

10.0F

面向6G的联盟网络体系 架构白皮书



目录

摘要	2
本白皮书所涉主要名词注释	3
一、 面向 6G 的网络新生态理念	4
1. 6G 生态价值要素	4
2. 6G 生态融合趋势	5
3. 联盟网络生态构想	6
二、 联盟网络典型场景和应用	8
1. 典型场景	8
2. 典型应用和服务	9
3. 新型商业模式构想	10
三、 联盟网络设计理念	12
1. 网络自主	12
2. 服务关系灵活化	12
3. 分布式协同和共享	13
4. 多方可信与安全隐私	13
5. 智能化自动运行	14
四、 联盟网络体系架构	15
1. 体系架构概述	15
2. 主体网络层	15
3. 互联互通层	16
4. 联盟应用层	18
5. 联盟权益管控	18
6. 联盟可信保障	18
五、 相关关键技术	20
1. 自主数字身份	20
2. 分布式服务管理	22
3. 权益管理	24
4. 多方共识可信	25
5. AI 赋能网络自智	27
6. 其他技术	27
六、 总结与展望	32
白皮书中所涉英文缩写表	33

摘要

随着 5G 网络的全面建设和应用，移动通信网络已经在众多民生和垂直行业领域取得了显著成果，展现出了巨大的商业和社会价值。6G 将在 5G 的基础上进一步扩展与信息消费、实体经济、民生服务等多个领域的更深层次融合，实现从为终端用户服务为主，转向为全产业链生态的服务。6G 新网络将成为 ODICT 技术融合的综合平台，覆盖空天地一体和通感算智信等业务服务。

在未来多元化的新价值驱动下，各行业原有的商业运营模式将不断经历重塑和试验性创新，以适应不断变化的生态需求。这将促进生态体系的重组和更新迭代，最终形成融合革新的生态体系。传统的“中心化”和“通用性”的网络设计和运行范式将难以满足未来生态体系的各种需求。本白皮书提出“联盟网络”体系生态，是一种通过多个网络的协作实现资源和服务的流通的体系架构，由多个主体网络组成，其参与主体可以是个人、家庭、政企、运营商等，各主体通过联盟网络实现多方共识信任和权益保障，从而使得主体网络之间可以进行资源和服务的灵活共享和交易。

本白皮书主要由六部分组成，分别为网络新生态理念、典型场景和应用、设计理念、体系架构、相关关键技术和总结展望。第一章从 6G 生态的价值要素及融合趋势出发，提出联盟网络的生态构想。第二章从个人及家庭网络、政企及行业网络和空天地一体化网络三个典型应用场景，对联盟网络的典型应用及收益和潜在新型商业模式进行阐述。第三章根据联盟网络新生态理念对联盟网络新型网络模式的典型特征进行了描述。第四章提出了三横两纵的联盟网络体系架构。第五章对联盟网络体系架构的关键技术进行了阐述。最后第六章对全文进行总结，展望未来发展。

本白皮书所涉主要名词注释

名称	定义
网络主体/主体	指参与到联盟网络各类型活动中的各类型的网络或者终端设备的所有者（例如运营商作为一种主体，或者行业、企业、家庭、个人作为不同类型的主体），在联盟网络中，通常将主体所对应的在联盟中的身份作为主体的标识。通常所有者可以对应到法人，例如运营商，企业或者个人，或者具有法人意义的联盟（例如车联网联盟）。
主体网络/网络	指运营商、行业、企业、家庭或者个人具有所有权的网络（可以是运营商网络、行业网络、企业网络、家庭网络或者个人网络）。
联盟网络	指由多个（分布式自治的）主体网络之间（在多方共识信任的基础上）通过特定的协议（例如服务注册、发现）相互连接所形成的跨行业生态的网络系统。这个系统允许各种类型的网络主体之间进行资源和服务的灵活共享和交易。

一、面向 6G 的网络新生态理念

传统电信级网络以“运营商”为主导，连接电信设备商、终端厂商等生态伙伴，创造价值。随着 5G 在信息消费、实体经济、民生服务等多个领域的融合应用，通信网络的角色从主要为手机终端用户服务逐步升级，转向为全行业乃至全产业链生态服务。随着 6G 新网络的到来，将进一步成为 ODICT（Operation Data Information Communication Technology，运营数据信息通信技术）技术融合的综合平台，覆盖空天地海，并提供通感算智信业务服务。6G 时代将从 5G 技术的融合探索应用转变为产业生态融合的时代。

1. 6G 生态价值要素

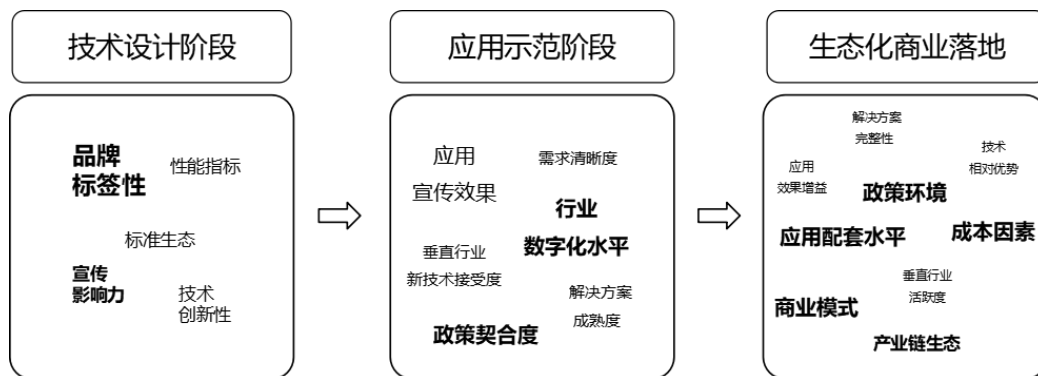


图 1-1 通信网络阶段性关键价值要素

随着 ODICT 在行业应用的深入，通信技术应用效果的决定要素愈发多维，从对通信性能的单一要求发展为受多方面制约的多维要素，包括生态环境、政策、整体解决方案等。这些影响因素涵盖了各行业上下游产业链、外部环境等多个层面。如图 1-1 所示，ODICT 技术融合到各行各业的过程可分为技术设计、应用示范和生态化商业落地三个阶段。不同阶段的价值和发展要素也各有不同。在技术设计阶段，主要价值和发展要素包括技术的客观性能指标、标准生态以及技术创新性等。同时，对外宣传的影响力和品牌的标签性也十分重要。在应用示范阶段，随着技术深入到各行业领域应用中，行业自身的数字化水平、整体解决方案的成熟度以及应用企业对新技术的接受度等将直接影响融合应用的效果。一旦应用示范得到充分验证，进入生态化商业落地阶段，利润率、成本因素、商业模式、运营模式等整体产业生态环境因素将变得更为重要。若无法建立良好的商业模式落地，就很难维持和发展生态系统。同时，此阶段也将直接体现 6G 对国家政策和社会民生的支撑作用。

目前，5G 技术在众多行业应用中进行了深入的示范探索，部分项目已经进入规模化落地阶段。随着行业应用的深入扩展，6G 将更多地面临应用生态化商业落地的需求，承担更多责任，并为信息消费、实体经济、民生服务等诸多领域的各个行业提供支撑服务。未来，6G 技术在适应性、演进性、商业模式、绿色发展等方面都面临着挑战，这也意味着 6G 网络的价值和发展要素正在不断多元化，这些要素不仅反映了 6G 的关键挑战，同时也是决定 6G 网络应用效果关键的价值要素。

2. 6G 生态融合趋势

在 ODICT 融合应用的探索初期的技术设计阶段，通常从各项技术本身特点出发，设计或寻找应用场景，主要使用技术性能通信指标 KPI（Key Performance Indicator，关键性能指标）来评估网络应用效果，应用效果类似的不同技术之间多为竞争关系。随着新应用场景的探索发掘，并经历了一段时期的应用示范后，融合应用的重心逐步转移至规模化商业落地，从潜力应用到商业落地的过程中，适配性、成本、易用性等偏主观 KVI（Key Value Indicator，关键价值指标）和各行业、领域的法规、标准、新商业模式、产业链生态重组等面向产业生态的 KDI（Key Development Indicator，关键发展指标）因素重要性逐步凸显，各技术间的竞争不仅在于技术指标，逐步变成了整体应用效果及成本收益的综合取舍。未来 6G 时代将从技术的替代及融合转向技术生态的替代及融合。

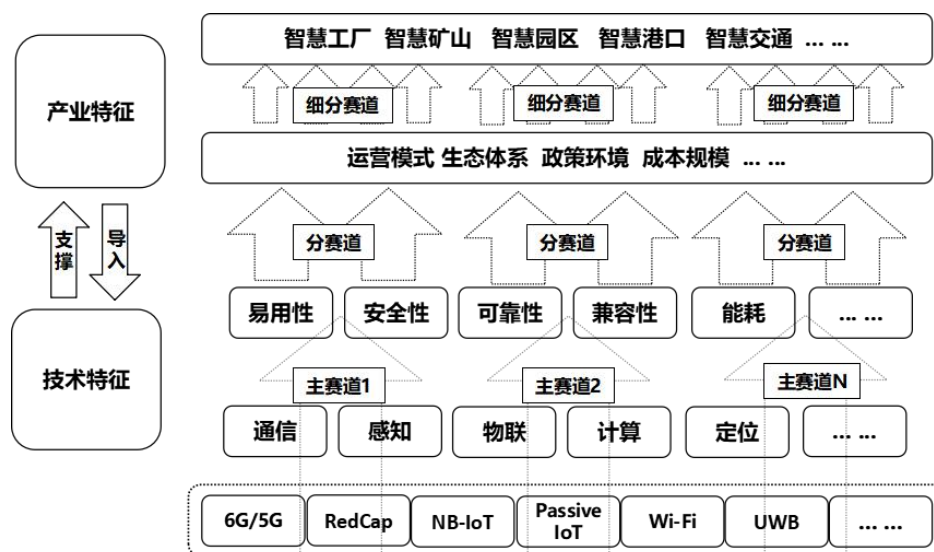


图 1-2 6G 时代的融合生态

如图 1-2 所示，6G/5G、RedCap、NB-IoT，Passive IoT 在设计规划时在传统

通信、感知、物联、定位等场景有着不同的侧重点，在不同赛道各司其职。而技术的最终落地则需要从技术特性（易用性、安全性、可靠性、兼容性、能耗、成本等 KVI 指标）及产业特性（运营模式、生态体系、政策因素等 KDI 指标）来综合选取，最终的应用场景可能会拆分为多条细分赛道，而每一个技术

（Passive-IoT、RedCap、5G、Wi-Fi、UWB），根据自身技术及生态特点，最终可能会达到某种平衡，各自占领其中一个或几个赛道。未来应用有各类技术协同应用的趋势，而不是完全替代、纯粹竞争的关系，如某些技术在定位的主赛道为竞争关系，但在易用性、安全性、成本因素的差别，最终应用适配在不同的细分场景，最终共同形成了相关产业生态。此外，为了应对多样的行业应用需求，产业特征与技术特征也是互相作用的关系，技术特征源自产业特征的需求导入，而技术特征也为产业特征做支撑。

3. 联盟网络生态构想

可以看出，随着 5G 网络及 ODICT 融合技术的发展深入，未来 6G 网络面对的融合应用将从技术融合探索逐步转向为产业生态的融合重构，为了应对多样的行业应用需求，产业特征与技术特征也是互相作用的关系，技术特征源自产业特征的需求导入，而技术特征也为产业特征做支撑。同时，各行业也将共同找寻最适合的运营模式及商业模式，在不断的探索迭代中，最终形成新的可良性运转的融合生态。

而联盟网络的设计理念，则可以将多个主体网络，在多方共识信任的基础上，通过特定的协议（例如服务注册、发现）相互连接，形成跨行业生态的网络系统。这个系统允许各种类型的主体网络之间进行资源和服务的灵活共享和交易，从而得以体现联盟网络中各主体价值，并将各主体所处的生态进行有机结合，更适配各行业应用的多样的定制化需求。系统还可以进行更加灵活的商业模式、运营模式、定价模式的设计，使网络更适配未来发展中生态融合的趋势理念，让网络更好的服务应用于各行业领域，最终形成良性运转的生态环境。

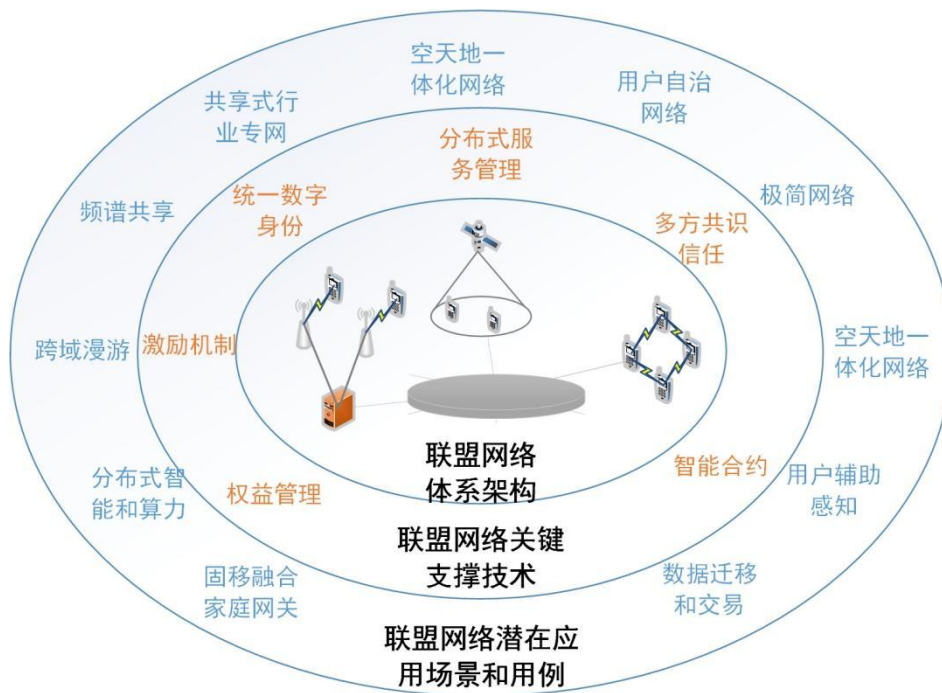


图 1-3 联盟网络白皮书架构

二、联盟网络典型场景和应用

联盟网络涵盖了个人、家庭、政府机构、企业和运营商等多种主体。这些主体能够将其网络资源整合入联盟网络中，实现互惠互利。一方面，各主体可以购买并使用联盟网络中其他主体提供的功能和服务；另一方面，也可以将所属网络资源提供给其他主体网络使用，并从中获得相应的收益。联盟网络为各主体可实现安全可信及权益保障的互联互通交易平台，在低成本获取功能及服务的同时增加变现能力，可以有机将各主体网络生态有机结合起来。

1. 典型场景

(1) 个人及家庭网络

在个人及家庭场景中，个人主体及家庭主体可以将个人网络或家庭网络加入到联盟网络中，极简形式的个人网络可以是单个终端设备产生的，如手机终端热点、个人低空飞行设备、智能网联汽车、网关设备等。可通过各类通信技术将运营商网络从基站扩展至个人及家庭网络中，是面向未来网络的一种高性价比的部署方案，可以充分利用个人及家庭设备潜力解决组网覆盖问题，加强终端通信能力。同时个人及家庭主体可通过联盟网络向其他主体出租个人及家庭网络中的网络资源获取对应的收益。

在联盟网络体系下，个人及家庭网络可以成为 6G 网络生态的一部分，在全域覆盖、泛在连接等方面发挥着重要作用。它不仅有效延伸了高频覆盖，还打造了一种终端轻资产网络化的新的网络共享生态。同时也为个人健康管理、智能家居、车联网等生态间融合应用搭建了新的桥梁。

(2) 政企及行业网络

对政企及行业主体而言，可将其所属的企业网络、园区网络或行业网络等纳入联盟网络体系中。举例来说，企业园区可以共享其部署的网络设备给运营商，并通过联盟网络租用运营商的网络频谱及购买网络运维服务。从而满足企业网络建设的隐私安全要求，将数据处理等任务留在本地，仅从运营商处购买所需的服务，降低企业网络运维成本。同时，企业也可以通过联盟网络，将计算、存储、数据等网络资源提供至其他网络使用，在降低了网络部署的成本和复杂度的同时，通过服务流转实现自身资源的最大化增值。

对于运营商而言，这种做法可以降低网络建设成本，并可以与行业专网结合，

为不同类型的企业提供定制化的高性价比解决方案。在联盟网络的体系下，网络之间形成了按需相互交易的创新模式，如转买为租，企业建立网络，运营商租用企业部分网络服务，企业网还可以代替运营商网络提供接入功能，这样可以减少网络受到的限制，提升垂直行业网络业务的成本回报速度，并扩展运营商网络的覆盖范围，双方的能力得以扩展，实现共赢。

(3) 空天地一体化网络

空天地一体化网络是未来较为重要的一种新型的网络架构，其中涉及不同地面运营商、卫星运营商、政企、个人等多个主体，在实际部署和实际运行方面，由于涉及多个利益相关方，各方的利益诉求和目标可能存在差异。通过联盟网络体系可更好地协调各方的利益关系，平衡各方需求，确保网络建设和运营的顺利进行。如卫星运营商 A 可通过联盟网络与卫星运营商 B 进行卫星网络资源的动态共享，当中低轨卫星在移动到不同国家时，可以被其他国家地面运营商 C、D 共享，通过联盟网络可实现国家间的平台共享，提供泛在连接等。并可根据需求提供针对性服务，如卫星仅作信号透传，满足其他国家地面运营商的数据安全需求等。

在空天地一体化网络的场景中，涉及到跨域、跨国、跨运营商间可信安全、权益保障，以及整个系统的成本控制、性能体验等多方面因素。联盟网络的体系架构十分适合用于解决多方跨主体的复杂业务场景，联盟网络通过去中心化的安全体系架构及权益保障机制，将各种类型的主体网络之间进行资源和服务的灵活共享和交易。从而将联盟网络中各主体价值得以体现，更适配复杂多样的定制化需求，并可以进行更加灵活的商业模式、运营模式、定价模式的设计。

2. 典型应用和服务

在联盟网络的生态体系中，各主体网络可将各自的资源以功能及服务形式提供给其他网络进行使用并获取收益，潜在可提供的功能及服务包括：

(1) 频谱、算力等资源租借

未来，面向虚拟和增强现实、8K 视频流、全息投影、智能家居、雾计算、集成人工智能服务、无人机和自动驾驶汽车等各类应用对频谱及算力等资源类需求将急剧上升，通过联盟网络可以提高频谱利用效率，并带来更多资源管理新方法的可能性。且通过权益体系，联盟网络还可以建立跨主体的信任合作环境，从

而实现动态的跨运营商频谱共享，同时利用加密和匿名化技术，联盟网络可以保护频谱共享参与者的隐私和共享数据的安全，并可通过算法在智能合约上实现最优的频谱分配等。

(2) 数据、模型等资源共享

随着人工智能的发展及应用，未来对于数据、模型等资源的共享需求逐步提升，不同于频谱、算力等可租借的资源，因涉及隐私、所属权、二次开发价值等内容，数据、大模型的权益保障体系更为复杂，传统的购买、租借模式无法最大化保证数据、模型提供者的权益，利用联盟网络，可以灵活制定数据、模型的迁移、共享及收益方式，此外，联盟网络可以引入合理的奖励机制来促进资源共享，从而提升联盟网络中各主体网络多种类型资源利用率及收益等。

(3) 跨主体接入切换等漫游服务

通过联盟网络，可以协调原本相互独立的主体网络，充分利用个人、家庭、政企、运营商的网络资源，实现泛在接入，并提供安全灵活的认证/授权设置，为用户提供更加便捷的跨主体网络的漫游访问，确保无线服务连续性，另一方面也能改变传统的静态协议，规范联盟网络内部各主体网络的行为，打造利益共同体，提高漫游协议的灵活度从而提升成本效益，实现联盟网络内安全的共享、共赢。

(4) 可信安全、权益保障等服务

除了各主体网络之间网络资源、能力的共享、租借、交易等模式外，联盟网络还可以通过其自身的体系架构为各主体提供可信安全、权益保障等系统平台服务。比如，为主体提供身份认证、隐私保护、资产确权、交易保障等服务，联盟网络可作为一个更加全面、安全和可信的平台，为各类主体提供了更广泛的支持和保障。

3. 新型商业模式构想

通过联盟网络的设计，未来网络的商业模式也有了更多的可能性，一些潜在的新商业模式可总结为以下几个方面：

①资产所有权模式变更。如从重资产到轻资产模式的转变，从购买实体产品到购买功能和服务的转变。在联盟网络的设计中，主体可根据自身的需求选取其他主体网络提供的网络功能及服务。联盟网络变成可提供多种服务模式的综合业

务平台，将各主体网络的能力资产化，可根据需求选取对应的网络应用模式，可能方式如：

- 基础功能交易模式：如基础连接、计算、存储服务、通信控制及执行等功能，包括寻呼、访问、移动性等。
- 平台服务交易模式：如行业应用运营、网络性能管理等、意图引擎、用例分析、智能决策、数据搜索、数据分析等。
- 系统交易级服务模式：如数字资产、区块链服务等。

②网络建设模式变更。在传统网络中，往往收到网络建设成本的限制，无法完全满足网络建设的个性化需求，而利用联盟网络，对于网络的部署建设运维方式可以非常灵活，可实现对需求的精准定位，并快速、精准且低成本地提供定制化服务。

③定价计费模式变更。利用联盟网络可信安全、权益保障等体系，综合上述两点中的极致定制化及服务类型选取，各网络间有望实现更有针对性的定价计费方式，包括租借、购买、按需、按量、按时等多种模式，从而让需求方以更低的成本获取对应的服务。

在联盟网络体系中，更多适配各领域、行业应用中多样化需求的新商业模式变为可能，这样的模式能够打造与未来多样网络需求特征相适配的商业运营模式及生态体系，这是联盟网络的重要价值之一。在适配的运营及商业模式下，网络能够更好地服务于各行业领域，从而形成良性运转的生态环境。

三、联盟网络设计理念

根据联盟网络的生态构想，可以将多个主体网络生态有机结合起来，通过网络间的协同，使网络资源和网络功能以服务的形式在网络间流转，扩展每个网络主体的服务范围，允许各种类型的主体网络之间进行资源和服务的灵活共享和交易，从而将联盟网络中各主体价值得以体现。联盟网络在不同的场景中面向行业应用多样的定制化需求，可以采用灵活的商业模式、运营模式、定价模式，但其都具备共同的特征，联盟网络的基本特征如下：

1. 网络自主

网络自主是联盟网络的基本要求。联盟网络中最基本单元是主体网络，功能组织方式便捷，有着自身特有的应用场景和需求。每个联盟成员都拥有独立的决策权和控制权，可以自主管理自己的资源和业务，而不受其他成员的影响，实现网络高效响应。每个成员都可以根据自己的需求和策略来管理和配置自己的网络，其基础设施规则、连接协议、服务化功能、开放能力均可按场景需求进行定制化设计，从而更好地适应不同的业务场景和需求。比如 ToB（To Business，面向商业）场景中，垂直行业可以根据自身具体要求，自主进行网络的建设和管理，实现完全自定义化。这种自主性有助于确保联盟网络的灵活性和可扩展性，使其能够适应不断变化的需求和环境。

2. 服务关系灵活化

服务关系灵活化是联盟网络的重要特点之一。一方面，联盟网络中的主体网络能力参差不齐，专一化、极简化网络需要其他网络提供的服务。另一方面，网络的通感、人工智能、算力等功能单纯通过自身无法实现最优化，需要边缘网络和终端的辅助才能实现。因此未来联盟网络中各主体间的服务关系将发生变化，不仅运营商大网可以作为服务提供者，网络中的各类主体都可以根据自身能力对外提供服务、获取收益。这将构建新的网络生态，意味着网络不止是一种消费，还有一种广泛产生生产力的基础设施，所有使用其他主体网络的主体都可以通过网络完成生产、消费。在基建角度，除运营商外的各类主体可以在获得许可的情况下在授权频段自费建设通信设施，终端用户可以通过此类通信设施接入网络，运营商租用或者授权其他主体运营通信设施，其他主体通过租金和服务分成获得

收入。在服务角度，各类主体可以为运营商提供计算任务的卸载、AI（Artificial Intelligence）学习的辅助、周围感知的提供等服务，运营商为服务进行付费。在数据角度，各类主体可以通过出售或出租自身持有的数字资产获得收益。一方面，主体可以通过协助运营商获得收益。另一方面，在主体与运营商交互之外，主体之间也可以进行服务的交互以获取收益，比如为其他主体网络中的远端用户提供信号数据的中继、为其他主体提供数据缓存资源降低传输时延等。

3. 分布式协同和共享

分布式协同和共享作为联盟网络的核心特点之一，强调网络与网络之间的协作。在联盟网络中存在不同种类的网络，有运营商的大网，有政企及行业网络，通过跨网络、跨地域、跨业务的协作，组成联盟网络，形成一个更加紧密的整体，实现共同的目标。通过共享网络资源和功能，主体网络可以获取自身以外的能力，避免网络的重复建设，提高资源利用效率。这也有助于降低部署网络的门槛，使得极简网络成为可能，对于 ToB 行业有着极大的意义。比如中小制造业无需自建一套完整的网络，只需部署接入网节点和服务路由网关，将核心网及辅助算力、人工智能等资源通过其他网络的共享实现，有效降低了企业的试错成本。分布式协同架构具有良好的可扩展性，能够灵活地支持各种规模和复杂度的应用场景。通过网络资源和功能共享，可以实现网络快速部署和灵活扩展各类应用和服务，满足不断增长的网络需求，降低网络更新的成本和时间要求，使网络迭代加速，提高整个网络的性能和服务质量。通过分布式协同，网络能够更好地支持各种新型业务和应用，如虚拟现实/增强现实、自动驾驶等。无论是大规模的物联网还是小规模智能家居，都能在分布式协同架构下得到有效的支持。这有助于提升用户体验，满足用户多样化的需求。分布式协同能够降低网络的运营和维护成本，减少对中心节点的依赖，提高网络的自适应性和可维护性。通过分布式的部署和协同工作，系统能够在不同节点之间实现负载均衡和故障冗余，从而提高整个系统的可靠性和稳定性。分布式协同结合了去中心化和密码学等技术，能够提供更好的安全性和隐私保护，确保用户数据的安全和完整性。

4. 多方可信与安全隐私

联盟网络中的各网络主体为平等地位，不存在上位的中央节点，因此联盟网络依赖多方协商来保障整个网络的可信能力。多方信任通过多主体的协商和共同

保证来提供信任，根据类区块链共识机制算法保障交互的可信性。多方信任还包含了自动运行的智能合约机制，实现多方确认即是事实，避免了单方违约的风险。多方信任保障网络在不同场景和需求下的可信能力，并且实现全网任意节点间信任。多方信任还包括了分布式数字身份，身份是交互的凭证，分布式数字身份可以实现对于身份的自主可控，根据不同需求生成包含不同内容的实时数字身份，保护身份其他信息不外露。联盟网络借助拟态、分布式、AI 实现主动安全免疫，形成网络的内生安全。另外对于交互的内容，在信息传输维度通过对称加密和非对称加密技术对传输接收者身份以及传输内容进行加密，在信息处理维度通过隐私计算保障数据处理不泄露信息。

5. 智能化自动运行

智能化自动运行在联盟网络中不仅仅是传统网络中提升网络运维效率、增强网络通信性能等用途，还有保障多种交互的用途。联盟网络通过多方可信技术来实现各主体之间的可信交互过程，因为缺乏中心节点或者中央机构，无法实现第三方保障的强制执行，因此联盟网络通过智能化来实现交互和合约的自动执行。如多方经过共识后形成合同，在服务结束后划拨资金。使用传统方式则可能产生资金延后、资金拖欠等问题。联盟网络使用智能化的方式保障运行，在合同中加入智能化自动执行的功能，在服务结束后自动划拨资金，使用服务方无法通过强制手段阻止这一行为的发生。不仅仅是合同领域，在其他交互方式中智能化也可以保障交互的可信进行。

四、联盟网络体系架构

1. 体系架构概述

联盟网络的体系结构可以概括为“三横两纵”，为包含主体网络层、互联互通层和联盟应用层的三层以及贯穿三层的联盟权益管控和联盟可信保障。其中主体网络层是联盟网络的基础，包含联盟网络中各类主体网络，每个主体网络有自身的身份、资源、服务等。其上为连通各个主体网络的互联互通层，提供服务的注册、发现、调用等能力，实现网络之间的通信、协作。最上为联盟应用层，为各类应用提供底层服务的调用能力，可以实现并不限于泛在接入、资源共享、数据流通等服务能力。联盟权益管控提供策略规划和权益管理功能，为各层提供自动合约执行、交易策略制定等能力。联盟可信安全提供整个联盟网络的可信安全保障，维护多方共识、隐私保护等多种能力。

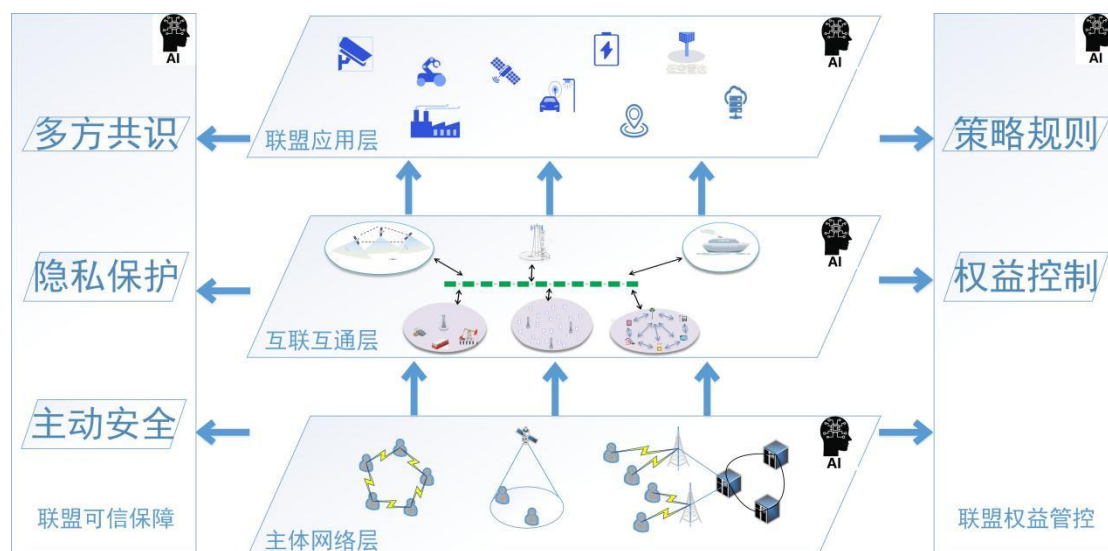


图 4-1 联盟网络“三横两纵”体系架构

2. 主体网络层

主体网络层为联盟网络的基础，由各个自主的主体网络构成，主体网络可以是运营商大网，也可以是政企及行业网络，还可以是个人及家庭网络。主体网络首先需要实现不依赖外部的自运行，是一个自主的主体，所有决策、管理都由网络主体做出，主体可以支配网络中的元素，这是构成联盟网络的前提。主体网络中可以包含更子层的网络，也可以包含用户如终端等，这些网络内部个体通过主体网络实现与外部其他主体网络及主体网络中个体的交互。

主体网络还包含三个主要基本元素：网络身份、网络资源和网络数据。网络身份是网络间互联互通的基础之一。在与其他网络交互时，需要网络身份作为认证的凭证和内容分发的标识。联盟网络是一种分布式的网络结构，没有中心化管理机构，因此联盟网络的网络身份需要使用分布式的身份机制，如 DID

（Decentralized Identity，去中心化身份）等。网络资源是网络间共享和服务的重要组成部分，资源可以是无线频谱资源，可以是网络自身的基础设施如通信、算力、感知，也可以是数字资源。网络数据与模型一起作为人工智能和大数据分析的主要元素，无法实现与传统资源相同的共享，比如网络自身管理运行数据和网络中个体隐私数据等，其需要采用专门的处理方式。

3. 互联互通层

(1) 架构总述

互联互通层是实现网络间互联互通的关键，其在横向看为总线式网络架构。联盟网络中各个网络为相互平等的关系，传统的中心式控制在此无法实现，因此通过总线式互联互通架构实现网络间的交互。自治网络都通过总线上的接口与其他自治网络进行交互，这样的架构设计避免了随着网络数量增长带来的指数级连接管理复杂度。并且总线式架构支持网络的灵活加入和退出，不对联盟网络中其他网络带来过多影响。在总线式架构中网络之间的交互都以服务的形式进行，服务的交互有不同的实现形式，现有主流的两种实现方式是分布式网络功能管理和去中心化类区块链。分布式网络功能管理使用分布式网络管理功能（DNMF，Distributed Networks Management Function）单元作为交互的接口，通过形成注册中心完成服务管理。去中心化类区块链式将信息都上传至类区块链节点，通过多方共识机制完成更高级的服务交易。

(2) 分布式网络功能管理

联盟网络支持高量级开放多元化网络和多模态的网络架构，网络拓扑的发现和管理是一个需要解决的的重大挑战。基于算力、数据、AI、安全等关键技术对原有的 NRF（Network Repository Function，网络存储功能）和 SCP（Service Capability Exposure Function，服务能力发现功能）进行功能扩充，形成新的网络功能单元 DNMF。

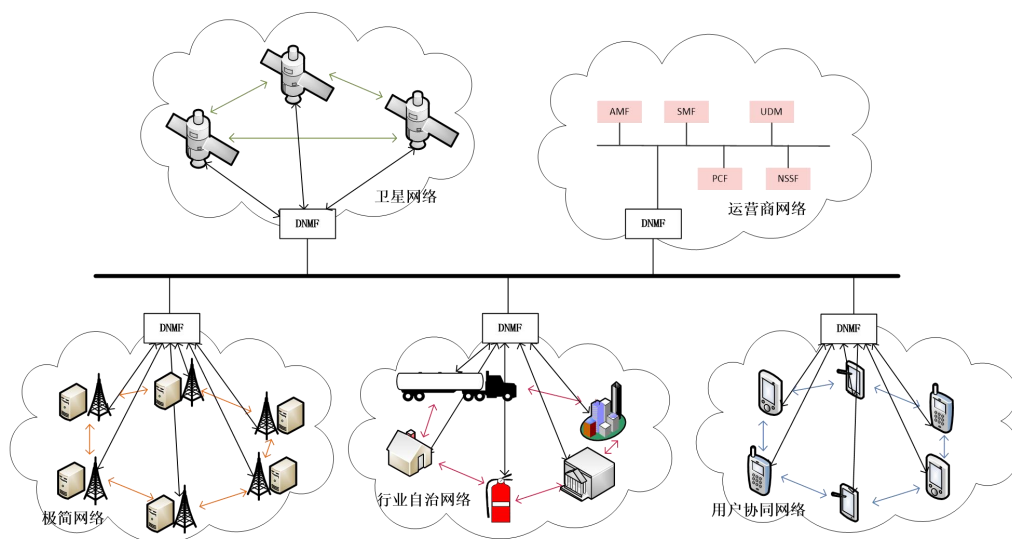


图 4-2 DNMF 式联盟网络架构

联盟网络架构内的 DNMF 除维护原有的各个控制面网元的网元基本信息，还在非运营商网络内维护网络根据业务等特征按需生成的网络功能信息、资源信息、服务信息等。通过维护多种信息，多元化网络平台得以适应 6G 的多种场景需求。

同时，DNMF 为各网络提供对外接口，承担起各个网络的管理、鉴权、组网等工作。这有利于实现网络拓扑的弹性自组，同时实现可信安全的网络发现和通信机制，提高整个网络的安全性和可靠性。DNMF 用于实现网络粒度的信息维护和更新、自动注册、去注册、保活等。该网络功能维护的信息包括主体网络自身的服务信息、相连其他网络的服务信息、网络间的拓扑连接关系等。其中服务信息包括主体标识、主体网络类型、DNMF 的地址信息、主体网络功能属性、主体网络所在位置信息、主体网络服务区域信息、数据网络信息、切片信息、算力资源等。各网络可以通过 DNMF 进行协同控制、计费奖励监控、主体数字资产应用管理等。

(3) 类区块链式去中心化

类区块链式去中心化架构使用类区块链技术作为网络间交互的总线，每个网络的区块链模块是总线上的接口，其可以分为区块链交易共识功能模块和区块链账本记录功能模块及自定义功能模块等。

当网络主体可以对外提供服务时，区块链模块可以发布服务列表信息，对其

进行数字签名，然后形成交易信息广播出去。其他网络主体验证了签名和信息是对应关系，则交易信息就能被写入区块。当网络主体需要服务时，也可以使用与发布服务信息相同的流程，主动发布招募或悬赏信息。当网络主体的服务发生变化时，可以使用相同流程发布服务更新信息写入区块。网络主体定时接收这些信息并存储。

4. 联盟应用层

联盟应用层是联盟网络体系中的最高一层，在下面两层的基础上，联盟应用层直接与实际的应用相接。一方面，本层可以提供常见的网络基础应用服务，如泛在接入、资源共享、数据流通等。另一方面，本层可以为在其上承担的其他应用提供下层映射管理接口。这方面，联盟应用层具备调用、组织、聚合功能，可以将下层的各种资源、基础功能进行编排，将应用映射到相关的管理控制单元，为应用提供精确的按需保障，实现跨主体网络层级的服务保障能力。

5. 联盟权益管控

联盟权益管控是实现联盟网络中新型组织模式和新生态的重要支撑。联盟权益管控包含了策略规则和权益控制。策略规则主要体现在激励机制，激励机制扮演了资源交换规则的角色，其规定了网络如何协商不同资源之间的兑换，包含资源交换的数量和价值，允许网络之间形成个性化的兑换规则。权益控制的代表为智能合约，智能合约是“合同”的技术升级版本，通过代码的方式将“合同”记录下来，当条件或者期限到达时即强制执行。在实际应用中还需要配合多方信任技术使得强制执行的结果形成多数承认的事实。因此联盟权益管控指导并协调网络间订立了“合同”，并通过技术的设计保障了“合同”的强制执行，杜绝了违约的现象，有力支撑了上层各种应用的展开。

6. 联盟可信保障

联盟可信保障提供整个联盟网络中各网络主体之间的可信交互。因为网络主体之间相互平等的关系，没有上层机构进行协调和管理，实现资源的对等交换必须通过网络间的协商机制。联盟可信保障提供多方共识、主动安全和隐私保护等能力。多方共识是实现激励机制的基础，通过一定机制的多方协商过程，形成资源交换的共识。其规定了多方在协商过程中使用何种方式达成最终的共识，方式

可以是预先制定的集中默认规则，也可以是多方自行定义的方式。主动安全能力通过联盟网络分布式的特点，协调各主体网络形成优势互补的主动安全能力，实现防患于未然。隐私保障能力保护各主体在交互过程中的隐私内容，使交互既可以受到参与方之外主体的可信支撑，又不对外泄露隐私内容。

五、相关关键技术

1. 自主数字身份

联盟网络代表了网络从封闭单一系统向开放、分布式和互联系统的显著转变。这涉及众多参与者和利益相关者，如频谱交易方、有线和卫星服务提供商、物联网和 OTT 服务提供商等。这些新兴参与者在联盟网络中提供移动连接和相关服务，扮演着越来越重要的角色。在联盟网络的框架下，移动网络运营商（Mobile Network Operators, MNO）的角色将从传统的网络运营商转变为连接提供者，负责协调复杂多变的移动连接市场中各种参与者的互动。这意味着网络连接将成为一个跨领域的服务，依赖于分布在联盟网络内多个信任领域之间的资源。随着越来越多的参与者加入解聚的联盟网络运营，对跨领域接口的需求不断增加。在联盟网络中，信任成为一个关键设计原则，必须通过统一的访问管理在各方及其涉及的网络之间建立信任。

联盟网络需要有效协调包括云服务、边缘计算和硬件供应商在内的各种新兴参与者。为了形成一个多元利益相关者的服务生态系统，这种协调必须建立在经济可行且无缝连接的基础上。联盟网络的每个参与者都需要具备安全认证和授权机制的接口，并满足复杂的公共密钥基础设施（Public Key Infrastructure, PKI）的身份和密钥管理要求。因此，联盟网络的核心是促进各种新兴和传统参与者之间的协作，同时在开放、分布式的环境中维护安全性和信任。这样的网络结构将提升网络的灵活性、可扩展性和效率，以满足未来通信的需求。在联盟网络架构下，6G 移动网络面临着身份验证和授权程序的多样化挑战。例如，在 5G 网络中，移动用户主要使用对称加密进行身份验证，但在漫游时，运营商之间可能使用基于非对称加密的安全传输层协议和预共享的公钥。为了在联盟网络中实现非对称加密的身份验证，需要建立并维护一个复杂的 PKI，同时还要确保不同运营商之间的安全互联。

此外，全球范围内缺乏共同信任的认证机构（Certificate Authority, CA），加上地缘政治差异和防止单点故障或攻击的需求，使得建立一个统一、基于集中式 PKI 的身份管理方法变得复杂和不切实际。在 5G 中，尽管 GSMA 建议每个 MNO 至少运营一个根 CA，但这并未解决共同信任的 CA 缺乏的问题。同时，随着个人数据保护法规（如欧洲的 GDPR）的实施，用户越来越关注其个人数据

的处理方式。在涉及众多参与方的联盟网络中，遵守这些新的隐私和透明度法规对 MNO 是一个重大挑战，因为个人数据通常由 MNO 及其合作伙伴集中处理。因此，在联盟网络下的 6G 移动通信网络中，必须采用一种全新的、统一的身份管理方法，以应对目前系统的异质性、缺乏全球信任的 CA，以及对个人数据保护需求的增加。6G 的数字身份管理系统必须满足包括但不限于用户、物联网设备、MNO、虚拟移动网络、云或物联网运营商、制造商，甚至 NF(Network Function, 网络功能)的普适性需求。

当前集中式 PKI 技术尽管在受限和受信任的环境中技术上可行，但面临跨领域互操作性、国家数据保护法规和地缘政治策略的限制。因此，联盟网络架构需要探索新的身份管理解决方案，例如 W3C 提出的 DID。这种分散式身份管理为联盟网络提供了一种全网统一、安全、防篡改且跨领域的身份管理方法，不再依赖于集中式身份提供者或认证机构。在联盟网络结构中，不同的实体网络（如天基网络和地基网络）可以通过智能合约和类似区块链的技术来确保服务权益的记录和保护，同时实现更广泛的跨境服务和协作。这不仅提高了网络的灵活性和可扩展性，也为联盟网络的发展提供了新的动力，使其能够更好地满足未来的通信需求和挑战。自主数字身份的设计应当遵循以下原则：

①隐私保护：数字身份必须设计得既不透露身份主体（Identity Subject, IS）的真实身份，也不包含与 IS 的真实身份相关的任何个人数据。利用如智能合约和区块链技术可提供这种级别的隐私保护，同时确保身份信息的安全和透明处理。

②互操作性：数字身份应该是独特的、机器可读的、标准化的格式，确保在联盟网络的不同参与者和平台之间可以普遍访问和识别。这种互操作性对于实现多利益相关者之间的无缝协作至关重要。

③可验证性：数字身份在密码学上应该是可验证的，使身份主体能够证明对其数字身份的所有权，同时让其他人能够验证由身份主体共享的个人数据的有效性。这种特性对于增强交易和交互的信任度和安全性至关重要。

④可扩展性：考虑到潜在应用领域的多样性，数字身份系统应具有在支持验证方法方面的可扩展性，能适应不断变化的技术和需求，支持从个人用户到大型企业的不同类型的身份验证。

⑤独立性：数字身份应能独立于任何公司、组织和政府，包括身份提供者和

CA，确保身份管理系统的去中心化，降低了对单一实体的依赖，从而增加了系统的弹性和安全性。

自主数字身份引入了一种新的身份管理方法，它使身份能够以统一、分散的方式进行管理，无需依赖于集中的身份提供者或 CA。例如，通过使用分布式账本，自主数字身份的分散特性具备了统一网络中跨领域访问管理程序的潜力。在联盟网络生态系统中，分布式账本可以作为所有参与者间非隐私敏感访问管理数据的唯一真实来源，以可验证凭证的形式存储访问授权。这种方式不再是集中式存储，而是分散在授权方，例如在客户设备上。将自主数字身份应用于联盟网络以实现分散化的身份管理，不仅能降低因去除 CA 而带来的单一故障点或攻击风险，还能使 MNO 更好地遵循隐私设计原则。

此外，自主数字身份的应用有望降低跨领域身份管理的运营成本和复杂性，同时增加安全性和可靠性。这将促进未来高度异构的 6G 网络中，身份验证和授权机制的协调一致性。总体来说，这些创新对于构建联盟网络背景下的高效、安全、用户驱动的合作开放至关重要。

2. 分布式服务管理

服务管理是当前 5G 网络使用的 SBA（Service-based Architecture，服务化架构）中的重要机制。相对于其“节点”或“网元”通过接口相连的前几代传统网络架构，5G 网络功能之间使用基于服务的交互，每个网络功能为网络中的其他网络功能提供一项或多项服务。当两个网元 NF 进行通信时，它们将扮演不同的角色：发送请求的 NF 为服务消费者，接受请求的 NF 为服务生成者。服务管理是这其中用于确定服务消费者如何找到并联系服务生产者的机制。该机制依赖于网络中集中的 NF，即 NRF。同一个网络中的其它 NF 将提供的服务注册到 NRF 中，而后 NRF 对其提供的服务进行管理。不同网络之间的服务调用则进一步依赖于各网络的 NRF 之间的交互。

面向 6G 的联盟网络在组网架构上的分布化趋势将会更加显著，整个联盟网络由众多归属于不同主体的网络组成。主体除了运营商，还可以是政企及行业客户或个人和家庭用户，网络的形式也由传统网络向传统网络与终端自治网络等多样化共存的方式转变。

考虑到联盟网络服务关系的灵活化，服务管理涉及的信令需要携带更多的信

息，发生频次也将增多，传统的基于 NRF 的管理机制需要进一步增强以满足分布式的服务管理，同时网络中需要引入类似 SCP 的功能，实现网络间的服务路由及转发；此外，多样化的网络生态参与方意味着服务管理机制需要搭建可信公平的运营环境，并提供分布式的服务管理能力，以激励各方的合作，最终实现资源和数据在整个联盟网络内的高效流转；最后，当前 5G 网络的服务管理主要聚焦在 NF 层面，而联盟网络的分布式服务管理需要进一步考虑网络层面的发现和协商问题。

作为一种分布式记账系统，区块链天然地适合联盟网络对分布式服务管理的种种诉求。一种基于区块链的分布式服务管理方案的总体描述如图 5-1 所示，联盟网络中有若干个独立的网络，这些网络各自部署代表自身所属主体的服务节点，这些服务节点作为区块链节点共同构成一个区块链网络作为联盟网络的分布式服务管理底座。服务节点为主体网络提供服务注册、更删、调用和路由协商等能力，并将服务信息和调用记录记录在区块链上。利用智能合约和链式数据结构等特性来实现服务权益的记录和保障，该方案提供了一种方法来保护联盟网络内具有共同目标但彼此不完全信任的实体之间的交互。

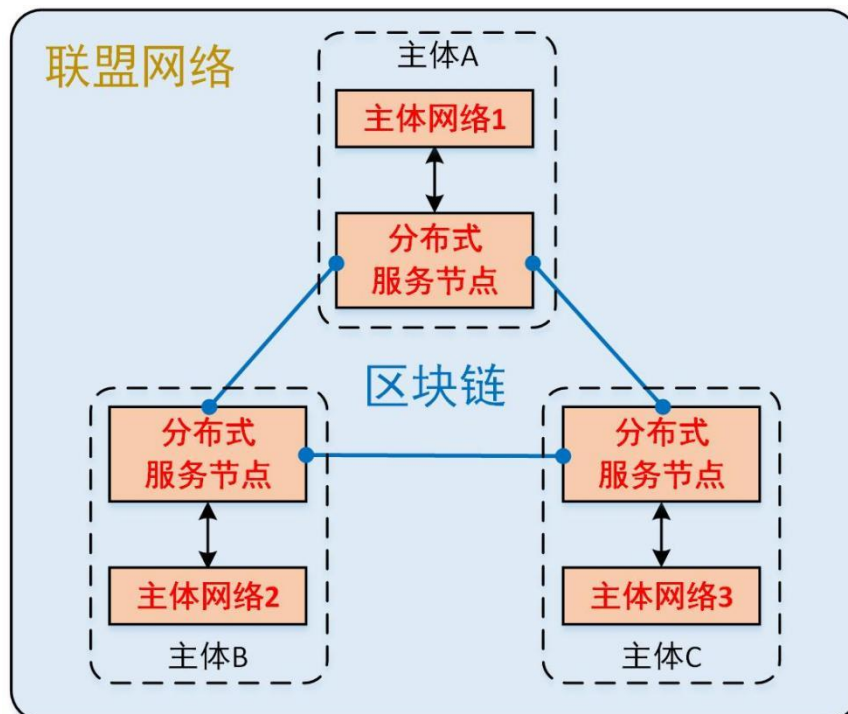


图 5-1 基于区块链的分布式服务管理方案

具体来讲，加入到联盟网络中的各个自治网络向属于同一主体的分布式服务

节点发起网络能力或 NF 服务的注册/更新/删除请求。收到请求的分布式服务节点将请求内容写入交易，区块链网络对该交易达成共识。自治网络随时可以通过分布式服务节点查询区块链以获取所需的信息。当需要特定内容时，由分布式服务节点协商路由，将调用记录记录在区块链上，最终完成调用。

3. 权益管理

权益泛指特定主体被分配拥有的角色、地位、权利和益处等，包括权利和利益两个方面。网络主体的权益保障不仅能够促进各网络主体公平竞争、增强合作信任还有利于网络稳定和可持续发展，对联盟网络的成功至关重要。网络主体的权益保障需要通过权益管理来支撑，权益管理可以划分为权益策略、权益控制和权益执行三个功能。

权益策略是对网络中的策略规则进行管理。在联盟网络中，存在多种类型的网络主体。例如，在车联网中有车辆制造商、电信运营商、软件和平台提供商、政府机构、保险公司、维修和服务提供商、数据分析公司等多种网络主体。这些主体在车联网生态系统中相互协作，共同推动车联网技术的发展和运用，以提高交通安全、效率和便利性。通过策略规则明确网络中各方的权益，可以平衡和协调各主体需求，有利于实现车联网多方共治共赢。可以看到，权益策略制定是权益管理的核心。具体来说，权益策略管理包括主体管控、权益划分、权益交易等多种策略规则的制定。权益主体管控策略规则包含对主体资质判断、主体合法性判断、法律法规对主体的规定、合同协议对主体的约定、主体身份确认等相关策略规则。权益主体管控策略保障了合法主体的权益以及防止非法或不符合规定的主体获得权益。权益内容策略规则明确了各个主体在联盟网络中资产的归属权、网络知情权、服务使用权等权利以及各主体对网络贡献应该获得的激励/奖励。权益交易策略规则规定了在交易过程中交易双方要遵从的各项规则，如是否有第三方证明、如何控制交易周期、交易是否可撤销、是否同意评分、具体的评分策略、电信网区块链如何进行账本选择、是否需要隐私保护、隐私保护的程度等。

权益控制是对权益交互过程进行控制管理。网络中的权益交互过程非常多，如权益配置确认、权益注册发现、权益请求响应等都需要网络主体双方甚至多方的交互。权益配置确认过程指网络根据权益策略规则确定参与主体的权益信息（如归属权、管理权、定价权、分成比例等），并将权益信息发送给对应拥有该

权益的网络主体，使得网络主体不仅可以了解自己在网络中的权益，还可以选择接受还是拒绝网络所配置的权益。权益注册发现过程指每个网络主体可以将自己提供的资源、服务所能对应的权益信息注册到集中的权益信息库或者使用区块链上链，使得资源、服务的使用方在看到并认可这些权益信息的前提下进行公平交易。权益请求响应过程指网络主体根据自身能力主动发起对自身权益的请求，联盟网络中的管理方（如公证方、交易平台方）或使用方对权益请求进行应答。

权益执行是对权益策略和权益控制的实际执行过程进行管理。权益执行涵盖一系列与权益相关的操作和活动，以确保权益管理的有效实施和维护。具体来说，权益执行的操作有：确定和设置网络主体的权益、网络主体查询权益、对权益进行修改或更新、终止或撤销网络主体的权益以及恢复被终止或受损的权益等。

权益策略规则管理	权益交互控制管理	权益执行管理
• 主体管控规则 • 权益划分规则 • 权益交易规则	• 权益配置确认 • 权益注册发现 • 权益请求响应	• 权益生成 • 权益变更 • 权益消亡 • 权益恢复 • 权益查询

图 5-2 联盟网络中的权益管理

在权益管理中，权益策略为权益控制和权益执行提供指导，权益控制保证权益策略的有效实施，而权益执行则是实现权益策略的具体手段。通过这三个功能的协同工作，可以实现对网络主体权益的全面保障。

4. 多方共识可信

在分布式系统中，缺乏各个节点都信任的中间机构来进行交互的担保，各个节点之间的资源和服务交换通常是不可靠的，因此需要一种机制来确保节点之间的信任关系。一种机制是通过节点过往行为形成对于其可信任度的评价，其他节点基于评价决定可以与此节点发生何种程度的交互，这种方式的典型应用为征信。其缺点是需要经过节点的多次交互才能形成。多方共识信任技术正是为了解决这个问题而提出的。多方共识信任技术的核心思想是通过多个实体的共同参与和协商，达成一种共识，从而建立起信任关系。最典型的实现方式是基于区块链的共识机制，它通过去中心化的账本和智能合约等技术，实现了无需信任第三方的信任建立和管理。

面对传统通信网络中数据安全和共享的挑战，通信网的区块链技术探索在去

信任环境下赋予网络韧性可重构能力，以支撑通信网络的发展和创新。在联盟网络的早期阶段，耦合区块链是一种重要的技术形态。这种区块链与通信网络在协议流程中有紧密的耦合交互，包括离线连接和在线检查。例如，基于区块链的身份验证业务中，信息所有者或授权运营方将信息（如凭证）或哈希值存储在区块中。当联盟网络中的一个主体收到通信请求时，它在区块链中搜索请求者的凭证以进行身份认证。一旦认证成功，该主体接受连接请求并继续后续流程。这种方式在联盟网络中提供了一种灵活而安全的身份验证机制。

随着联盟网络的发展，区块链技术将进一步的与通信网络嵌入和融合，发展成为通信网络不可或缺的组成部分。在这个过程中，区块链的算法、通信协议和使能功能将完全融入到通信网络的功能和协议之中。在这样一种交织的形态下，区块链的写入和搜索操作将实时在线进行，成为通信过程的一部分。但是，要实现区块链技术在通信网络中的实时应用，面临着一系列挑战。为此，通信网区块链的发展可以围绕以下三个核心目标展开：

①建立适应联盟网络的区块链理论基础：未来联盟网络建设的核心之一是构建一个实时、大规模的区块链系统，这将成为网络运营的可信基础。为此，首先需要发展针对联盟网络特性的区块链理论基础。这种理论基础应考虑到联盟网络中各类网络的特性，包括运营商网络、行业网络 and 用户网络的特点，以确保区块链技术能够有效地应用于这样一个多样化和动态变化的环境中。

②开发适配联盟网络的区块链体系架构：区块链架构需要原生设计，以适应联盟网络中无线和网络传输的特点，例如确定性的低时延和高吞吐量需求。同时，这个体系架构还需考虑隐私保护的要求。因此，研究和开发一个适应联盟网络的区块链体系架构显得尤为重要。这种架构应能够高效处理各类数据和信令交互，例如在一个基于权限的超级账本上，确保每个实时数据会话和信令交互都被不可篡改地记录。

③构建面向联盟网络的区块链平台：为了提高区块链技术在联盟网络中的应用效率和可行性，需要构建一个专为通信网络设计的云边协同软硬件一体化区块链平台。这个平台应当能够支撑联盟网络中各种网络主体之间的服务和资源流转，包括地基网络与天基网络在内的不同网络形态。此平台将成为实现资源和服务流通的关键，同时保障服务权益的透明性和安全性。

5. AI 赋能网络自智

联盟网络中主体网络间交互频繁，单纯依靠即定策略和人工控制即粗糙又缓慢，同时也无法满足交互的可信性，因此在联盟组网中智能化自动运行得到了更广泛的应用。借助先进的算法和模型库，包括机器学习、深度学习和强化学习等算法，通过多网络的大规模语言模型训练和分布式生成，实现整个网络更高阶的自治水平，网络能够实现自动化决策、资源管理和流量调度等功能。这将有助于提高网络的运行效率和响应速度，降低运营成本。例如，节点可以根据流量负载情况，协同地调整路由和流量分配，以提高网络性能。同时，智能化自动运行还将支持个性化的服务需求，为用户提供更加优质、高效的网络体验。随着环境和业务需求的变化，网络能够自动调整其运行参数和策略以适应变化的环境和需求。这有助于提高网络的灵活性和可扩展性。智能化自动运行还体现在对异常事件的快速响应和处理上。通过实时监测和分析网络状态数据，网络能够及时发现异常事件并进行快速处理。这有助于降低故障发生的风险并提高网络的可靠性。同时，智能化自动运行还有助于提高网络的自适应性。

6. 其他技术

(1) 网络服务快速建立

在多方共识可信技术和分布式服务管理的帮助下，联盟网络中的多个网络主体能够与用户之间建立网络服务，其中的用户可能并不隶属于提供服务的网络主体。同时，随着接入需求的激增，网络的质量、多方的管理和安全会面临更大的挑战。网络服务快速建立技术可以在确保服务质量（Quality of Service, QoS）的前提下，兼顾安全与高效地提供网络服务，也为联盟网络中跨域接入的难题提供了解决方案。

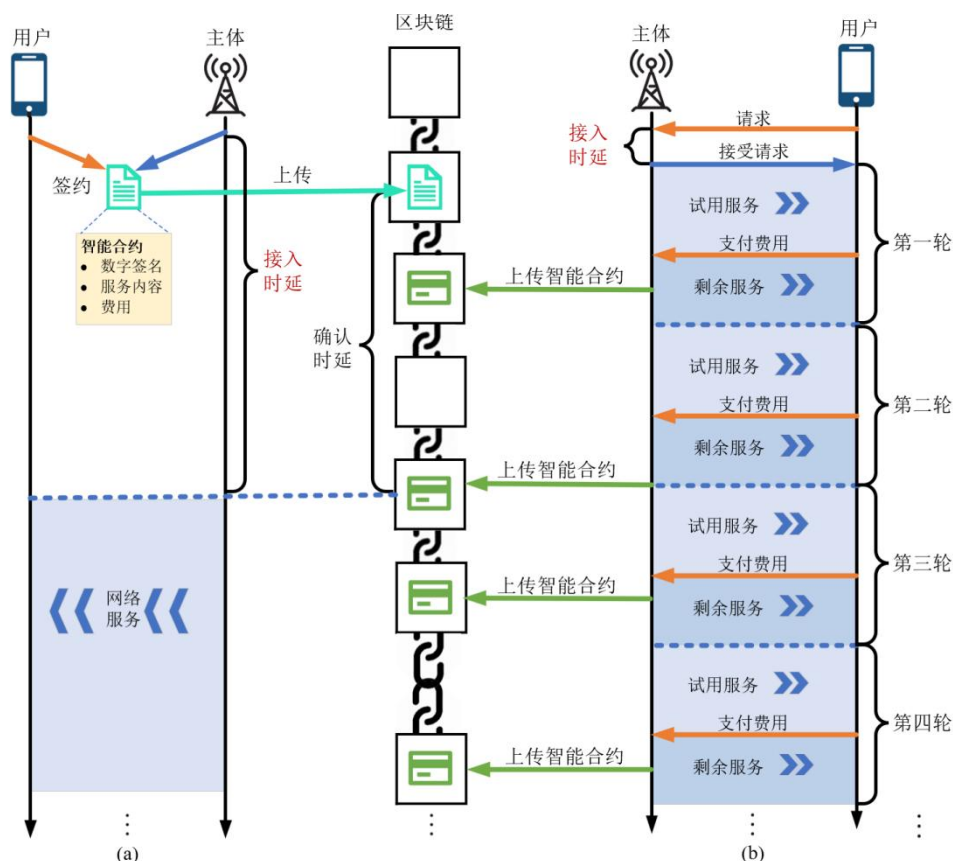


图 5-3 网络服务建立方案

在传统方案中，用户若想使用网络服务，需要先与联盟网络中的主体签署合同，在彼此之间建立信任后，主体为用户提供所需的服务。然而，通过网络服务快速建立技术，用户向网络主体发送请求，主体可以立刻为用户提供网络服务，通过切分服务并分多次签署智能合约的方式实现服务建立，省去了相对繁复的建立信任过程，达到快速建立网络服务的目的。

图 5-3 展示了该框架的工作原理，其工作流程可以表述如下：

- ①首先，用户向联盟网络中的主体发送接入请求；
- ②在主体接收到接入请求后，立即为用户提供网络服务；
- ③整个建立过程被划分为多个轮次，每轮开始时，主体会为用户提供一段试用的服务时间；
- ④在每轮试用时间结束之前，用户通过签署智能合约的方式承诺将费用支付给网络主体，包括已经接收到的试用服务的费用和当前轮次剩余时间的服务的费用，从而弥补之前主体提供无尝试用服务所承担的风险；
- ⑤如果用户按要求签署智能合约承诺支付费用，主体则立即为用户提供当前轮次的剩余服务，并且在本轮次结束前将智能合约上传到区块链网络，在包含该

智能合约的区块成功上链后，费用会自动由用户转移到网络主体；

⑥如果用户没有按要求智能合约诚实支付费用，主体则不再提供进一步的服务，双方也不再合作；

⑦如果双方都诚实，该轮次可以成功完成，之后，重复上述步骤，直至完成整个用户请求的网络服务；

⑧用户可以通过在某个轮次停止支付来终止服务，主体也可以通过停止提供服务来停止与用户的合作。

这种网络服务快速建立的跨域接入框架的优点如下：

①如果用户对联盟网络中的主体提供的网络服务不满意或者发现主体的其他不当行为，可以在任何轮次离开，从而可以确保服务质量，弥补了分布式系统对链下操作监管有限的问题。

②利用多次交互的思想省去相对复杂的信任建立过程，提供了更快速的网络服务，减少了接入延迟，使得主体能够在智能合约上传到区块链网络之前就为用户提供服务，为用户带来了更加即时且高效的服务体验。

③由于用户不需要与联盟网络中的主体建立预先的信任，因此比传统的网络服务建立方案更具灵活性，增强了用户和主体之间的信任关系，可以激励双方在没有可信第三方的情况下进行合作，从而高效处理高频次的服务建立请求，解决联盟网络中接入需求激增的问题。

(2) 基于区块链的网络层技术方案

用区块链安全需要大量共识节点的支持与维护，而通信网系统存在设备多样性、数据异构性以及网络复杂性等特点，难以保障共识节点可信性。网络层在扩散区块信息和交易信息的过程中，存在恶意基站限制扩散等风险，因此需要设计拜占庭容错的网络层信息扩散协议，实现高效的泛在可信通信网络。由于频繁的节点间通信，现有 PBFT (Practical Byzantine Fault Tolerance, 实用拜占庭容错) 的消息扩散协议的可扩展性较差，难以应用于存在大量基站的通信网络场景。双层区块链共识机制解决传统共识的可扩展性限制，一定程度上满足了通信网络对于快速共识、并发处理、高吞吐量、低时延、低费用、易于扩展和健壮安全等应用需求。

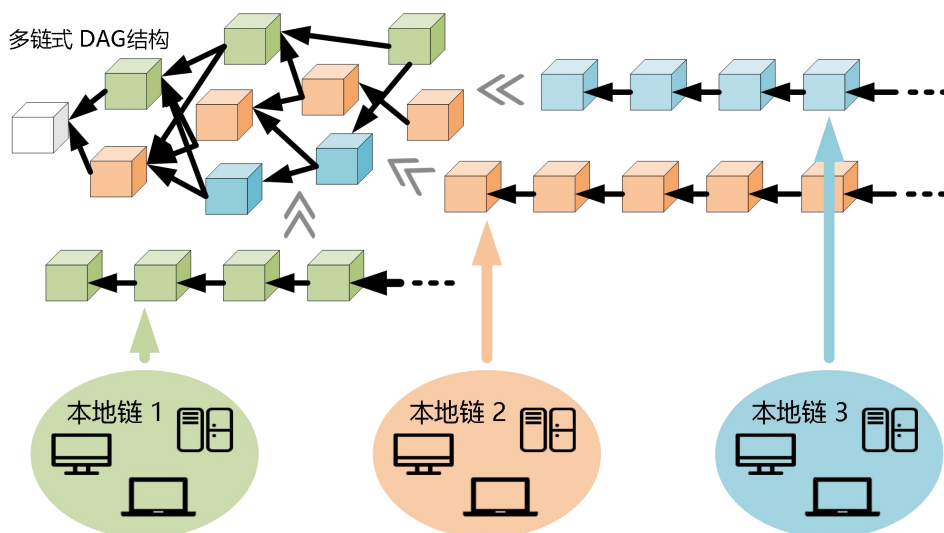


图 5-4 基于 DAG 的跨链协同共识结构

图 5-4 展示了基于 DAG (Direct Acyclic Graph, 有向无环图) 的跨链协作共识结构。链 1、链 2 和链 3 代表了独立本地区块链系统。为了预防恶意本地链系统的生成, 本地链系统的数量需要提前确定。基于分区独立与跨层协同方式, 突破区块链不可能三角限制, 实现区块链与通信网络的有效结合。底层分区隔离保障安全隐私和资源切片独立性的同时, 实现泛在可信网络的去中心化需求; 共识机制分为两层: 基于 DAG 的跨链协作共识和本地区块链系统内的独立共识。

第一层: 基于 PoW (Proof of Work, 工作量证明) 的区块生成共识机制

每个节点仅在其本地链系统内生成和接收交易信息。例如, 链 1 系统中的节点只能接收链 1 内的交易信息, 而不能接收来自链 2 或其他独立本地区块链系统的交易信息。当节点接收到交易信息时, 会通过验证交易的完整性和有效性来确认交易的合法性。如果交易验证失败, 则不会将其打包进新的区块。在验证过程中, 节点尝试解决一个 PoW 问题, 该问题基于本地链系统信息 (用于调整区块生成速率) 和区块链难度信息 (确保每个本地区块链系统面对的 PoW 问题难度相同, 并保证新区块的 PoW 问题是唯一的)。首个解决 PoW 问题的节点可以广播带有已验证数据集的新区块。

第二层: 基于 DAG 的跨链协作共识

步骤 1: 节点生成新区块后, 将获得一定的权重 (例如 1), 并需要验证两个权重为 1 的不同区块 (称为头部), 这些信息在 DAG 账本中本地存储, 用以确认区块的合法性和进行跨链交易验证。

步骤 2：当验证通过后，区块将被广播至全球区块链节点。

步骤 3：本地区块链系统中的新区块现成为等待其他区块链系统节点验证的头部。

步骤 4：交易在全球范围内被认为是合法的，仅当累积的权重达到共识阈值。

值得注意的是，DAG 中的权重通过后续生成的区块数量累积。根据“最长链”规则，最长链中的交易在全球范围内被认为是合法的。恶意分叉（将主链分成一个由诚实节点扩展的诚实链和一个恶意链）需要超过 51% 的计算资源。

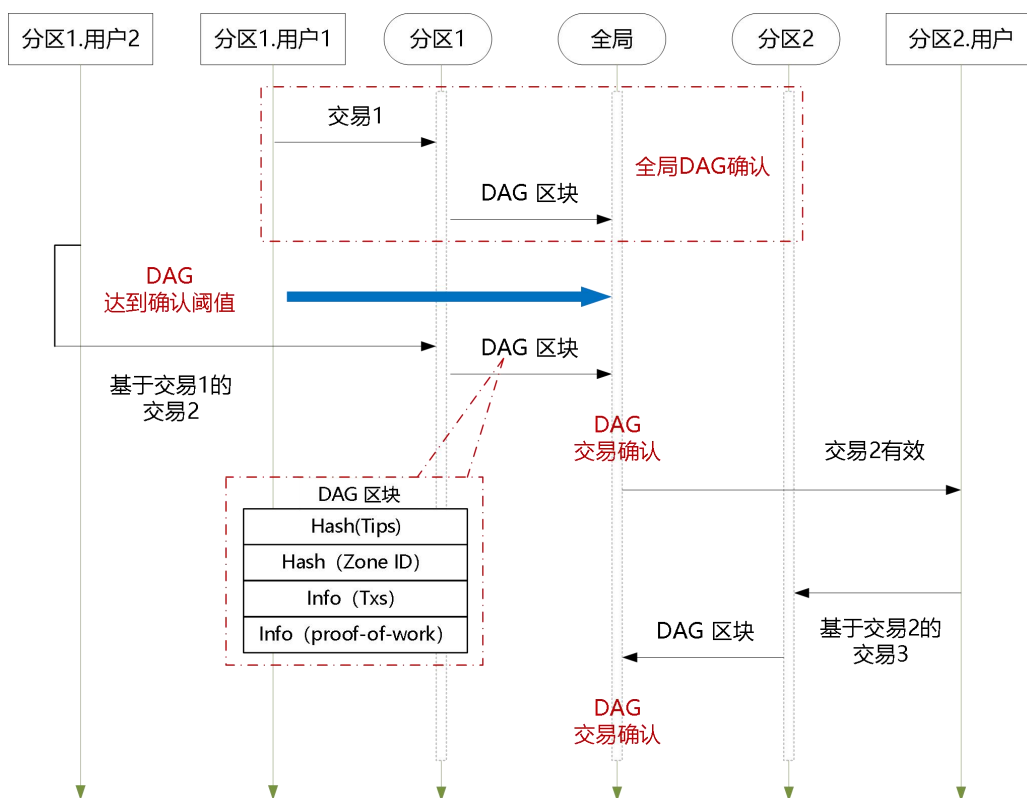


图 5-5 跨链交易确认流程

图 5-5 展示了跨链交易确认过程。如图所示，链 1 用户与链 2 用户进行交易。独立区块链系统中的交易信息将在该系统的区块中广播。无论是链 1 用户还是链 2 用户发起的交易，在交易确认过程中都是等同的。此外，不同层次也相互连接，以实现跨链协作共识。为减少互联带来的影响，该共识机制以不同的方式验证跨链交易和普通交易。跨链交易验证分布到全球区块链系统中的所有互联节点，大大提高了跨链交易双重支付的难度。跨链交易验证是对原始区块链系统普通交易验证的补充，通过这种方法，能够协调区块链系统，并确保每个本地区块链系统保持其独立性。

六、总结与展望

爱因斯坦说过：一个问题不可能从导致它出现的层面来解决。移动通信网络经过几十年的发展，业界普遍认为到 6G 时代移动通信网络需要上升到更高的维度，才能打开全新的业务空间并拓展客户范围，打造新的增长点和商业模式。联盟网络应运而生，它将归属于不同主体的网络（例如地面及卫星运营商网络、政企及行业网络、家庭及个人网络）组织到一起，通过互联互通、可信安全和权益保障，形成资源、功能和服务可以互相共享和交易的生态体系，在降低资源获取成本的同时增加变现能力，从而打造出更轻量化、更具性价比、投资回报率更高、更泛在的网络基础设施。

联盟网络的体系生态不可能一蹴而就，本白皮书虽然名为面向 6G 的联盟网络体系架构白皮书，并不意味着必须要等到 6G 才能开始联盟网络的技术和产业实践。实际上，近年来在全球范围内相关的实践不断推陈出新，国内 IMT2030 围绕分布式自治网络和区块链可信网络的体系架构开展了讨论和测试验证，在欧洲有以子网（subnet）/网络之网络（network of networks）为代表的架构设计，在美国有以 HELIUM 为代表的结合 WEB3 和无线通信网络的商业实践。这些实践为联盟网络提供了一些早期的相关技术或商业模式方面的验证，在此基础上，联盟网络重新打造体系架构，可以走出一条更加稳健可行，更有共识的发展道路。

作为全球第一本以联盟网络为名的白皮书，本白皮书仅涉及了联盟网络的基础概念，价值场景，核心特征，体系架构和关键技术，目的是抛砖引玉。联盟网络是个全新生态，不仅需要网络形态和网络技术的更新换代，还需要从小到大，从局部到全局，多维度长时间的市场验证和磨合。本白皮书为电信行业的从业者以及非电信行业的合作伙伴介绍联盟网络，并邀请工业界和学术界的专家学者加入到联盟网络的生态中，不断完善联盟网络的业务和技术体系，推动联盟网络不断向成熟演变。

白皮书中所涉英文缩写表

英文缩写	全称	中文
ODICT	Operation Data Information Communication Technology	运营数据信息通信技术
KPI	Key Performance Indicator	关键性能指标
KVI	Key Value Indicator	关键价值指标
KDI	Key Development Indicator	关键发展指标
ToB	To Business	面向商业
AI	Artificial Intelligence	人工智能
DID	Decentralized Identity	去中心化身份
DNMF	Distributed Networks Management Function	分布式网络管理功能
NRF	Network Repository Function	网络存储功能
SCP	Service Capability Exposure Function	服务能力发现功能
MNO	Mobile Network Operators	移动网络运营商
PKI	Public Key Infrastructure	公共密钥基础设施
CA	Certificate Authority	认证机构
NF	Network Function	网络功能
IS	Identity Subject	身份主体
SBA	Service-based Architecture	服务化架构
QoS	Quality of Service	服务质量
PBFT	Practical Byzantine Fault Tolerance	实用拜占庭容错
DAG	Direct Acyclic Graph	有向无环图
PoW	Proof of Work	工作量证明

参与单位：

序号	单位名称	主要参与人员
1	中兴通讯股份有限公司	谢峰、张康杰、黄峰鹤、薛妍
2	中国电信集团研究院	林奕琳、刘洁、陈思柏
3	北京邮电大学	曹宾、刘家硕、李灏洋
4	东南大学	凌昕彤、陈诗怡、胡竞翔
5	中信科移动通信有限公司	程志密、李慧欣
6	中国联合网络通信集团研究院	梁婷婷、孙明锐
7	维沃移动通信有限公司	姜大洁