last accessed).

[58] Eyal I and Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. In: International conference on financial cryptography and data security. Berlin, Heidelberg, DEU, 2014. 436–54.

[59] Bahack L. Theoretical Bitcoin attacks with less than half of the computational power (draft). arXiv:13127013.

[60] Bai Q, Zhou X and Wang X et al. A deep dive into blockchain selfish mining. In: IEEE International Conference on Communication. Shanghai, CN, 2019. 1–6.

[61] Mayer H. ECDSA security in Bitcoin and Ethereum: A research survey. CoinFaabrik 2016; 28: 126.

[62] Bos J W, Halderman J A and Heninger N et al. Elliptic curve cryptography in practice. In: 18th International Conference on Financial cryptography and data security. Christ Church, BB, 2014. 157–75.

[63] Howgrave-Graham N A and Smart N P. Lattice attacks on digital signature schemes. Des Codes Cryptography 2001; 23: 283–90.

[64] Yin W, Wen Q and Li W et al. An anti-quantum transaction authentication approach in blockchain. IEEE Access 2018; 6: 5393–401.

[65] Li A, Wei X and He Z. Robust proof of stake-a new consensus protocol for sustainable blockchain systems. Sustainability 2020; 12: 2824.

[66] Ekparinya P, Gramoli V and Jourjon G. Impact of man-in-the-middle attacks on Ethereum. In: IEEE 37th Symposium on Reliable Distributed Systems. Salvador, BR, 2018. 11–20.

[67] Douceur J R. The sybil attack. In: 1st International Workshop on Peer-ToPeer Systems. Cambridge, US, 2002. 251–60.

[68] Zhao Q and Sadler B M. A survey of dynamic spectrum access. IEEE Signal Process Mag 2007; 24: 79–89.

[69] Weiss M B H, Werbach K and Sicker D C et al. On the application of blockchains to spectrum management. IEEE Trans Cognit Commun Networking 2019; 5: 193–205.

[70] Han S and Zhu X. Blockchain based spectrum sharing algorithm. In: IEEE 19th International Conference on Communication Technology. Xi'an, CN, 2019. 936–40.

[71] Kotobi K and Bilen S G. Secure blockchains for dynamic spectrum access a decentralized database in moving cognitive radio networks enhances security and user access. IEEE Veh Technol Mag 2018; 13: 32–9.

[72] Zhou Z, Chen X and Zhang Y et al. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. IEEE Network 2020; 34: 24–31.

[73] Fan X and Huo Y. Blockchain based dynamic spectrum access of non-realtime data in cyber-physical-social systems. IEEE Access 2020; 8: 64486–98.

[74] Maksymyuk T, Gazda J and Han L et al. Blockchain-based intelligent network management for 5G and beyond. In: 3rd International Conference on Advanced Information and Communications Technologies. Lviv, UA, 2019. 36–9.

[75] Sevindik V. Autonomous 5G smallcell network deployment and optimization in unlicensed spectrum. In: IEEE 2nd 5G World Forum. Dresden, DE, 2019. 446–51.

[76] Guo S, Dai Y and Xu S et al. Trusted cloud-edge network resource management: DRL-driven service function chain orchestration for IoT. IEEE IoT J 2020; 7: 6010–22.

[77] Li Z, Yang Z and Xie S et al. Creditbased payments for fast computing resource trading in edge-assisted Internet of Things. IEEE IoT J 2019; 6: 6606–17.

[78] Chatzopoulos D, Ahmadi M and Kosta S et al. FlopCoin: A cryptocurrency for computation offloading. IEEE Trans Mob Comput 2018; 17: 1062–75.

[79] Sun W, Liu J and Yue Y et al. Joint resource allocation and incentive design for blockchain-based mobile edge computing. IEEE Trans Wireless Commun 2020; 19: 6050–64.

[80] Wang S, Ye D and Huang X et al. Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach. IEEE Trans Network Sci Eng 2020. doi: 10.1109/ TNSE.2020.3004475.

[81] Sun J, Yao X and Wang S et al. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access 2020; 8: 59389–401.

[82] Xu Y, Ren J and Zhang Y et al. Blockchain empowered arbitrable data auditing scheme for network storage as a service. IEEE Trans Serv Comput 2019; 13: 289–300.

[83] Mafakheri B, Subramanya T and Goratti L et al. Blockchain-based infrastructure sharing in 5G small cell networks. In: 14th International Conference on Network and Service Management. Rome, IT, 2018. 313–7.

[84] Dong Z, Luo F and Liang G. Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. J Mod Power Syst Clean Energy 2018; 6: 958–67.

[85] Huh S, Cho S and Kim S. Managing IoT devices using blockchain platform. In: 19th International Conference on Advanced Communication Technology. PyeongChang, KR, 2017. 464–7.

[86] Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J 2018; 5: 1184–95.

[87] Košt'ál K, Helebrandt P and Belluš M et al. Management and monitoring of IoT devices using blockchain. Sensors 2019; 19: 856.

[88] Yu B, Wright J and Nepal S et al. IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain. IEEE Cloud Comput 2018; 5: 12–23.

[89] Rost P, Mannweiler C and Michalopoulos D S et al. Network slicing to enable scalability and flexibility in 5G mobile networks. IEEE Commun Mag 2017; 55: 72–9.

[90] Backman J, Yrjölä S and Valtanen K et al. Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. In: Internet of Things Business Models, Users, and Networks. Copenhagen, DK, 2017. 1–8.

[91] Valtanen K, Backman J and Yrjölä S. Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case. In: IEEE Wireless Communications and Networking Conference Workshops Barcelona, ES, 2018. 185–90.

[92] Zanzi L, Albanese A and Sciancalepore V et al. Nsbchain: A secure blockchain framework for network slicing brokerage. In: IEEE International Conference on Communications. 2020. 1–7.

[93] Togou M A, Bi T and Dev K et al. DBNS: A distributed blockchain-enabled network slicing framework for 5G networks. IEEE Commun Mag 2020; 58: 90–6.

[94] Huang Z, Su X and Zhang Y et al. A decentralized solution for IoT data trusted exchange based-on blockchain. In: 3rd IEEE International Conference on Computer and Communications. Chengdu, CN, 2017. 1180–4.

[95] Shi P, Wang H and Yang S et al. Blockchain-based trusted data sharing among trusted stakeholders in IoT. Software Pract Experience 2019; 1–14.

[96] Liu X, Huang H and Xiao F et al. A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. IEEE Internet Things J 2020; 7: 4101–12.

[97] Cinque M, Esposito C and Russo S. Trust management in fog/edge computing by means of blockchain technologies. In: IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. Halifax, NS, Canada, 2018. 1433–9.

[98] Chai H, Leng S and Zhang K et al. Proof-of-Reputation based-consortium blockchain for trust resource sharing in Internet of Vehicles. IEEE Access 2019; 7: 175744–57.

[99] Javaid U, Aman M N and Sikdar B. Drivman: Driving trust management and data sharing in VANETs with blockchain and smart contracts. In: IEEE 89th Vehicular Technology Conference. Kuala Lumpur, Malaysia, 2019. 1–5.

[100] Ma Z, Wang X and Jain D K et al. A blockchain-based trusted data management scheme in edge computing. IEEE Trans Ind Inf 2020; 16: 2013–21.

[101] Yang Z, Yang K and Lei L et al. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet Things J 2019; 6: 1495– 505.

[102] Yang Y, Chou L and Tseng C et al. Blockchain-based traffic event validation and trust verification for VANETs. IEEE Access 2019; 7: 30868–77.

[103] Javaid U, Siang A K and Aman M N et al. Mitigating loT device based DDoS attacks using blockchain. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. New York, NY, USA, 2018. 71–6.

[104] Pinno O J A, Gregio A R A and Bona L C E D. ControlChain: Blockchain as a central enabler for access control authorizations in the IoT. In: IEEE Global Communications Conference. Singapore, 2017. 1–6.

[105] Zhang Y, Kasahara S and Shen Y et al. Smart contract-based access control for the Internet of Things. IEEE Internet Things J 2019; 6: 1594–605.

[106] Ding S, Cao J and Li C et al. A novel attribute-based access control scheme using blockchain for IoT. IEEE Access 2019; 7: 38431–41.

[107] Xu R, Chen Y and Blasch E et al. Blendcac: A blockchain-enabled decentralized capability-based access control for IoTs. In: IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. Halifax, NS, Canada, 2018. 1027–34.

[108] Ouaddah A, Abou Elkalam A and Ait Ouahman A. FairAccess: A new blockchain-based access control framework for the Internet of Things. Secur Commun Networks 2016; 9: 5943–64.

[109] Le T and Mutka M W. CapChain: A privacy preserving access control framework based on blockchain for pervasive environments. In: IEEE International Conference on Smart Computing. Taormina, Italy, 2018. 57–64.

[110] Cha S, Chen J and Su C et al. A blockchain connected gateway for BLEbased devices in the Internet of Things. IEEE Access 2018; 6: 24639–49.
[111] Xu H, He Q and Li X et al. BDSSFA: A blockchain-based data security sharingslatform with fine-grained access control. IEEE Access 2020; 8: 87552–61.
[112] Dorri A, Steger M and Kanhere S S et al. BlockChain: A distributed solution to automotive security and privacy. IEEE Commun Mag 2017; 55: 119–25.
[113] Guan Z, Si G and Zhang X et al. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Commun Mag 2018; 56: 82–8.
[114] Lei A, Cruickshank H and Cao Y et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE IoT J 2017; 4: 1832–43.
[115] Lu Z, Liu W and Wang Q et al. A privacy-preserving trust model based on blockchain for VANETs. IEEE Access 2018; 6: 45655–64.
[116] Gai K, Wu Y and Zhu L et al. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet Things J 2019; 6: 7992–8004.
[117] Keshk M, Turnbull B and Moustafa N et al. A privacy-preserving framework based blockchain and deep learning for protecting smart power networks. IEEE Trans Ind Informat 2020; 16: 5110–8.
[118] Lu Y, Huang X and Dai Y et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans Ind Inf 2020; 16: 4177–86.
[119] Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 13th International Conference on Service Systems and Service Management. Kunming, China, 2016. 1–6.
[120] Caro M P, Ali M S and Vecchio M et al. Blockchain-based traceability in agri-food supply chain management: A practical implementation. In: IoT Vertical and Topical Summit on Agriculture - Tuscany. Tuscany, Italy, 2018. 1–4.
[121] Mitani T and Otsuka A. Traceability in permissioned blockchain. IEEE Access 2020; 8: 21573–88.
[122] Watanabe H, Ishida T and Ohashi S et al. Enhancing blockchain traceability with DAG-based tokens. In: IEEE International Conference on Blockchain. Atlanta, GA, USA, 2019. 220–27.
[123] Alkhader W, Alkaabi N and Salah K et al. Blockchain-based traceability and management for additive manufacturing. IEEE Access 2020; 8: 188363–77.
[124] Liu H, Zhang P and Pu G et al. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing. IEEE Trans Veh Technol 2020; 69: 4221–32.
[125] Kleinaki A S, Mytis-Gkometh P and Drosatos G et al. A blockchain-based notarization service for biomedical knowledge retrieval. Comput Struct Biotechnol J 2018; 16: 288–97.
[126] Wang R, He J and Liu C et al. A privacy-aware PKI system based on permissioned blockchains. In: IEEE 9th International Conference on Software Engineering and Service Science. Beijing, CN, 2018. 928–31.
[127] Kubilay M Y, Kiraz M S and Mantar H A. Certledger: A new PKI model with certificate transparency based on blockchain. Comput & Secur 2019; 85: 333–52.
[128] Wang Z, Lin J and Cai Q et al. Blockchain-based certificate transparency and revocation transparency. IEEE Trans Dependable Secur Comput 2020. doi: 10.1109/TDSC.2020.2983022.

[129] Cheng J, Lee N and Chi C et al. Blockchain and smart contract for digital certificate. In: IEEE International Conference on Applied System Innovation. Chiba, JP, 2018. 1046–51.
[130] Xie R, Wang Y and Tan M et al. Ethereum-blockchain-based technology of decentralized smart contract certificate system. IEEE IoT Mag 2020; 3: 44–50.
[131] Lin S, Li J and Liang W. Research on strong supervision algorithm model based on blockchain in e-government. In: 5th IEEE Information Technology and Mechatronics Engineering Conference. Chongqing, CN, 2020. 345–9.
[132] Peng S, Hu X and Zhang J et al. An efficient double-layer blockchain method for vaccine production supervision. IEEE Trans NanoBiosci 2020; 19: 579–87.
[133] Hassija V, Chamola V and Krishna D N G et al. A blockchain and edge computing-based secure framework for government tender allocation. IEEE IoT J 2021; 8: 2409–18.
[134] Liu C, Xiao Y and Javangula V et al. Normachain: A blockchain-based normalized autonomous transaction settlement system for IoT-based ecommerce. IEEE IoT J 2019; 6: 4680–93.
[135] Ling X, Le Y and Wang J et al. Hash access: Trustworthy grant-free IoT access enabled by blockchain radio access networks. IEEE Network 2020; 34: 54–61.
[136] Ling X, Gao Z and Le Y et al. Satellite-aided consensus protocol for scalable blockchains. Sensors 2020; 20: 5616.
[137] Decker C and Wattenhofer R. Information propagation in the bitcoin network. In: IEEE International Conference on Peer-to-Peer Computing. Cambridge, MA, USA, 2013. 1–10.
[138] Wei H, Feng W and Zhang C et al. Creating efficient blockchains for the internet of things by coordinated satellite terrestrial networks. IEEE Wireless Commun 2020; 27: 104–10.
[139] Zhang Y H and Liu X F. Satellite broadcasting enabled blockchain protocol: A preliminary study. arXiv: 200414591.
[140] Le Y, Ling X and Wang J et al. Prototype design and test of blockchain radio access network. In: IEEE International Conference on Communication Workshops. Shanghai, CN, 2019.
[141] Lightning Network. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf (10 December 2020, date last accessed).
[142] Zhang B, Ling X and Le Y et al. Analysis and evaluation of hash access for blockchain radio access networks. In: IEEE International Conference on Wireless Communications and Signal Processing. Nanjing, CN, 2020.
[143] Ling X, Le Y and Wang J et al. Practical modeling and analysis of blockchain radio access network. IEEE Trans Commun 2021; 69: 1021–37.
[144] Cheng L, Liu F and Yao D D. Enterprise data breach: causes, challenges, prevention, and future directions. WIREs Data Mining and Knowledge Discovery 2017; 7: e1211.
[145] Voigt P and von dem Bussche A. The EU general data protection regulation (GDPR). https://link.springer.com/content/pdf/10.1007/978-3-319-57959-7.pdf (25 March 2021, date last accessed), 2017.
[146] Hawley J. National security and personal data protection act of 2019. https://www.congress.gov/bill/116th-congress/senate-bill/2889/text?r=1&s=2 (25 March 2021, date last accessed), 2019.

[147] Kumar S, Turner J and Williams J. Advanced algorithms for fast and scalable deep packet inspection. In: 2nd Symposium on Architectures for Network ing and Communications Systems. San Jose, UA, 2006. 81–92.

[148] Willinger W, Taqqu M S and Leland W E et al. Self-similarity in high-speed packet traffic: analysis and modeling of Ethernet traffic measurements. Statistical science 1995; 10: 67–85.

[149] Yu W, Fu X and Graham S et al. DSSS-based flow marking technique for invisible traceback. In: IEEE Symposium on Security and Privacy. Berkeley, CA, USA, 2007.

[150] Luo J, Wang X and Yang M. An interval centroid based spread spectrum watermarking scheme for multi-flow traceback. J Network Comput Appl 2012; 35: 60–71.

[151] Biryukov A and Tikhomirov S. Transaction clustering using network traffic analysis for bitcoin and derived blockchains. In: IEEE 38th Conference on Computer Communications Workshops. Paris, FR, 2019. 204–9.

[152] Azaria A, Ekblaw A and Vieira T et al. MedRec: Using blockchain for medical data access and permission management. In: 2nd International Conference on Open Big Data. Vienna, AT, 2016. 25–30.

[153] Yan F, Liu W and Tian L. LVQ neural network approach for fault location of distribution network. In: International Conference on Electrical and Control Engineering. Yichang, CN, 2011. 237– 40.

[154] Zhao X, Yang H and Guo H et al. Accurate fault location based on deep neural evolution network in optical networks for 5G and beyond. In: The Optical Fiber Communication Conference and Exhibition. San Diego, CA, USA, 2019. 1–3.