



中国移动 5G 联合创新中心
China Mobile 5G Innovation Center

中国移动 5G 联合创新中心创新研究报告

区块链+边缘计算 技术白皮书

(2020 年)



2020 年 6 月

前 言

区块链作为新型信息处理技术，在信任建立、价值表示和传递方面有不可取代的优势，目前已经在跨行业协作、社会经济发展中展现出其价值和生命力。边缘计算作为 5G 面向垂直行业的新技术，在网络和资源组织方式、业务体验提升方面都具有良好的竞争力。

本白皮书聚焦于探讨区块链与边缘计算技术和应用的结合点，探索二者结合产生的相互赋能、相互促进效果，在分析一些典型应用场景的需求、方案的基础上，提出通用性技术方案，包括服务模式和部署方案。最后，总结了“区块链+边缘计算”应用拓展面临的挑战和发展趋势。

“区块链+边缘计算”作为通信和信息技术融合发展的新领域，必将共同推动跨界融合创新、促进社会经济转型和发展。我们期望通过本白皮书启发业界思考和探索区块链+边缘计算的跨界应用创新，我们愿携手产业共同推动区块链+边缘计算技术的应用和推广，为区块链技术和产业创新发展注入新活力。

参与本白皮书撰写的主要专家包括中国移动研究院何申、陆璐、李征、杨波、王珂、耿亮、杭小勇、阎军智、郭义华、刘福文，中兴通讯的郭海生、郑锦荣、王海峰、朱堃、杨春建、王德政、林兆骥、章坚、张再军、周晶、张强、高洪、法润容，区块链技术与数据安全工业和信息化部重点实验室潘妍、李卫、李磊、余宇舟，北京大学新一代信息技术研究院董宁等。在此表示感谢。

目 录

引言	1
1 区块链与边缘计算相互促进、协同发展	2
1.1 区块链是 IT 技术的革命，是“价值互联网”的载体	2
1.2 边缘计算是运营商针对新商业模式的网络架构创新	3
1.3 区块链+边缘计算促进跨界协同和创新、加快社会信息化转型	4
1.3.1 边缘计算为区块链服务提供资源和能力	4
1.3.2 区块链为边缘计算提供信任	4
1.3.3 区块链+边缘计算产生促进效应	5
2 区块链+边缘计算的应用场景	6
2.1 共享类应用：区块链辅助边缘计算信息与资源的共享	6
2.1.1 跨节点业务层数据同步	6
2.1.2 边缘计算平台资源能力共享	7
2.1.3 共享经济	8
2.2 存证类应用：边缘计算支持区块链进行高效存证	9
2.2.1 视频存证	10
2.2.2 物联网数据的防伪存储	11
2.2.3 个人数据存证	12
2.2.4 行业数据可信处理	13
2.2.5 通信设备资产管理	14
2.2.6 通信设备巡检	15
2.2.7 通信设备的运维管理	16
2.3 安全类应用：区块链提供边缘计算安全增强	17
2.3.1 终端设备认证	17
2.3.2 IT/CT 域互信	17
2.3.3 应用、配置的完整性	18
3 区块链+边缘计算的技术实践	19
3.1 区块链+边缘计算的服务模式	19
3.2 区块链+边缘计算的部署方式	21
3.2.1 边缘计算部署现状及与区块链融合部署	21
3.2.2 On MEC--区块链部署在 MEC 资源池内	22
3.2.3 Off MEC--区块链部署在 MEC 资源池外	23

3.2.4	Hybrid MEC--混合部署.....	24
4	边缘计算+区块链的发展展望.....	25
3.3	面对的挑战.....	25
3.4	发展畅想.....	26
	缩略语.....	28
	参考文献.....	29
	联合编写单位及作者.....	30

引言

区块链作为一项新型信息处理技术，其在表示价值、传递信任方面具有天然的优势，是“价值互联网”的核心要素。边缘计算是 5G 系统针对低时延、大带宽、汇聚流量大、海量物联、高可靠特定应用场景的新型解决方案。5G 时代，区块链与边缘计算的结合，将助力运营商面向产业开拓 to-B 新市场。

本白皮书基于区块链与边缘计算各自的特点，在分析其技术结合点的基础上，梳理区块链+边缘计算的典型应用场景，并归纳出区块链+边缘计算的技术实现和部署方式，为产业提供发展建议。





1 区块链与边缘计算相互促进、协同发展

1.1 区块链是 IT 技术的革命，是“价值互联网”的载体

2019 年 10 月 24 日，在中共中央政治局第十八次集体学习会上，习主席提出区块链在“技术革新和产业变革中起着重要作用”，“把区块链作为核心技术自主创新的重要突破口”。2020 年 4 月，国家发改委将区块链确立为“新基建”的新技术基础设施。区块链是互联网之后信息技术又一次突破，是“价值互联网”的基石。互联网技术实现了信息的高效流通，而区块链技术将实现信任建立和价值传递的新机制，进一步促进社会生产和生活中新型协作体系的建立和完善。

区块链技术具有分布式处理、数据防篡改、多方共识等技术特征，实现了去中心化的信任建立、保存和传递能力。分布式是技术基础，防篡改保证了数据的稳定性和可靠性，透明性多方共识保证了数据的可验证和可信性。去中心化信任是区块链技术特征的自然结果，确保了价值能够高效、透明、安全、可信地存储和传递。

目前国家、多个省市和地区政府已经发布了区块链相关政策和指导意见，将区块链技术列入发展规划，积极开展区块链产业布局，为区块链产业的发展提供了政策基础。区块链技术已在供应链金融、物品溯源、智能制造、数字资产管理等领域开展了有益和成功的探索。以区块链为主营业务的创新公司数量增长迅速，产业已经初步形成。随着技术的发展，区块链将在更多产业领域得到应用：

- **数字金融：**基于区块链构建信用体系，降低金融服务的成本，解决中小企业贷款融资难、银行风控难、部门监管难等问题；
- **数字经济：**区块链和实体经济结合，利用区块链技术探索数字经济模式创新，打造便捷高效、公平竞争、稳定透明的营商环境，推进供给侧结构性改革，实现各行业供需有效对接提供服务，加快新旧动能接续转换，推动经济高质量发展；
- **数字身份：**在移动互联网向产业互联网发展过程中，每个人、每个企业甚至



每台设备，都会通过数字孪生科技拥有线上的数字身份，而区块链技术将作为数字身份的基础设施，对现有数字证书体系产生重大变革；

- **产业协同：**随着产业数字化进展的加快和供应链业态的不断演进，原有的产业生态抓手会逐渐从线下转移到线上，区块链起到传递信任、企业协同、数据资源共享等关键作用，最大化提升产业整体发展的效率；
- **社会民生：**通过区块链技术在教育、就业、养老、精准扶贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务；
- **智慧城市：**区块链底层技术服务和新型智慧城市建设相结合，在信息基础设施、智慧交通、能源电力等领域进行推广应用，提升城市管理的智能化、精准化水平。利用区块链技术促进城市间在信息、资金、人才、征信等方面更大规模的互联互通，保障生产要素在区域内有序高效流动；
- **智慧政务：**利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，为人民群众带来更好的政务服务体验。

1.2 边缘计算是运营商针对新商业模式的网络架构创新

边缘计算是网络演进和云计算技术发展的产物，在靠近用户的地方提供计算、存储、网络等基础设施，通过在该基础设施上部署和运行应用，为用户就近提供边缘云服务。相比于传统云计算的集中部署模式，边缘计算解决了通信时延长、汇聚流量大等问题，为低时延和高带宽的业务提供了更好的支持。边缘计算的本质是云计算在集中化数据中心之外汇聚节点甚至接入节点的延伸和扩展，以“边缘智能”、“端边互补”、“边网协作”和“云边协同”为核心能力^[1]。

超低时延和高带宽业务的需求、新型网络架构共同促进了在 5G 网络中引入边缘计算技术。边缘计算带动了运营商网络的变革，形成了“中心+边缘”的新型分布式网络架构。由于边缘节点位于用户到核心网的通信路径上，因此，运营商和设备制造商在边缘计算业务中具有不可替代的地位。随着边缘节点部署数量的增加，将逐步形成“边缘云+中心云”的新型云计算架构，培育出多样化的创新业



务和商业模式。

同时针对特定企业应用场景（如：工业互联网、园区办公网）提供数据本地分流和处理机制，实现了数据不出园（厂）区，具有更高的安全性。

随着 5G 业务和垂直行业应用的拓展，新兴市场对边缘计算的需求十分迫切。在众多垂直行业新兴业务中，低时延、高带宽和高安全性三个方面成为边缘计算的独特优势^[2]。

1.3 区块链+边缘计算促进跨界协同和创新、加快社会信息化转型

1.3.1 边缘计算为区块链服务提供资源和能力

借助边缘计算能力，运营商部署和推广区块链应用具有独特优势，区块链平台/应用可以部署在边缘计算平台上，为电信网络和行业应用提供区块链服务：

- **资源层面：**边缘计算平台为区块链节点的部署提供了新的选择，区块链可以与业务应用共用边缘计算节点资源，节省云端资源开销。区块链节点和应用以软件形式快速部署在边缘节点/边缘云上，具有部署效率高等优势；
- **通信层面：**由于边缘计算平台靠近用户侧，相比数据传输到云端，降低了通信时延，从用户角度，传播路径更加可控。还可以采取优化策略，将经常使用的账本数据、账户状态等数据、业务数据缓存在边缘节点中，提高通信效率，降低数据传输时延；
- **能力层面：**边缘计算平台集成运营商网络能力，部署在边缘节点的区块链应用可调用运营商面向垂直行业开放的能力，从而形成“信息+信任”的运营商特色区块链服务。

1.3.2 区块链为边缘计算提供信任

边缘计算节点在运营商网络中处在“端-边-网-云”的关节位置，在边缘节点上



引入区块链能力将极大助力运营商的产业拓展，如果说“5G+”行动为单个垂直行业提供通信和信息服务，那么在边缘计算中引入区块链服务能够实现不同产业之间的协同，为垂直行业提供中立、可信、易用的“信息+信任”平台，实现生产要素和资源在不同行业之间更高效地流通、有机整合，产生由点及面的效果，促进经济转型，甚至重构产业结构：

- **赋能协同：**边缘计算多级网络协同，构建智慧边缘。运营商网络原有的架构（包括 5G 的新架构）中，采用逐级集中、骨干网互联互通的模式，不同的边缘节点之间无法协作同步，“端-边-网-云”各方无法协同取证。借助叠加在边缘节点上的区块链服务，可打通不同边缘之间、“端-边-网-云”各方间的孤岛，形成信息和价值的打通，产生跨网协同效应；
- **赋能安全可信：**边缘计算基础设施、数据转发设备、边缘计算平台等靠近用户部署，运营商控制能力相对较弱，其平台的设备、配置、数据、应用等应具备完整性和真实性，而“端-边-网-云”架构下分散的各方，也有互访的需求。区块链可帮助建立边缘计算系统的完整性保障和防伪存证，也可帮助“端-边-网-云”各方实现去中心的认证；
- **赋能共享：**边缘计算节点为运行于其上的各种服务和第三方应用提供计算、网络和存储资源，终端、数据、能力也可以作为公共共享资源，开放给多个应用使用，这些资源都可以统一通过边缘计算平台上承载的区块链应用进行交易，以充分发挥其价值。

1.3.3 区块链+边缘计算产生促进效应

区块链技术促进安全可信，边缘计算技术促进高效可用；边缘计算+区块链可以构成高效信息+价值平台，促进资源共享和最优化配置，对运营商网络、业务、生态产生的促进效应和深远影响。



2 区块链+边缘计算的应用场景

按照应用业务需求和技术特点，可将应用场景梳理为如下几类：

- 共享类应用：利用区块链分布式记账和共识机制等特性，可在边缘计算组织生态中各参与方之间形成互通互联，或者在供应链上下游进行穿透，从而实现信用传递、数据同步和资源共享。
- 存证类应用：使用区块链的数据一致性和防篡改特点，保证数字化信息的完整性、时序性；边缘计算为数字化信息的存储、传输提供高效保障。
- 安全类应用：基于区块链账本数据的不可摧毁和不可篡改，实现终端接入边缘认证、IT 与 CT 贯通和互信、边缘设备配置完整性校验等网络安全、应用安全等安全功能。

2.1 共享类应用：区块链辅助边缘计算信息与资源的共享

2.1.1 跨节点业务层数据同步

场景：多个有数据同步关系的行业应用（如：位于边缘节点的行业应用模块和位于云端或另一个边缘节点的边缘应用模块间），使用区块链技术进行数据的分布式存储、安全分发及共享。

需求：行业应用可以依据时延、组网以及相应业务位置的不同，部署在接入、一般汇聚、重要汇聚以及地市核心等不同位置的边缘云中的边缘节点上。同时，边缘行业应用通常需要和部署在中心 DC、企业 DC 上的行业应用进行业务交互，其特征是不同位置的应用之间进行数据交互，比如：

边缘应用采集本地数据并且在本地进行业务处理，然后将统计、分析结果汇聚到核心云的行业应用进行统一呈现、统计及数据分析。典型应用如电力行业应用，发电、输电、配电及用电等边缘应用在完成本地业务处理后，将数据传送到集团汇聚，进行全局的数据分析及呈现^[3]；



对于低时延、高移动性的行业应用，不同边缘节点上的应用需要直接进行数据交互，以保证终端在移动、切换过程中应用层的业务连续性。典型的如车联网应用。

这些跨节点的业务交互和数据同步，需要保证节点间数据的一致性，有的业务或节点可能会要求数据发送或使用可追溯，对数据同步权限、实时性等方面提出了不同的要求，处理的数据量级不同。

方案：联盟链具有强一致性的共识机制、可追溯、无法篡改、时序不可逆等特点，在身份管理方面具有健全的成员身份管理和追溯机制。可以采用区块链的分布式账本进行数据同步过程中的一致性控制，使用智能合约等进行数据授权和使用追踪、数据一致性校验功能。

针对不同类型的业务，可根据数据交互的特点设定适当的区块链运行参数和采用特定的处理流程：针对如车联网等实时性要求高的应用，需要设置比较小的区块生成间隔时间；针对较少数据量，提交完整数据上链，通过区块链节点之间的数据同步机制共享数据；针对较大数据量，可使用区块链的身份管理系统所定义的数字身份和安全机制，由数据发起方向数据接收方发起连接认证，建立安全数据通道，进行数据的发送，同时将数据的摘要上传到区块链，保证数据的完整性和数据发送过程的可追溯。

2.1.2 边缘计算平台资源能力共享

场景：边缘计算平台可向第三方应用开放平台资源、网络能力等，第三方应用根据其业务需求动态申请资源，并通过区块链进行记账，运营方按照资源、能力使用记录进行计费和结算。

需求：边缘计算平台为运行于其上的各种服务和第三方 APP 应用提供资源 and 能力，包括计算、存储等通用资源，特殊资源（如 GPU、FPGA 等硬件加速资源）或网络能力（如定位，短信等）。边缘计算平台以租户为单位分配，通常采



用固定分配方式，向第三方业务提供者计费的方式也比较单一，常常是按第三方应用部署使用的时长、调用次数进行计费。随着边缘计算生态圈的发展，按需分配资源能力实现资源的高效利用、按实际使用进行高效可信结算的需求越来越强烈。这需要对资源能力的使用进行详细的计量，可采用区块链进行资源共享管理和记账，建立互信并优化处理流程。

方案：使用区块链记账时，边缘节点上的第三方边缘计算应用，有其自身的区块链节点或其信任的区块链节点。同样，边缘计算平台也有其自身的或其信任的区块链节点。区块链上同时有其他组织的节点。

边缘计算应用需要新申请资源时，例如有终端用户进入云游戏需要 GPU 资源时，通过边缘计算统一运营入口发起资源申请，由边缘计算统一运营平台进行资源分配。此时边缘计算平台生成区块链交易提案，提交给平台和 APP 的区块链节点进行审批，审批通过后，将数据（开始使用资源的记录）通过共识算法存储于区块链。当 APP 不再使用资源时，向边缘计算平台发出资源释放申请，停止资源的使用。资源释放后，APP 生成区块链交易提案，节点审批通过后，将数据（停止使用资源的记录）通过共识算法存储于区块链。边缘计算平台运营方定期搜集区块链上的记账数据，向提供 APP 的第三方收费，第三方可以通过区块链上的记录进行计费数据的核实。

综上，通过将共识后的使用数据及时上链，可避免事后对账时双方数据的差别导致不信任，在出现问题时也能及时发现解决，在提高资源使用计量的认可度的同时也提升了效率，有利于优化资源，促进边缘业务的发展。

2.1.3 共享经济

场景：拥有设备、资源、数据的个人/组织，通过邻近边缘节点的区块链进行共享、交易和评价，使得闲置的分散资源得到有效利用，帮助企业快速跨越数据积累阶段，提升用户体验，支持高效监管，促进共享经济的发展。



需求：边缘节点支持多种终端访问，如移动终端和传感器、摄像头等各种物联网设备，以及本地网络的电脑/服务器等。近年来，终端性能不断提高，大部分终端具有较强计算能力，支持存储能力和专用硬件资源，部分终端还拥有现场视频记录等内容资源、用户位置数据等，可以作为共享资源，授权开放给多个应用使用。而不同个体或机构间缺乏合作的保障和信任关系，不敢开展交互应用，形成孤岛，特别是数据具有价值不透明、可复制、易篡改、难确权、难追溯的特点，建立信任的过程冗长、效率低下。

方案：个人/组织有其自身的区块链节点或其信任的区块链节点，在本地安装区块链应用软件，使用积分或者绑定的支付手段进行链上支付，计费方式可以按使用时间、使用次数等。

资源拥有者通过区块链应用软件将其资源信息登记到区块链，包括资源类型、配置信息、资源访问授权信息(加密存储)等。资源需求者在链上进行检索匹配，找到合适的资源并付费后，获取到资源访问授权信息，访问目标设备，在其区块链应用软件的监控下进行资源的使用，并将使用记录上链存储。在使用完后可提交评价信息上链存储。

在区块链上进行设备、资源、数据的交易，通过授权机制保证安全，使交易过程、设备使用和数据访问记录、评价信息等不可篡改，各参与方都可对信息进行监督，更加公开透明和真实可信，从而促进公正合理的商业秩序及诚信和绿色节能的社会生活方式。

2.2 存证类应用：边缘计算支持区块链进行高效存证

信息存证是指从用户身份验证到信息创建，并对创建的信息数字化、存储和传输的全过程，通过采用一系列安全技术，全方位确保数字化信息的真实性、完整性和可信度。

在边缘计算应用场景中，结合边缘计算和区块链技术，可以为数据存证业务场景提供服务。边缘计算可以为区块链服务提供如下能力支撑：



- 缓解带宽压力：数据在公有云端完成分析，涉及海量数据的传输、处理和存储，给用户带来大量的带宽压力。边缘计算帮助解决传输的带宽问题；
- 提升传输实时性：网络传输时延会造成数据丢失，或者时序混乱，影响区块链对数据进行存储。通过就近的边缘节点可以加速数据传输存储和处理，提高数据读取的实时性；
- 提供数据安全：传统云端处理数据时，数据不加区别送往云端，路由复杂，数据缺乏安全信道。使用部署在边缘节点的区块链服务，传播路径高效可控；
- 提高可用性：边缘计算服务器为区块链提供存储资源，同时，部分业务数据本身会保存在边缘计算服务器上，或者通过边缘计算服务器进行流转，如有数据存证的需要，边缘计算服务器可以很方便地将数据/数据的特征值保存在区块链平台/BaaS（区块链即服务）平台上，无需额外的平台/系统间的数据对接。

2.2.1 视频存证

场景：视频数据通过边缘节点上的区块链进行本地数据存证。在业务方查询数据的时候，自动完成数据的验真服务，业务方能方便高效地获知数据真伪。

需求：矿区、校园、码头、海关等区域的监控视频、公检法等部门执法视频等，由各单位自行存储，当有特定情况发生需要调阅视频时，只能查询各单位自身存储的视频数据，而各单位基于本单位利益考量，很可能对本单位不利的视频数据进行删除、伪造等处理，这样数据存在造假的隐患，不利于还原事实真相进行追责。视频存证的需求，往往是存在视频记录方和监督方的情况下产生，例如集团公司对分公司的监控，以及出于公共安全方面的统一要求等。视频记录的可靠性，特别是经过长时间存储的历史视频的真实性可能被质疑。使用区块链记录进行佐证，可大大提高视频的可靠性。



方案：视频文件通常比较大，而区块链账本存储空间有限，在业务方案和流程的设计上考虑将视频文件摘要信息上传到区块链存证，而视频源文件还是物理分散在各单位原有的存储介质上。视频摘要信息包括视频文件的哈希值及文件名、文件大小等信息，可以在视频文件生成、存储的地方，如摄像头、视频服务器，安装一个边缘视频服务软件，定期检查视频文件生成摘要，发送给边缘区块链节点。区块链系统经过共识处理，将摘要数据存储到区块链网络上。

业务人员在调取本地视频文件进行查看时，边缘视频服务软件向区块链系统发出验真的请求，用视频文件重新生成摘要信息，如果和区块链上存储的摘要信息匹配，则表明其为当时记录的视频，没有被篡改，最终将验真的结果反馈给业务人员。

2.2.2 物联网数据的防伪存储

场景：物联网平台可以作为一个应用部署在边缘计算平台上，可存储物联网终端采集的数据，包括周边地区大气、水源、土壤等环境数据等。将物联网数据保存到区块链上，确保上链数据来源真实且不可篡改。监管者可以随时追溯到信息来源的全部视图，并通过区块链发布环境监控数据可提高公信力。

需求：物联网传感设备能获取到大量的物联网数据，通常情况下这些数据保存在云端物联网平台上，这将给运营商网络以及云端物联网平台的云服务器带来带宽、存储等资源压力，而且数据的真实性也得不到很好的保障。随着物联网应用的快速发展，对物联网可信的数据存证需求越来越迫切。

方案：该业务场景下，物联网设备采集的数据通过不同的边缘计算节点做汇聚，边缘计算节点将需要上链的数据通过内部接口发送到本边缘计算节点上的区块链服务，最后，可基于链上的可信数据提供发布、验真以及跨领域的业务协作等增值服务。



物联网业务使用区块链技术和 MEC 技术进行融合创新的前景十分广阔，一方面，借助物联网设备的物理防篡改特性，有助于实现区块链数据从链下到链上的“过程可信”；另一方面，区块链将各自分离、协议不同的物联网设备链接在一起，并通过事先约定规则、“沙箱式”数据处理等方式，形成下一代跨系统跨边界的数据共享协作新模式。而 MEC 技术则提高了物联网应用处理大量物联网数据的效率。

2.2.3 个人数据存证

场景：个人数据存证涉及到数据存储、检索、查验等业务场景，将个人数据存证的区块链功能部署于移动边缘计算的网路实体，从而充分发挥区块链与边缘计算的双重优势，获取更大收益。

需求：个人数据存证在我们日常生活中非常普遍，当前大多数还停留在纸质证明的阶段，比如个人用户之间的交互信息，如借条；政府机关颁发的证书，比如身份证、户口本、营业执照、学业证明等；还有日常经济活动中的各种票据、清单等，这些数据对电子存证需求巨大，应用领域十分广泛。

方案：在应用系统设计的时候，重点需要考虑哪些数据上链、数据采用什么形式上链的问题。通常情况下，当数据量较大时，采用数据特征值上链，包括数据哈希、大小、类型等；当数据量较小且标准化时，也可采用全数据上链。根据不同的业务场景，可设计不同的应用系统。完成业务数据上链是关键的一步，后续的数据查验即基于链上的可信数据做对比。业务人员发起数据查验时，平台将区分是全量数据还是数据特征值。对于全数据的查验，可直接对比链上数据；对于数据特征值，则可计算待查验数据的特征值后再跟链上保存的特征值做对比，给出查验结果。

个人数据存证涉及大量数据的处理和存储，将区块链节点部署在边缘云中，可以降低分布式节点区块链部署成本，改善用户体验、缓解云端资源占用。



2.2.4 行业数据可信处理

场景：区块链与边缘计算共同为行业生产活动的数字化提供可信与效率价值：行业多方将行业长流程业务各环节的生产数据实时向边缘云传输，部署在边缘计算节点的区块链服务可以提供实时存证，并基于可信数据的分析处理支持业务的可信执行，解决业务数据处理的带宽、实时性、安全与高可靠问题。

需求：传统行业与新一代数字化技术逐步融合带动产业发展，行业活动伴随多方参与、长流程、大量数据产生与智能处理。以现代农业为例，智慧农业希望依托传感器采集数据的多样性，对数据进行分析 and 智能处理，并将数据传感、存储、分析、联动整合为一体，完成远程监测、控制与预警。又如，航运物流业，海运环节涉及货主、货代、海关和船公司等多个参与方，航运业务繁多流程复杂，协同效率低成本高，需要联系各方实现协同商务，进而重构国际贸易产业链模式。这些都需要建立多方间的数据可信。

方案：

随着设备数量、数据传输量、数据计算量的快速增加，整个系统对传输带宽、计算和响应速度的要求越来越高，可以通过边缘计算提供低功耗大连接、低时延高可用等服务。同时利用区块链服务提供全流程数据多方交互、可信存证、可信执行，从而实现全过程的监测管控。

将行业长流程业务各环节的生产数据发送给就近部署的边缘节点上的相关应用，如监控信息、设备实时情况、单据等，借助区块链技术的数据透明性将信息流程实时上链，进行数据存证，为流程跟踪和业务追溯（如导航、作业调度、事故原因等）提供更加直观、细致的数据支撑；利用边缘计算能力对数据进行分析决策，依托区块链的智能合约进行流程管控、实时反馈、触发告警，生成双向追溯可靠的电子证据等。



2.2.5 通信设备资产管理

场景：使用区块链技术为电信设备资产管理提供设备信息上链、设备溯源等功能。并将区块链服务部署在边缘计算节点服务器上，无需另外提供区块链服务器，即可提供通信设备的存证、溯源等能力，为运营商的设备资产提供全生命周期管理服务。

需求：电信设备资产主要包括传输线路、基站设备及配套、直放站室分及WLAN、铁塔及天馈、业务系统支撑设备、测试设备等。运营商在日常的电信设备资产管理过程中，比如日常的设备安装、使用、外部借用等场景，经常会遇到设备丢失、设备出现故障却无法追责等问题，给运营商带来了不少损失。

方案：将基于区块链的通信设备管理系统部署在边缘计算节点上，为通信设备的管理提供设备登记、设备检索、可视化展现等功能。对通信设备信息数据，可以采用统一的数据结构，将其保存在区块链中。区块链链中的设备信息在全网节点中进行共享，便于使用及对设备信息进行统计、查询等。

针对已有现存的设备资产管理系统，则可以通过接口方式与区块链设备资产管理系统进行对接。区块链管理系统通过接口与通信设备的管理系统进行交互，获取现网设备的各类状态数据，并可以做到实时更新设备信息。如果没有现存的设备管理系统，则由区块链设备资产管理系统提供对电信设备资产信息进行录入、修改、可视化展现等功能。有些设备如基站、空调、交换机等在设备入仓后，可在设备外壳粘贴或嵌入条形码、二维码等标识，利用移动终端扫描或近场通讯技术进行识别。每次设备检修、更换时，可以通过终端 APP 扫描二维码进行状态信息的录入。运营商在进行设备管理时，要求所有设备发生状态变化都需要登记信息，且信息都保存在区块链上，以备追溯。



2.2.6 通信设备巡检

场景: 在边缘计算节点服务器上部署区块链服务, 为设备巡检提供数据采集、信息登记、数据存证、设备查询、可视化展现等功能, 提供巡检数据的全程可追溯能力, 保证巡检结果真实可靠。还可以针对巡检的数据进行数据分析, 为运营商提供巡检数据的管理服务, 从而提高巡检质量和效率。

需求: 在运营商日常通信设备巡检场景中, 巡检耗时长, 效率低, 成本高, 电信设备数量多、种类多、厂家多、批次多, 且巡检工作外包给第三方公司也会有信息造假情况出现。

数据采集可分为人工巡检和自动巡检两种方式。人工巡检是指运维人员前往巡检现场进行巡检数据的采集, 巡检信息由人工登记上传至区块链巡检管理系统。自动巡检, 一部分数据是来自巡检现场安装相应的传感设备, 这些感知设备可对巡检指标数据进行自动采集与上传; 另一部分数据, 可以来自现网的网管平台, 通过巡检管理系统与网管平台接口与进行交互, 获取部分设备的巡检数据。自动巡检的方式能够有效降低人工巡检的成本, 并能杜绝人工巡检工作中的造假现象。通过自动巡检, 能够极大的提升巡检效率, 尤其是对一些偏远地区, 人工进行巡检的成本比较高, 自动巡检则无需运维人员赶赴设备现场, 便可以完成巡检任务。

方案: 保存人工巡检或自动巡检过程采集到的各种巡检数据, 同时将其哈希值保存到区块链中, 保证数据的准确性。集团公司及省公司或地市公司, 通过该巡检管理系统查询巡检结果。

将区块链巡检系统部署在边缘计算服务器上, 可以利用边缘节点资源; 涉及多地区的巡检数据上链时, 可以很方便地与集团公司、省公司形成多节点架构, 比如集团公司、省公司节点部署在运营商云计算平台上, 地市节点可以就近部署在边缘计算平台上。



2.2.7 通信设备的运维管理

场景：在边缘计算节点服务器上部署区块链服务，可以方便地收集设备的操作日志、告警和性能等数据，将这些数据或数据的哈希值传输至区块链上来提供存证业务，上链后数据具备高度可靠、无法篡改、强安全、时序不可逆等特点，并可以实现数据的全程可追溯，让运营商准确地评估网络运行质量。

需求：通信设备的操作日志、告警和性能等数据对网络的维护和评估十分重要，为了满足考核管理要求，日常运维过程中难免存在重要故障瞒报和误报等情况，甚至还存在修改和伪造数据的情况，但有时候问题和责任却难以追溯，导致网络维护人员无法对网络质量做到正确的评估。

方案：将基于区块链的运维管理系统部署在边缘计算节点上，可以根据需要将网元数据、网管数据上传到区块链链上进行保存，实现可信存证管理。

比如针对操作日志，可以将操作人的姓名，工号，IP 地址，操作时间，甚至 GPS 地址信息等数据上链，或者把这些数据的哈希值传输到区块链上，该哈希值可以理解为这个操作动作的唯一 ID，以实现高度可靠的操作存证，可供后续查询和追溯。

针对告警、性能等数据，可以选择将关键告警信息和性能指标数据上链，或者把这些数据的哈希值上传到区块链上，以实现高度可靠的数据存储，可供后续查询和追溯。

基于区块链的通信设备运维管理方案可以解决电子数据的“易变性、易改无痕性”等固有缺陷，让通信设备的日志记录、告警记录、性能指标等数据，实现可证明，可追溯，可信赖，进一步提升了电信级产品的可靠性和可用性。基于区块链的运维管理系统，部署在边缘计算服务器上，相比部署在物理机服务器上，其优势是节约物理空间和易于形成云、边共同部署的架构。



2.3 安全类应用：区块链提供边缘计算安全增强

2.3.1 终端设备认证

场景：构建基于区块链的身份认证系统，服务于物联网终端设备认证。设备生产商可直接将设备的身份信息写入区块链，不再依赖 CA，提高效率。通过区块链的多点数据同步防篡改特性提高设备身份的安全性。

需求：边缘节点上的物联网应用接入大量的物联网终端，物联网终端和边缘计算应用之间需要建立双向认证，以保证系统及物联采集数据来源的双向身份安全。基于 PKI 的身份认证体系是目前常用的身份认证方式，但它存在一定缺点：集中化的数字证书认证中心 CA 一旦遭受安全攻击或自身出现故障，会影响到证书用户。用户证书只能由所属根证书进行验证，不同 CA 之间不能相互认证，针对此问题的交叉认证等解决方案目前都存在一定的局限性^[4]。

方案：物联网设备出厂时，产生公私钥和自签名数字证书，由生产商写入设备，并向区块链身份认证系统提交发布申请。区块链身份认证系统对证书检查后，将证书记录到区块链中。边缘计算物联网应用同样将其证书登记到区块链中。

物联网终端和边缘计算应用之间需要建立连接时，物联网终端向边缘计算应用发送证书标识，边缘计算应用向区块链身份认证系统查询证书，身份认证系统返回证书及状态，边缘计算应用对设备进行认证，物联网设备以同样方式对边缘计算应用进行认证。之后两者继续进行 TLS 握手流程，建立安全的数据传送通道。

2.3.2 IT/CT 域互信

场景：IT/CT 参与方加入到区块链，利用区块链数据不可篡改的特点，对交



互信息、执行信息进行监督,使得媒体流转移流通过程更加公开透明和真实可信,进而满足 IT、CT 之间的安全、追溯、结算的互信要求。

需求: MEC 采用本地数据分流的方式就近处理业务,它集成了 CT 和 IT 域功能,同时连接本地网/园区网 IT 域,带来了 CT 云和 IT 云之间的安全及互信问题。目前通常是在 IT 与 CT 域之间部署防火墙,在网络连接层面解决分流策略安全以及接口安全等典型问题,但是互信及结算问题实际还没有真正解决。

方案: 部署在边缘计算节点上的 UPF/GW-U/本地分流网关等 CT 域实体,及部署在边缘计算平台上的 IT 应用通过区块链节点加入到区块链网络中。当两者发生交互时,在信令面上,例如 IT 应用向 CT 域实体发起路由策略、网络能力数据请求时,CT 域实体执行后将操作记录上链存储,作为存证;在用户面上,CT 域将其与特定 IT 应用之间的数据收发统计数据上链存储,用于电信运营商与 IT 应用提供商之间的计费结算。

2.3.3 应用、配置的完整性

场景: 借助于区块链,将校验码发布于区块链,当软件、配置、通信加载启动时进行验证。

- **版本安全:** 确保 APP 版本加载与运行时不被篡改。防止第三方 APP 在分发环节中被植入木马、僵尸病毒等,同时 MEC 平台的设备安全补丁、安全配置基线、虚拟机/容器镜像等,也需保证完整性并防篡改;设备商、ISP 与运营商建立联盟链,推送版本给客户时,通过区块链保证版本分发、传输过程的可信;
- **流量通信安全:** 利用 APP 唯一特征建立互信关系,只有具备相互信任关系的 APP 与 APP 间、APP 和 MEC 平台间等才允许通信和流量交互;
- **重要记录保存:** APP 的关键配置、操作日志等信息不可篡改,支持安全审计和举证;



- 业务敏感信息：对诸如 MEC 业务转发策略、业务话单、流量镜像等数据进行完整性保护；
- 终端接入认证：应用终端用户接入数据网络时的数据网络认证对终端芯片和系统均有特定要求。可以通过对终端用户与数据网络信息上链进行认证，以确保用户与数据网络之间的互信。

需求：边缘计算节点会承载大量的非电信类应用和 UPF 等电信应用；重要的垂直行业和工业互联网要求高安全性；设备商及软件开发商在发布版本时，需要保证软件版本的完整性，以防止在软件包在发布、分发或传递过程中被篡改、植入木马或病毒等；当前的解决方案是进行数字签名，通过 CA 完成，但 CA 管理流程较为复杂。MEC 需要赋能应用及配置信息安全^[5]。

方案：该业务场景下，将应用软件及镜像、业务敏感配置信息等通过设置，上传区块链系统，存储在不可篡改区块链上，可供获取、查询、追溯等；系统间的交互通过设置上链进行可信认证。

3 区块链+边缘计算的技术实践

一方面，区块链应用为 MEC 系统赋能信任和安全，另一方面，把更靠近用户的 MEC 系统作为区块链业务的承载平台为用户带来更高效快捷的业务体验。

本章首先给出边缘计算+区块链的不同服务模式和系统架构，再分析如何提供更合理的融合部署方式。

3.1 区块链+边缘计算的服务模式

IaaS、PaaS 和 SaaS 是云计算的三种服务模式。三种模式针对不同使用领域，提供不同等级的服务。SaaS（软件即服务），提供给客户的服务是运营商运行在

云计算基础设施上的应用程序；PaaS（平台即服务），提供给消费者的服务是开发语言、工具及组件服务等平台能力；IaaS（基础设施即服务），提供给消费者的服务是对所有计算基础设施的利用，包括处理 CPU、内存、存储、网络和其它基本的计算资源。

从将区块链引入 MEC 平台的视角，边缘计算融合区块链的服务方式也可按照这三种服务模式规划：

- **IaaS 服务模式：**边缘计算部署的多地分布式 ICT 云，可以为区块链提供分布式、去中心化的资源供给，便于区块链的快速部署；
- **PaaS 服务模式：**区块链也可以以服务的模式，集成在基于 PaaS 架构的 MEP 平台上，提供 API 供边缘计算 APP 的调用，即 PaaS 服务提供方式的模式服务；
- **SaaS 服务模式：**区块链可以以 SaaS 模式，提供应用级的服务，直接提供数据存证等应用服务。

通过区块链和 MEC 的三种服务模式上的深度融合，使得两者均可发挥其最大作用，相得益彰，相互赋能。MEC 和区块链融合架构示意图如下：

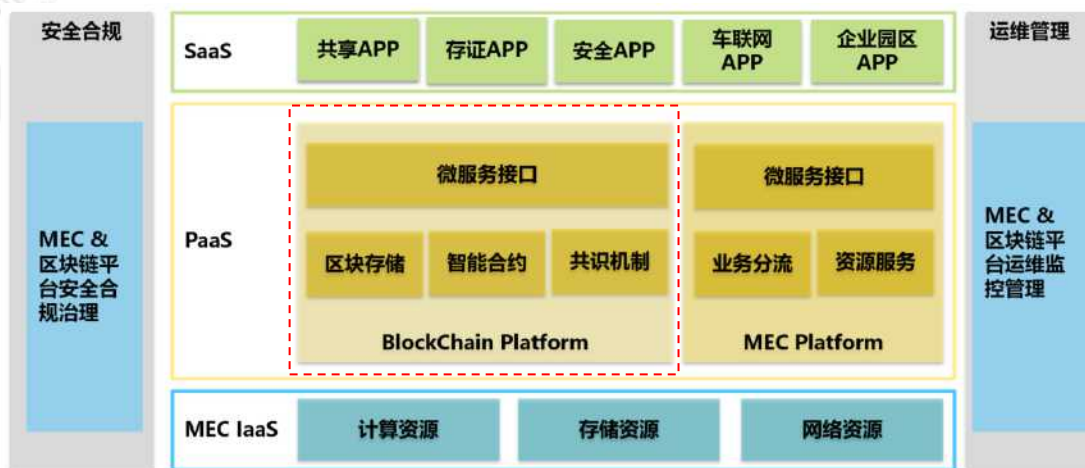


图 3-1 MEC 和区块链融合架构

如上图所示，整个系统分为三个层次，按服务模式做模块耦合：

- **MEC IaaS 层：**位于最底层，负责计算、存储、网络资源的分配和调度，也可为外部区块链系统提供服务器资源；
- **PaaS 层：**该层中 MEC 平台提供网络及业务能力，区块链平台提供区块

链核心支持功能：块存储、智能合约和共识机制，丰富完善了 MEC 能力，通过能力开放框架，共同为上层电信级 APP 和第三方 APP 提供使能服务。而在资源层面，区块链平台所需资源受统一调度分配。

- SaaS 层：是整个系统对外提供的应用服务能力。应用也可使用部署在边缘计算节点资源池外部的区块链。

纵向贯通的是安全合规、运维监控管理和运维管理；前两者负责整个 MEC 和区块链平台的统一部署和管理，为融合系统安全平稳的运行保驾护航；后者实现资源池的统一管理和监控。

3.2 区块链+边缘计算的部署方式

3.2.1 边缘计算部署现状及与区块链融合部署

当前，区块链系统通常作为一个 IT 应用系统，位于 IT 的应用侧，部署在企业局域网和互联网上。典型部署图如下图所示。

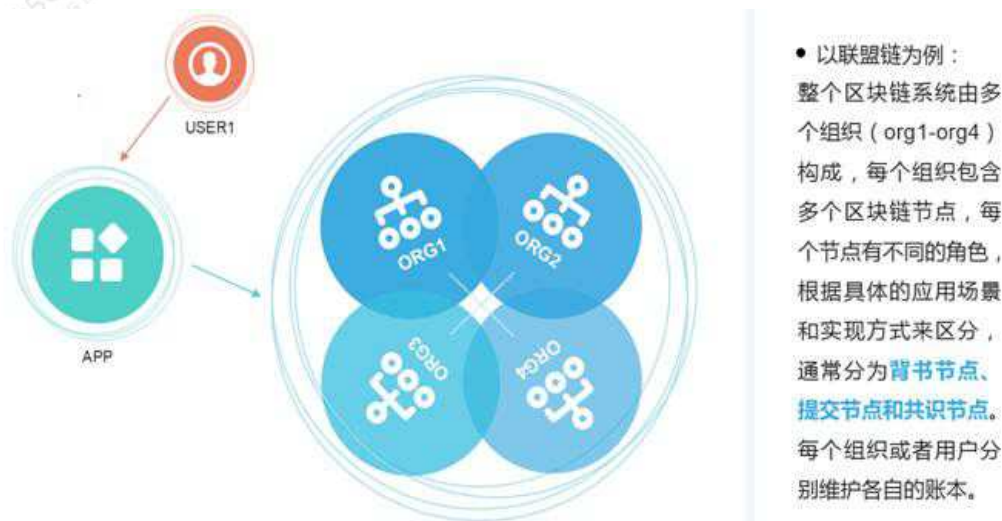


图 3-2 区块链部署现状图

MEC 一般部署在运营商网络的接入层和汇聚层，它采用虚拟化架构，支持通过虚拟机/容器方式灵活加载软件。MEC 提供了运营商的用户面功能用于本地分流数据能力，及其它多种有线和无线接入能力，可以部署多种边缘特色应用。除了对运营商网络的增强，MEC 也常常服务于企业、园区等本地网络。MEC 部

署位置处于 CT 域的边缘，其典型部署图如下图所示。

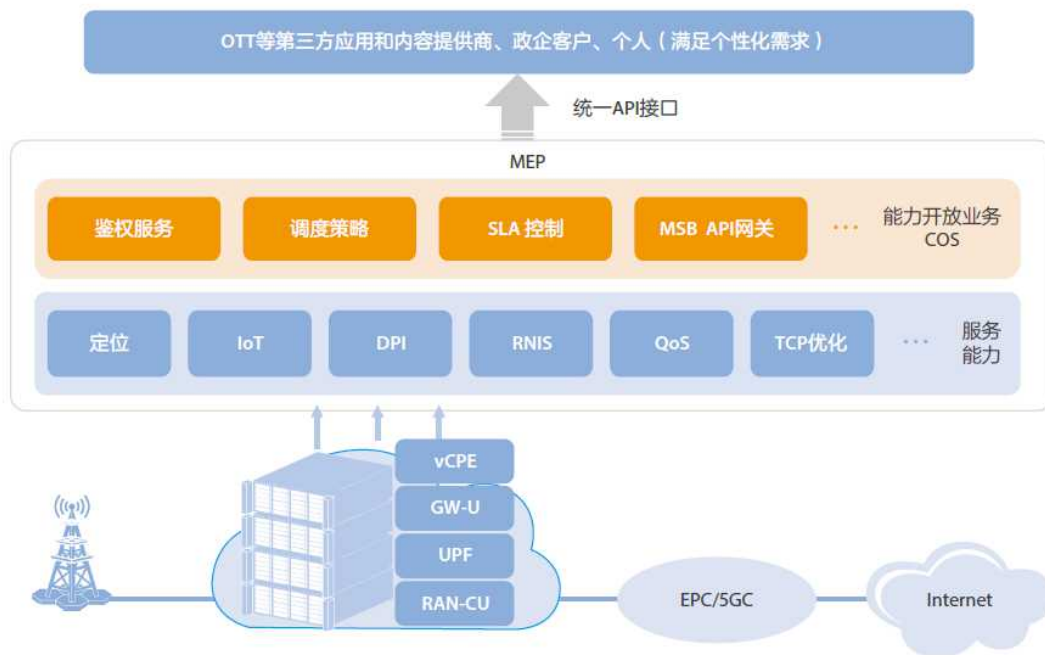


图 3-3 MEC 部署图

从区块链系统是否部署在 MEC 资源池上这一视角来看，MEC 和区块链的融合可有三种部署模式：On MEC（区块链部署在 MEC 资源池内）、Off MEC（区块链部署在 MEC 资源池外）和 Hybrid MEC（混合部署）。On MEC 是指区块链系统各个节点全部部署到 MEC 提供的资源池上，赋能 MEC 且通过 MEC 对外提供服务和应用。Off MEC 是指区块链系统各个节点部署到企业私有云、公有云上，使用的资源和 MEC 无关，由区块链系统提供服务、应用接口供 MEC 应用使用，从而赋能 MEC。Hybrid MEC 则是融合了 On MEC 和 Off MEC 两个方式，部分区块链节点部署到 MEC 节点上，其他部分区块链节点部署到企业私有云或公有云上，形成一种混合组网的模式。部署方式的选择主要看行业用户的业务需求和已有部署条件。

3.2.2 On MEC--区块链部署在 MEC 资源池内

MEC 把电信网络和互联网有效融合在一起，在网络边缘提供计算和网络能力，应用服务和内容部署在本地边缘，可以减少数据传输环节，提高数据安全性，

降低端到端时延，减少带宽占用，并降低功耗。对数据安全及时延等要求高的行业用户应会自购使用 MEC 来提升用户体验；在引入区块链应用时，可以首选考虑把区块链随同部署到已有 MEC 上。

所有 MEC 节点均位于同一个 SP 的网络中，所有区块链节点均部署到 MEC 提供的资源中并维护账本。每个应用 APP(例如存证 APP)直接访问就近的 MEC 提供的区块链服务，从而完成相应的区块链应用。区块链节点之间通过边缘计算节点或边缘云提供通路实现互联，完成账本数据的同步、共识机制的达成。



图 3-4 ON MEC 部署模式

3.2.3 Off MEC--区块链部署在 MEC 资源池外

此场景与传统区块链系统的部署类似，但是需要打通与 MEC 平台之间的业务通道。由于没有充分利用 MEC 靠近用户的优势，所以适用于轻量业务的场景中。该部署模式是 MEC 和区块链应用融合部署的一个补充。部署到公网或私网的区块链系统为 MEC 上应用提供区块链能力和服务，而区块账本的同步，借助公网或私网的通道来实现。

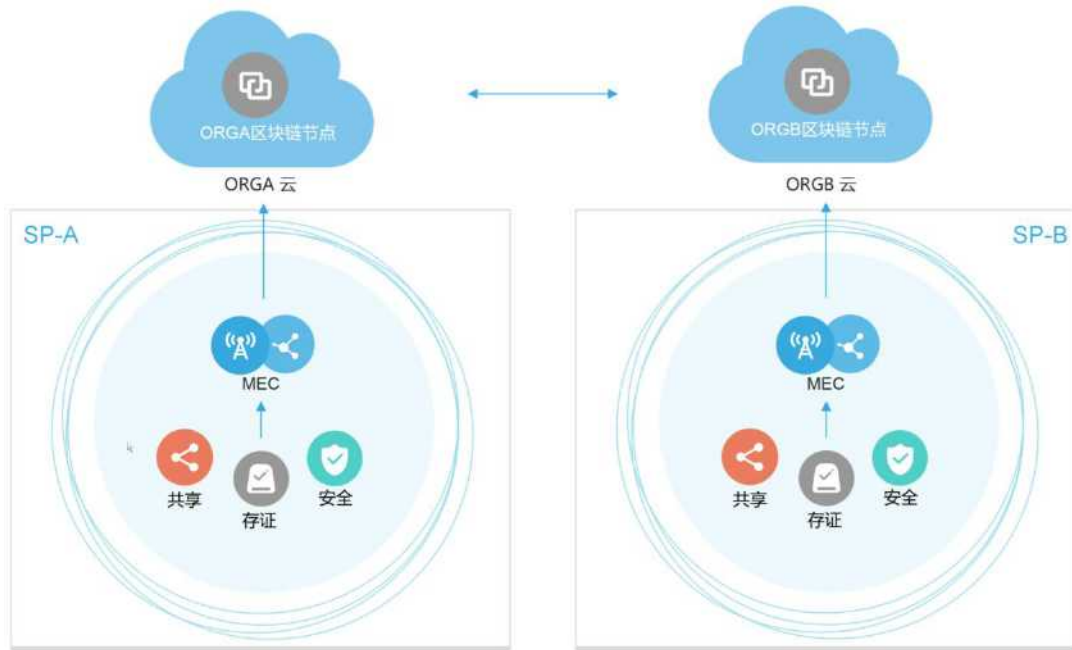


图 3-5 OFF MEC 部署模式

3.2.4 Hybrid MEC--混合部署

部分区块链节点部署在多个边缘计算节点上，同时由于业务需要，在组织所属的公网/私网中，也需要部署对应的区块链节点，通过云边协同，实现混合模式的区块链应用。

这种模式通过方便灵活的组网方式，极大的拓展了区块链+MEC 部署的应用场景，能够覆盖现阶段各类区块链业务在边缘计算节点上的部署。

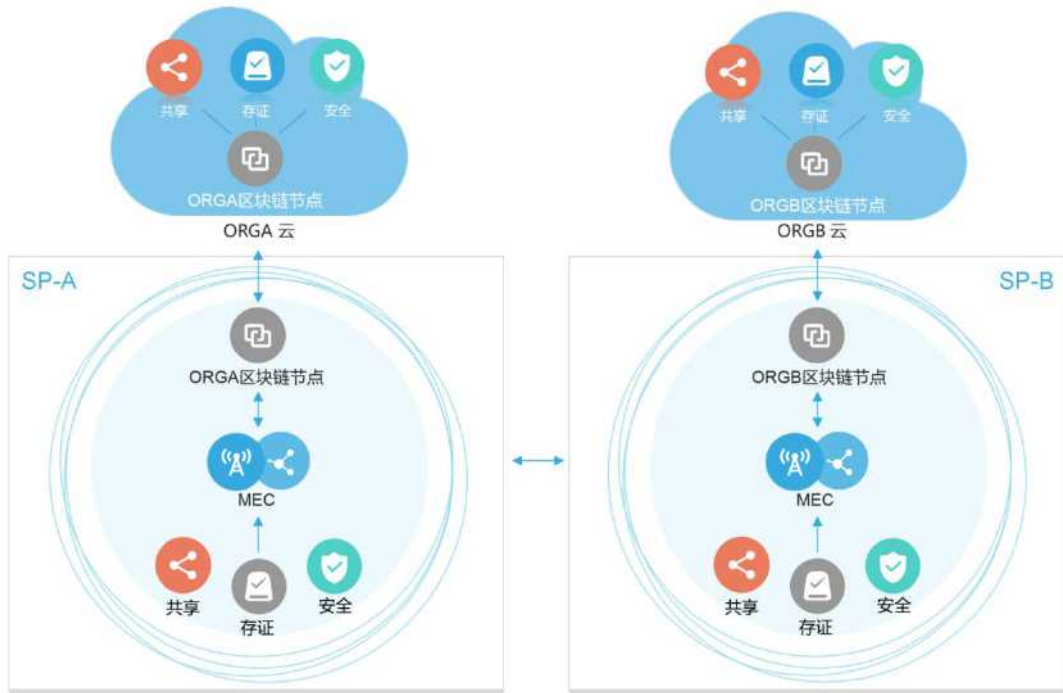


图 3-6 混合模式组网部署图

4 边缘计算+区块链的发展展望

4.1 面临的挑战

边缘计算与区块链的结合是一个全新的交叉领域，其大规模应用之前还面临如下挑战：

- 技术成熟度尚待提升：
 - 当前，全球运营商、主流设备商正在研发和部署基于 5G SA 架构的边缘计算和边缘云，针对垂直行业的应用尚处于技术验证、试点试用阶段；
 - 区块链技术虽然经历了近十年的发展，但尚未达到与数据库、文件系统等传统技术类似的成熟度；
 - 边缘应用和区块链应用开发工程师不足，其交叉领域的人才更是稀缺；
- 资源开销尚待降低：
 - 作为分布式处理系统，由于增加了分布式账本和共识机制，区块链相对于分布式数据库存在通信和处理资源消耗较大、并发事务处理能力较



弱；

- 下沉位置较低的边缘节点通常资源受限情况比较严重，因此，需要考虑针对边缘计算场景对区块链平台进行必要的裁剪和优化；
- 区块链技术的时延是否能满足或影响边缘计算的时延要求尚待试用和优化。

- 应用场景尚待拓展：

- 本白皮书所描述的场景聚焦共享、存证、安全等领域，还有大量的典型业务场景需要不断探索、业务领域还需要不断扩展；
- 垂直行业对区块链+边缘计算的融合场景尚无普遍、直观认知，需要通过典型场景、示范应用获取客户的认可。

- 安全威胁有待解决：

- 区块链安全威胁既包括传统安全威胁也包括非传统安全威胁，涉及信息安全、数据出境、隐私管理等领域；不仅面临后门植入、DDoS 攻击、网站钓鱼等传统网络安全威胁，还面临共识算法攻击、“女巫”攻击、分叉等区块链特有的安全威胁^[6]。

4.2 发展畅想

随着社会经济发展和产业结构转型，跨组织、跨国家、跨行业的社会协作必将不断密切化，区块链作为“价值互联网”的载体，必将在社会经济发展中起到越来越重要的作用。

运营商联合通信产业面向垂直行业推出的边缘计算新特性，将吸引诸多对业务质量和数据安全有更高要求的垂直行业应用。

边缘计算和区块链两种技术的有机结合，将为多个垂直行业之间可信、高效协作打好基础：边缘计算、网络切片等新网络功能仅满足了特定行业用户自身的业务需求，将区块链引入运营商网络并与边缘计算技术配合，将帮助已经使用这些新功能的节点之间加强协作，实现信息、资源、生产要素的协作共享，促进生产关系的优化和生产力的解放，促进全社会多个产业的协同发展，切实履行通信



产业“5G 改变社会”的愿景。

让我们携手，共同加速区块链与边缘计算的深度融合，为优化社会资源、提升社会协作水平、促进经济发展和社会进步做出贡献！





缩略语

缩略语	英文全称	中文含义
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G	5th Generation	第五代（移动通信网络）
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
APP	Application	应用程序
BaaS	Blockchain as Service	区块链即服务
CA	Certificate Authority	证书颁发机构
CT	Communication Technology	通信技术
DC	Data Center	数据中心
FPGA	Field Programmable Gate Array	现场可编程门阵列
GPU	Graphics Processing Unit	图形处理器
GW-U	Gateway User	用户面网关
ISP	Internet Service Provider	互联网服务提供商
IT	Information Technology	信息技术
MEC	Multi-access Edge Computing	多接入边缘计算
QoS	Quality of Service	服务质量
SP	Service Provider	服务提供商
TLS	Transport Layer Security	传输层安全协议
UPF	User Plane Function	用户面功能
WLAN	Wireless Local Area Network	无线局域网



参考文献

- [1] ITU-R M.2083-0. IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond
- [2] 中国移动边缘计算技术白皮书, 中国移动
- [3] MEC 行业应用白皮书 (2018 年), SDN/NFV 产业联盟
- [4] 基于区块链的数字证书管理技术研究, CCSA TC8WG1
- [5] 边缘计算安全白皮书, 边缘计算产业联盟与工业互联网产业联盟
- [6] ITU-T X.1401 Security Threats to Distributed Ledger Technology



联合编写单位及作者

中国移动通信有限公司研究院：

中国移动研究院何申、陆璐、李征、杨波、王珂、耿亮、杭小勇、阎军智、郭义华、刘福文

中兴通讯：

郭海生、郑锦荣、王海峰、朱堃、杨春建、王德政、林兆骥、章坚、张再军、周晶、张强、高洪、法润容

区块链技术与数据安全工业和信息化部重点实验室

潘妍、李卫、李磊、余宇舟

北京大学新一代信息技术研究院

董宁



关于中国移动 5G 联合创新中心

2016年2月，中国移动5G联合创新中心（以下简称“5G联创中心”）成立，旨在4G向5G演进过程中，联合合作伙伴共同推进5G基础通信能力成熟，孵化融合创新应用和产品，构建合作共赢的跨行业融合生态。5G联创中心聚焦基础通信能力、智能交通、视频娱乐、工业能源、智慧城市、教育、医疗、农业、金融等领域，与合作伙伴开展联合创新项目，并在国内外构建区域开放实验室，提供基础通信实验、业务开放实验、成熟度测试认证、用户分析及体验四大能力。截至2020年5月，已有695家合作伙伴加入，其中垂直行业合作伙伴达到589家，在北京、上海、浙江等地构建22个境内实验室，在美国（硅谷）、香港、瑞典（斯德哥尔摩）构建3个境外实验室，并成立多媒体创新联盟、自动驾驶联盟、飞联网联盟、智能城市联盟、5G能源互联网联盟、精准定位联盟推动5G在垂直行业的广泛应用。

中国移动 5G 联合创新中心

网址：www.hc.10086.cn/5gic/index.html

联系我们：admin@cmcc-5gic.org







Copyright© 2018 中国移动 5G 联合创新中心版权所有

您可以为内部参考的目的引用本文件。本文件未授予任何其他许可。

本文件“按原样”提供，不作任何明示或暗示的保证。任何保证均明确予以否认，包括但不限于不侵权、商用性以及特定目的适用性的保证。中国移动 5G 联合创新中心不负责保证所呈现信息的精确性。本文件提供的任何信息可能会被纠正、修改和改变，恕不另行通知。使用或信赖本文件所提供信息的风险自行承担。本文件提供的所有关于第三方的信息均来源于公开资源或他们发布的报告和报表。

转载、摘编或利用其它方式使用本报告，请注明来源“中国移动 5G 联合创新中心”。违反上述声明者，我们将保留追究其相关法律责任权利。



中国移动5G联合创新中心
China Mobile 5G Innovation Center

