

未来网络白皮书系列

基于确定性网络的 智能体可信数据空间

第九届未来网络发展大会组委会

2025年8月

版权声明

本白皮书版权属于紫金山实验室及其合作单位所有并受法律保护，任何个人或是组织在转载、摘编或以其他方式引用本白皮书中的文字、数据、图片或者观点时，应注明“**来源：紫金山实验室等**”。否则将可能违反中国有关知识产权的相关法律和法规，对此紫金山实验室有权追究侵权者的相关法律责任。

编写说明

主要编写单位：

江苏未来网络集团有限公司、清雁科技（北京）有限公司、润泽集团河北省算力产业技术研究院、菲尼克斯电气（中国）投资有限公司、紫金山实验室、南京新一代人工智能研究院有限公司。

主要编写人员：

叶迎春、陈刚、钱锐、华强、葛宇、邵静兴、王俊颀、张英伟、林杨、王远、张秀芳、胡华、梁恩泉、方毅然、李政隆、张萌。

前 言

（一）数字经济发展对可信数据空间的需求

当前，全球已进入以数据为核心驱动力的数字经济时代。2023 年我国数字经济核心产业增加值占 GDP 比重达 10%，数据总产量达 32.85 泽字节（ZB），同比增长 22.44%。然而，数据要素的价值释放仍面临严峻挑战：仅有 2.9% 的数据被有效保存，企业超过一年未使用的数据占比近 40%，数据资源“沉睡化”现象突出。这一矛盾的核心在于数据要素市场化循环体系的梗阻——传统数据流通模式难以平衡“安全可控”与“高效利用”的双重需求，具体表现为三大困境：

1. 数据流通的“信任困境”

数据作为新型生产要素，其价值释放依赖跨主体、跨域的高效流通。但企业间因商业机密保护、权属界定模糊、合规风险高等顾虑，形成“不敢共享、不愿开放”的僵局。全国人大代表柳江在 2025 年全国两会中指出：“多方数据跨界融合需求明确，但大规模数据流通利用场景仍在探索”。尤其在 AI 驱动的智能体协同场景中，数据需在算法模型间高频交互，传统点对点交易模式无法满足实时性、高并发需求，亟须构建基于共识规则的可信环境。

2. 数据应用的“效能困境”

现有数据基础设施存在“三低”短板：

- 互通效率低：政务、金融、工业三大重点领域数据空间占比超 52.5%，但平台间因技术标准不统一难以互联互通；

- 场景适配低：实体企业数字化转型进入“数据流通赋能”第三阶段，但医疗、能源等行业因数据格式异构、协议差异导致协同效率低下；
- 价值转化率低：据调研，数据流动量每增加 10%可带动 GDP 增长 0.2%，但对各行业利润的平均促进率仅 10%左右，需通过可信机制提升数据要素的乘数效应。

3. 数据安全的“合规困境”

数据跨境流动、隐私泄漏风险加剧监管复杂性。例如，欧盟通过 GAIA-X 计划构建行业数据空间核心平台，美国科技企业推出数据空间沙盒环境，均以技术主权争夺为导向。我国虽出台《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》，但在执行层面仍面临两难：

- 技术层面：隐私计算、区块链等核心技术的自主可控性不足，数据脱敏与可用性难以兼顾（如医疗数据共享需动态脱敏但可能失真）；
- 机制层面：数据权属划分、收益分配规则缺失，导致企业间协作动力不足

4.可信数据空间：破解困局的中国方案

为应对上述挑战，可信数据空间（Trusted Data Space,TDS）应运而生。其本质是以共识规则为基石、技术赋能为支撑、生态协同为目标的下一代数据基础设施，核心价值在于：

- 构建信任基座：通过区块链存证、智能合约、数字身份认证

实现数据“权属清晰、用权可控、维权可溯”，降低流通信任成本；

- 激活要素效能：依托确定性网络技术（如 SRv6 可编程路由、意图驱动网络）绑定 SLA 服务质量，确保工业质检等场景端到端时延 $\leq 10\text{ms}$ 、算力可用性 $\geq 99.9\%$ ，支撑实时决策；
- 驱动生态革新：分企业、行业、城市、个人、跨境五类场景推进，如长虹供应链金融平台整合应付账款数据赋能中小微企业信用增值，济南财金集团通过城市数据空间实现全流程风控。

国家数据局《可信数据空间发展行动计划（2024—2028 年）》明确提出：到 2028 年建成 100 个以上可信数据空间，培育数据产业集群，激活万亿级市场潜能。这一战略部署标志着我国数据要素市场化改革从“概念验证”迈入“规模落地”新阶段，为智能体协同、产业数字化转型提供关键基础设施支撑。

（二）确定性网络与智能体技术的融合价值

在数字经济迈向纵深发展的关键阶段，确定性网络与智能体技术的深度融合，正成为破解数据要素流通“效能—安全—信任”三角难题的核心引擎。这一融合不仅重构了数据价值的释放路径，更推动了从“数据互联”到“智能协同”的范式跃迁，其价值主要体现在三大维度：

1. 技术协同：构建智能体实时决策的“神经中枢”

智能体的核心能力在于感知环境、规划任务并自主执行，其决策

效率高度依赖数据的实时性与可靠性。传统“尽力而为”网络难以满足毫秒级响应的工业控制、金融交易等场景需求，而确定性网络通过时延上限保障（端到端 $\leq 10\text{ms}$ ）、微秒级抖动控制（ $< 5\mu\text{s}$ ）及超高可靠性（丢包率 $< 0.001\%$ ）三大核心特性，为智能体提供了可量化、可验证的底层支撑：

- **强确定性保障**：在工业质检场景中，基于 TSN（时间敏感网络）的确定性调度机制，将机械臂控制指令的端到端时延压缩至 1ms 内，使智能体响应速度提升 20 倍，误操作率趋近于零；
- **资源动态适配**：通过意图驱动网络（IDN）技术，智能体可基于任务需求（如大模型训练需高带宽、自动驾驶需低时延）自动生成网络切片策略，实现“任务—资源—质量”的强一致性匹配；
- **算网一体调度**：光电融合确定性网络支持 2000 公里无电中继无损传输，使分布式的“东数西算”资源池化为智能体提供“一跳入算、一键调算”的全局算力供给，算力利用率提升 40% 以上。

2. 应用赋能：激活垂直行业的“智能生产力”

融合技术正从实验室走向产业核心场景，重构生产流程与商业模式：

- **工业制造**：海上油田钻井平台 PLC 控制智能体通过确定性网络绑定云化 PLC SLA，PLC 升级效率提升 20 倍，大大减少

现场施工作业人数，实现无人化 PLC 远程升级维护；

- **金融科技：**基于可信数据空间的跨机构风控智能体，依托 TEE（可信执行环境）与确定性切片技术，在保障原始数据“可用不可见”的前提下，实现征信查询时延 $\leq 15\text{ms}$ ，欺诈识别效率提升 35%；
- **城市治理：**铁路 IP 通信网采用 K 级物理切片技术，在列车定位、调度、监控多业务融合承载中，将发车间隔缩短至 2 分钟，定位精度控制在 15 米内，客运效率提升 50%；
- **医疗健康：**远程手术智能体依赖确定性网络实现 4K 影像传输与机械臂控制的同步，端到端时延 $\leq 5\text{ms}$ ，为跨地域精准医疗提供技术基座。

3. 生态重构：奠定可信数据空间的“规则底座”

融合技术通过“技术标准化+权属契约化”双路径，构建数据要素市场化流通的信任基石：

- **SLA 驱动的可信契约：**在清雁科技“可信智能体空间”中，智能体操作权限与数据使用权通过智能合约确权，并绑定确定性网络 SLA 参数（如时延、带宽、可靠性），任何违例行为自动触发链上清算与惩罚机制，实现“权责可追溯、违约可仲裁”；
- **跨域协同的信任传递：**依托 MCP（模型上下文协议），异构智能体可在统一框架下调用不同平台的数据与工具，而确定性网络为跨域交互提供时延与丢包率承诺，确保协同任务（如

供应链多智能体联合排产)的确定性执行;

- 价值闭环的经济模型:智能体通过加工数据生成新知识(如优化算法、决策模型),经算力验证后反馈至数据空间,形成“数据增值→算力消耗→智能体进化”的闭环生态,并通过分布式清算体系实现微服务交易的实时结算。

4.迈向“确定性智能”的新范式

确定性网络与智能体技术的融合,标志着数据基础设施从“连通能力”向“数智能力”的质变:

- 短期(2025-2026),聚焦工业互联网、智慧金融等高价值场景,以SLA绑定机制实现95%以上的任务确定性保障;中期(2027-2028),构建空间互联的算力调度网,支撑智能体“一点接入、全局协同”的泛在化应用;
- 长期(2028+),形成与数字生产力匹配的算网生产关系,为星地协同、元宇宙等泛在场景提供“零信任+强确定”的双重保障。

(三)白皮书目标与核心愿景

本白皮书以确定性网络技术为核心引擎,以智能体可信数据空间为载体,旨在构建支撑国家数字竞争力与驱动产业质效跃升的战略性基础设施。其核心目标体系围绕三大维度展开:

1、在支撑国家战略层面

白皮书聚焦破解“东数西算”工程中跨域算力协同的确定性瓶颈。传统广域网络因时延抖动与丢包问题,导致2000公里级算力传输带

宽利用率不足 20%，严重制约多模态大模型训练、科学装置数据的实时处理效率。确定性网络通过微秒级抖动控制与零丢包保障，将跨域无损传输效率提升至 88%，为 FA 射电望远镜（日数据量 2000TB）、散裂中子源（日数据量 600TB）等大科学装置提供协同分析基础。同时，通过自主研发广域确定性大网操作系统（CNOS）及异厂商设备互联互通技术（如华为与新华三异构组网），推动中国主导的 DetNet、FlexE 标准成为全球广域网核心规范，奠定技术主权与标准话语权。

2、在推动产业升级层面

白皮书重点赋能三大高价值场景：

- 工业制造领域：依托确定性内网（TSN：时间敏感网络）+确定性外网技术实现机械臂控制指令端到端时延 $\leq 1\text{ms}$ ，误操作率趋近于零，使汽车生产线良品率提升 15%、设备协同效率提高 20%。
- 医疗健康领域：确定性网络支撑跨域手术机器人精准操控，端到端时延压缩至 5–6ms，时延抖动 $< 20\mu\text{s}$ ，使青岛大学附属医院远程肾脏切除手术成功率与现场操作持平，推动优质医疗资源全域共享。
- 智慧交通领域：基于 K 级物理切片技术承载车路协同数据流，实现车辆定位精度 15 米、发车间隔缩至 2 分钟，综合提升路网通行效率 16%，事故率下降 25%。

3、在技术架构层面，白皮书提出“三层融合”体系：

- 资源层

整合 FlexE 硬切片（100G~400GE）、5G 确定性网络（99.9999% 可靠性）、TSN 微秒级整形等关键技术，打通“有线+无线”“局域+广域”的多维保障通道；

- 控制层

构建意图驱动网络（IDN）操作系统，将业务语义（如“AI 训练需高带宽”“远程控制需低时延”）自动转化为网络切片策略，资源匹配效率提升 40%；

- 应用层

开放智能体即服务（AaaS）接口，通过联邦学习、TEE 可信执行环境实现数据“可用不可见”，激活跨域协同价值。1

4、面向未来，白皮书规划三阶段愿景蓝图：

- 近期（2025–2026）：建成 10 个区域级智能体可信数据空间枢纽，在高端制造、远程医疗领域实现 95% 的任务与确定性网络 SLA 绑定，拉动产业规模超千亿；
- 中期（2027–2028）：基于确定性网络技术，形成高速数据网互联的可信数据空间，并实现算网协同调度，高速数据网覆盖 80% 核心产业集群，支撑智能体“端-边-云”全局协同，数据流通效率提升 50%；
- 远期（2028+）：构建与数字文明匹配的算、网、智生产关系，赋能星地协同、元宇宙等泛在智能场景，最终实现“数据要素零壁垒、智能协作无时滞”的数字中国终极目标。

目 录

前 言	I
目 录	X
一、基于确定性网络的智能体可信数据空间概述	1
1.1 概念定义	1
1.2 核心挑战	4
1.3 确定性网络的赋能作用	5
1.4 国内外趋势与实践	8
二、技术基石（一）：确定性网络体系	11
2.1 概念定义	11
2.2 关键能力指标	17
2.3 标准化进展	21
三、技术基石（二）：智能体可信数据空间体系	23
3.1 概念定义	23
3.2 关键能力指标	24
3.3 标准化进展	25
四、基于确定性网络的智能体可信数据空间架构设计	26
4.1 系统框架	26
4.2 核心机制	28
4.3 数网协同模型	31
五、典型应用场景与需求	34

5.1 智能制造可信协同	34
5.2 能源电力数据互联	37
5.3 公共数据可信交互	41
5.4 智慧城市智能体交互	43
5.5 车联网可信生态	46
5.6 元宇宙在线教育	50
六、关键技术实现路径	52
6.1 确定性网络部署	52
6.2 算力协同部署	54
6.3 数据空间可信引擎	56
6.4 智能体协同协议	57
七、产业实践案例	59
7.1 “江宁政企通 2.0”	59
7.2 菲尼克斯云化 PLC 智能体	62
7.3 杭州市“城市大脑”公共数据智能体应用项目	65
八、发展建议与展望	66
8.1 产业生态构建	66
8.2 标准体系推进	68
8.3 未来方向	69
附录 A：术语与缩略语	70

一、基于确定性网络的智能体可信数据空间概述

1.1 概念定义

1.1.1 智能体可信数据空间的内涵与特征

智能体是指能够感知环境并采取行动以实现特定目标的代理体。它可以是软件、硬件或一个系统，具备自主性、适应性和交互能力。本白皮书中指的智能体是在可信数据空间中的应用。

智能体可信数据空间是一个逻辑空间，它以智能体为核心，围绕智能体相关的数据、智能体本身以及智能体运行所需的算力资源进行组织和管理。其内涵包括以下几个方面：一是数据的安全存储与可信共享，确保数据在智能体之间的流通不会泄露或被篡改；二是对智能体的严格管控，防止恶意智能体进入数据空间造成破坏；三是智能体之间高效协同的机制，促进不同智能体之间无缝协作。

1.1.2 智能体流通利用的核心技术、特点、特征

其特征主要体现在三个维度：安全维度，通过加密技术、身份认证和访问控制等手段构建全方位安全防护体系；可控维度，实现对智能体行为的精准管控以及数据流通的有序调度；协同维度，设计智能体之间的交互协议和协同工作模式，打破智能体之间的沟通壁垒。

1.1.3 智能体可信数据空间与传统数据空间体系的差异

与传统数据空间体系相比，智能体可信数据空间有显著差异。传统数据空间更多关注数据的存储和静态管理，而智能体可信数据空间聚焦于智能体全生命周期动态管理，涵盖智能体的创建、运行、交互和消亡等各个环节。例如在工业自动化场景中，传统数据空间只是存储生产流程数据，智能体可信数据空间则会将参与生产的智能机器人、自动化控制系统等智能体纳入管理，实时监控智能体运行状态，动态调整智能体工作参数，优化生产流程。

1.1.4 基于确定性网络技术的智能体可信数据空间准确定义

基于确定性网络技术的智能体可信数据空间，是一种以确定性网络为基础设施支撑，以智能体为核心流通载体，融合算网协同调度、区块链、隐私计算等技术的新型数据基础设施。它通过构建“技术—规则—生态”三位一体的可信体系，实现智能体全生命周期管理与跨行业、跨域协同价值释放，是数字经济时代打通“数据—算力—网络—智能应用”的闭环的关键载体。

从技术架构看，其核心特征体现为“三基融合”：以确定性网络提供端到端时延 $\leq 10\text{ms}$ 、抖动 $< 5\mu\text{s}$ 、丢包率 $< 0.001\%$ 的基础设施能力基座，确保智能体实时交互的确定性；以区块链存证与智能合约构建信任基石，实现智能体身份认证、数据权属界定、操作行为溯源的全流程可信；以多级算力协同（如“东数西算”场景中“1-5-20”算力

网协同调度)支撑智能体动态算力需求,形成“数据跟着任务调度走、网络随着数据传输开”的资源适配机制。

从功能目标看,基于确定性网络技术的智能体可信数据空间聚焦三大核心价值:一是破解智能体跨域协同的信任壁垒,通过数字身份统一认证、数据“可用不可见”(如联邦学习、TEE 可信执行环境)等机制,打破“数据孤岛”与“协作壁垒”;二是提升数据要素流通效能,依托确定性网络 SLA 绑定(如工业场景算力可用性 $\geq 99.9\%$)与动态切片技术,实现医疗、工业等垂直领域的高并发、低延迟数据交互;三是构建可持续生态,通过智能合约自动执行收益分配、分布式清算体系实时结算,形成“数据增值—算力消耗—智能体进化”的价值闭环。

与传统数据空间相比,其创新性在于:将网络确定性从“尽力而为”升级为“可量化承诺”,使智能体实时决策具备技术保障;将管理对象从“静态数据”拓展至“动态智能体”,实现从数据存储向全流程协同的范式跃迁;将安全机制从“被动防护”进化为“内生可信”,通过技术手段与规则体系的深度融合,平衡数据安全与高效利用的双重需求。

1.2 核心挑战

1.2.1 智能体跨域流通的信任壁垒

智能体跨域流通的信任壁垒主要体现在身份认证、数据可信交换和智能体行为规范等方面。在身份认证环节，不同域采用的认证技术标准各异，如生物特征识别、数字证书等，导致智能体跨域时身份难以快速准确核验。在数据可信交换上，跨域数据格式不统一、数据语义不一致，使得智能体难以准确理解来自其他域的数据，影响数据流通的可靠性。

1.2.2 智能体实时交互业务的确定性需求

智能体实时交互业务在时延、抖动和带宽保障层面呈现显著约束。

时延方面，跨域场景下的实时响应要求端到端时延控制在毫秒级阈值内。例如工业控制智能体的指令交互，若时延超过 50ms 可能引发设备协同失误，而自动驾驶领域的紧急避障交互更需将时延压缩至 10ms 以内，否则会导致决策滞后风险。

抖动控制同样关键，不同域网络环境的动态波动会引发时延抖动，当抖动幅度超过平均时延的 20% 时，智能体的动作协同将出现相位偏移，如远程手术机器人的操作精度会因抖动超出 0.5ms 而显著下降。

带宽保障需满足双向动态适配，既要支撑高清环境数据的实时传输，又要在多智能体并发交互时保障带宽分配的确定性，避免因带宽争抢导致关键指令丢包率超过 0.1% 的临界值。

1.2.3 异构算力系统兼容性问题

智能体业务依赖底层算力，而目前各个算力中心存在算力异构的问题，主要体现在架构适配、指令集互通和资源调度协同等方面。在架构适配环节，不同算力系统采用的底层架构存在差异，如 CP 的 x86 架构与 ARM 架构、GPU 的 CUDA 架构与 OpenCL 架构，导致跨系统部署的程序难以高效运行。在指令集互通上，各类算力单元的指令集标准不统一，如专用 ASIC 芯片的定制化指令与通用处理器指令无法直接兼容，使得数据处理流程出现中断。而在资源调度层面，不同系统的调度算法和接口协议存在差异，导致多算力协同时出现资源分配冲突，影响整体计算效率。

1.3 确定性网络的赋能作用

1.3.1 未来网络相关算网基础情况

（1）网络设施情况

CENI 作为我国在通信与信息工程领域的唯一的国家重大科技基础设施，其建设将覆盖包括国内 40 个主要城市，包含 88 个主干网络节点、133 个边缘网络试验节点，以及 4 大云数据中心，目标为建设成一个先进的、开放的、灵活的、可持续发展的大规模通用试验设施，满足“十三五”和“十四五”期间国家关于下一代互联网、网络空间安全、天地一体化网络等重大科技项目的试验验证需求，获得超前于产业 5~10 年的创新成果。CENI 的建设对于我国未来网络领域具有

重大意义，从学术界角度，可提供一个大规模虚拟化网络环境，作为高校、科研院所科研人员的网络技术创新验证平台，显著增强创新成果的国际认可度；从产业界角度，可为运营商的新型网络服务部署、设备商新设备的大规模测试、互联网公司的新型网络业务提供测试平台和应用基础环境。

CENI 的整体架构分为主干网、边缘网，以及云数据中心。CENI 的光传输网络已建成 80 波、单波 100G 传输系统，且可以通过更换电层板卡平滑升级到 400G 系统。CENI 数通网络包括 SDN、可编程路由器、确定性三个平面，三平面的架构能够为业务提供高冗余、高可靠的保障。CENI 可以根据业务的不同需求，进行定制化的路由规划和网络优化，提供从 3 个 9 到 5 个 9 不同等级的业务可用率保障。CENI 主干网连接了全国 40 个主要城市。CENI 中的各个域的网络，都将通过网络操作系统 CNOS（China Network Operating System）进行集中式的管理，以及跨域的协同编排与调度。在此基础上，CENI 试验服务平台与管理系统将作为 CNOS 的关键应用，向试验用户提供自助式的一站式试验服务，可为 L0-L7 层的全层次、多场景的网络与网络安全的创新技术与应用，提供先进、开放、灵活、高速、可靠的试验环境。

（2）基于 CENI 的全国多元异构算力直连网

2023 年 7 月，未来网络集团启动基于 CENI 的全国多元异构算力直连网项目建设。按照“以网补芯”策略，该项目以 CENI 网络为大动脉，连接全国八大算力枢纽节点，形成建设技术上国际领先、安

全上自主可控、产业上协同创新的高速算力直连网，力图破解数据中心异构、异属、异域带来的协同难题，提供超大算力、超大带宽、低时延、低抖动、按需定制、分钟开通的个性化算网服务。同时构建算网调度中心协同东西部算力、网络调度，统筹应用、任务的跨区域分发，支撑数据、内容的高可靠流动，在全国范围内有序疏导智能应用“西训东推”、温冷数据“东数西存”，满足工业互联网、远程医疗、虚拟现实/增强现实、车联网等一线/近一线、高频/实时交互型的业务需求，加速集聚算力产业上、中、下游不同环节产业集群，为区域经济高质量发展提供新质生产力。

1.3.2 提供“可信可靠、高速互联、泛在连接、高度弹性、灵活计费”的数据传输基座

未来网络开发的数据传输基座以“可信可靠”为核心基石，采用加密技术与多节点备份机制，确保数据在传输全链路中不泄露、不丢失，为金融交易、医疗档案等敏感信息提供坚实安全屏障。

“高速互联”是核心优势，依托全光网络架构与智能路由算法，实现跨区域数据传输延迟低至毫秒级，大文件传输效率提升 300%，满足实时交互场景需求。

“泛在连接”特性打破设备与场景壁垒，支持物联网终端、云端服务器、边缘节点等多类型设备无缝接入，构建全域覆盖的数据交互网络。

“高度弹性”能力可根据业务负载智能扩容，峰值时段自动提升

带宽资源，低谷期灵活收缩，避免资源浪费。

创新的“灵活计费”模式按实际用量精准结算，提供按需付费、套餐包、阶梯定价等多元选择，大幅降低企业运营成本。

1.4 国内外趋势与实践

1.4.1 国外数据空间发展趋势

在国际上，数据空间的发展已经成为数字经济发展的重要驱动力。欧美等发达国家纷纷制定战略和政策，推动数据空间的建设和发展。例如，欧盟提出了“欧洲数据空间”计划，旨在建立一个统一、安全、可信的数据共享框架，促进成员国之间的数据流通和协同。美国则通过“联邦数据战略”，加强对政府数据的管理和利用，推动数据的开放共享，以促进创新和经济增长。此外，国际组织如 G20 和 OECD 也在积极推动全球数据治理框架的构建，以应对数据跨境流动、数据隐私保护等全球性挑战。

1.4.2 国外数据空间应用情况

国外的数据空间应用已经涵盖了多个关键领域。在医疗领域，数据空间的应用促进了电子健康记录的共享和远程医疗服务的发展，提高了医疗服务的可及性和效率。金融行业则利用数据空间增强风险管理和反欺诈能力，同时提供更加个性化的金融服务。工业制造领域通过数据空间实现供应链的优化和生产过程的智能化，提升了整体生产

效率和竞争力。此外，智能城市项目中，数据空间的应用使得城市管理者能够整合和分析来自不同部门的数据，实现城市资源的精细化管理和高效利用。

1.4.3 国内数据空间发展趋势

国内的数据空间发展同样呈现出快速发展的态势。中国政府高度重视数据作为关键生产要素的作用，出台了一系列政策和法规以推动数据要素市场的建设。例如，“东数西算”工程的启动，旨在优化数据中心的布局，提升算力资源的利用效率，促进数据的跨区域流通和协同处理。与此同时，《要素市场化配置综合改革试点总体方案》的发布，进一步明确了数据要素市场化配置的改革方向，为数据空间的发展提供了政策支持和制度保障。

1.4.4 国内数据空间应用情况

在国内，数据空间的应用实践也在多个领域取得了显著进展。在政务服务领域，各地政府通过建设数据共享交换平台，实现了政务数据的整合和共享，提高了政务服务的效率和透明度。例如，“江宁政企通 2.0”平台就是通过整合政府和企业的数据资源，为企业提供一站式的政策服务和精准的政策推送。在工业领域，工业企业利用数据空间实现生产设备的远程监控和故障诊断，提升生产效率和设备利用率。此外，城市大脑项目中，数据空间的应用使得交通、环境、安防等多个领域的的数据得以融合分析，为城市的智能化管理提供了有力支

持。同时，在金融、医疗、教育等行业，数据空间的应用也在不断拓展和深化，推动了行业的数字化转型和创新发展。

第九届未来网络发展大会白皮书

二、技术基石（一）：确定性网络体系

2.1 概念定义

2.1.1 基于 CENI 的确定性网络

确定性共享服务网络及控制平台，具备数据流通管控、数据流通枢纽、数据流通传输等功能。支持采用先进传输技术进行高速数据传输，通过传输协议优化，1Gbps-400Gbps 带宽场景下，实现 90%以上的传输带宽利用率，包含算网基础设施建设及共享服务网络建设。

数据共享服务网络的业务核心是解决数据流通利用中的数据流通管控、数据流通枢纽、数据流通传输等数据高效、安全传输问题。数据共享服务网络的使用者包括数据提供方和数据需求方，如政府、企业或数商等，也包括数据交易平台、数据交易所等数据交易机构。主要构建思路如下：

普适接入：实现随时随地的网络资源获取，支持多种接入方式，并提供灵活的计费模式。

弹性伸缩：根据数据传输需求动态调整网络资源，实现资源的弹性使用。

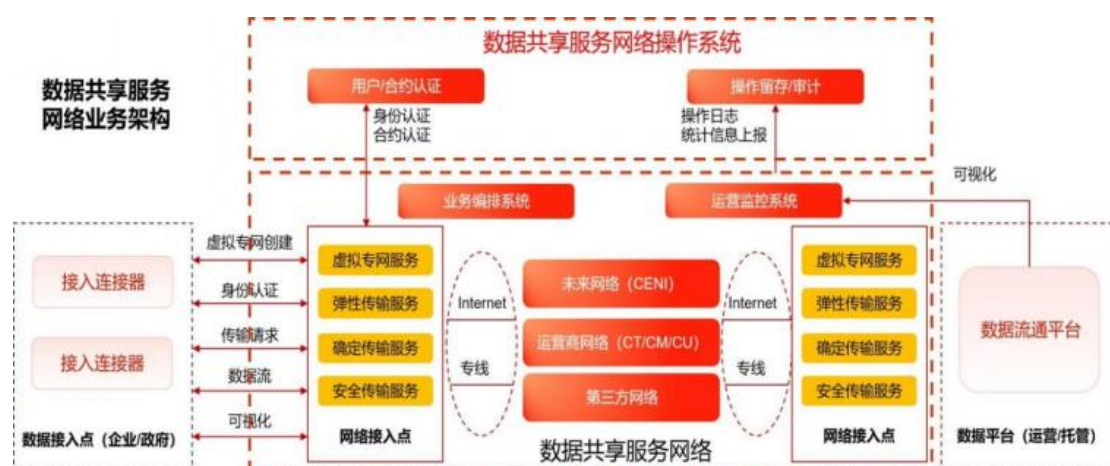
按需保障：允许客户灵活构建、管理和拆除虚拟专网，实现按需的网络连接和策略保障。

确定传输：提供低延迟、低抖动、大带宽、高稳定性，支持端到

端的高通量数据传输。

互联互通：利用已有的网络资源实现单服务商或跨服务商的网络接入。

数据共享服务网络系统架构图如下图所示：



基于未来网络数据共享服务网络基础设施等技术，通过 SRv6 分段路由、资源预留、时频同步、周期映射、门控队列调度、流量过滤和整形、路径规划、SDN 网络态势感知、SDN 智能编排等网络技术保障数据流通参与者大带宽、低时延、低抖动、高可靠等确定性能力需求指标；并通过数据共享服务网络接入层技术，结合数据流通参与者接入需求，通过一张物理网络可以为每个数据流通参与者提供个性化的确定性专网服务，满足不同数据流通参与者对网络的不同诉求。

为满足不同用户业务的差异化 SLA 资源隔离、灵活定制拓扑和智能切片管理的需求，同时利用 FlexE 技术、子接口切片技术和 Slice ID 等切片技术来实现在物理网络上划分逻辑网络的功能。

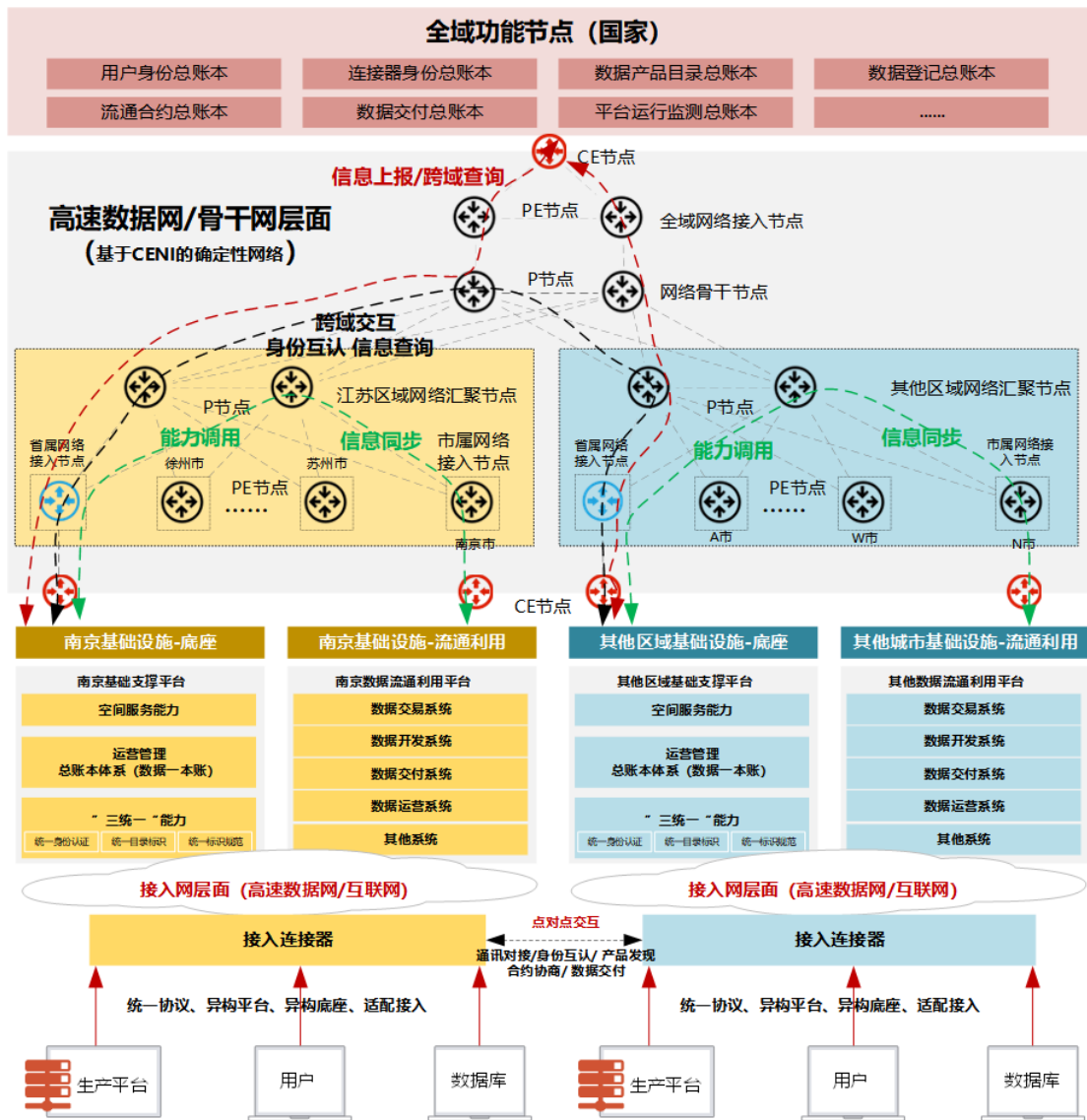
2.1.2 骨干层

骨干层作为确定性网络体系的核心脊梁，肩负着实现国家数据基础设施试点城市底座互联互通的重任。它构建起了城市间数据流通的高速通道，将各个分散的试点城市数据基础设施紧密相连。在这一层次中，采用了先进的网络技术和架构设计，以保障跨城市数据传输的高效性、稳定性与安全性。

通过在骨干层部署高性能的网络设备，具备光电融合能力的核心路由器、高速率的光传输设备等，能够满足海量数据在城市间快速传输的需求。同时，运用软件定义网络(SDN)和网络功能虚拟化(NFV)等新型技术理念，实现对骨干网络资源的灵活调配与智能管控。当某两个试点城市之间的数据流量突发增长时，SDN 控制器能够根据实时的网络状态信息，动态调整网络路由，将数据流量合理地分配到其他空闲链路，确保数据传输的顺畅，避免网络拥塞的发生。此外，骨干层还通过建立安全可靠的连接机制，采用加密隧道技术对传输的数据进行加密处理，防止数据在传输过程中被窃取或篡改，为国家数据基础设施试点城市底座互联互通提供坚实的安全保障。

基于 CENI 及其全国多元异构算力直连网，新建跨域确定性骨干网，并基于南京城市算力网现有资源，构建城市内（城域）确定性骨干网。其中，跨域部分，构建 1G-100G 弹性带宽的高速数据网络切片方式与国家数据基础设施试点城市如北京、苏州、杭州、温州、天津、福州、赣州广域高速互联骨干网；城域部分，主要利用南京城市算力

网现有资源，以 1*100G 方式在现有 8 个确定性网络接入 POP 点（未来网络 CENI 大厦、麒麟中国科学院、晨光科技园、鼓楼、江北新区、江宁格力基地、烽火祥云、六合化工园）基础上将市内各数据基础设施、数据参与主体就近接入，形成高速互联互通的骨干网。

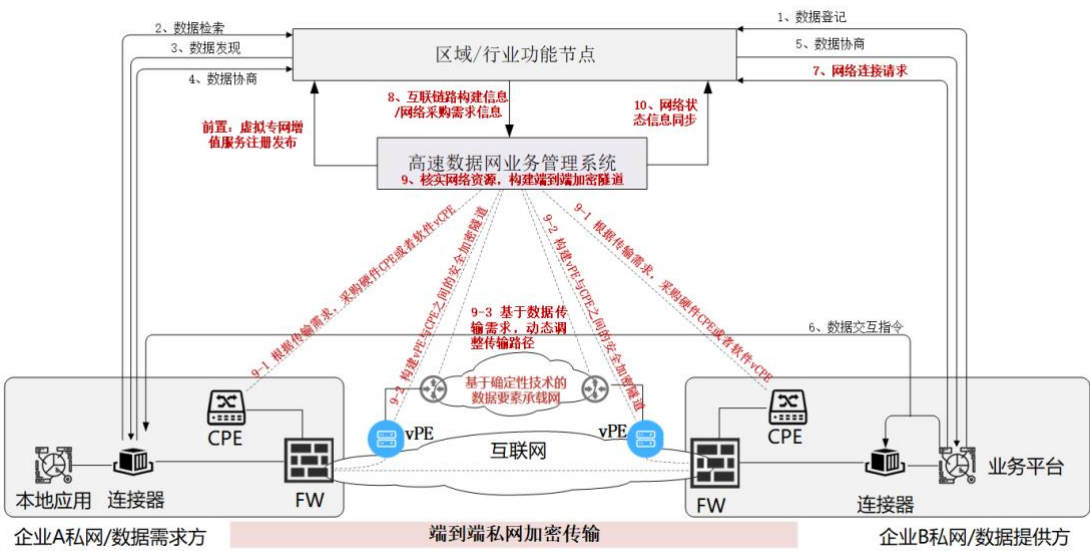


2.1.3 接入网

接入网是确定性网络体系深入到试点城市内部的神经末梢，负责实现试点城市内各个数据基础设施、连接器之间的互联。它如同城市

交通中的毛细血管，将城市内的各种数据节点紧密编织在一起，形成一个有机的数据流通网络。接入网的建设需要充分考虑不同数据基础设施和连接器的接入需求与特点，采用多样化的接入技术。对于一些对网络带宽和实时性要求极高的数据中心等基础设施，可采用光纤直连的方式，提供万兆甚至更高带宽的接入能力，保障数据的高速稳定传输。而对于分布较为分散、数据流量相对较小的连接器等设备，可利用 Internet 或者专线方式接入基于 CENI 的确定性数据共享服务网络，完成数据流通利用的数据流量传输需求。

南京市接入网络骨干层面构建 10Gbps 硬隔离的专网平面，满足南京市本地的数据流通利用用户的网络传输需求，并根据数据流通利用基础设施用户行业开设 N 个软隔离的网络切片，共享 10Gbps 的网络传输资源。



基于用户的接入连接器物理形态和部署方案，接入网方案可以分为：

1、软件形式+SAAS 云化部署：接入连接器统一部署在“政务云”中，各企事业单位通过 Internet 或者“云”专线的方式与接入连接器实现互通。数据交易双方的接入连接器通过“基于 CENI 的确定性数据共享服务网络”实现数据的流通和交易。

2、硬件形式+属地化部署：接入连接器统一部署在企事业本地，通过部署“SD-WAN 确定性网关”设备，采用 Internet 或者专线形式实现与“基于 CENI 的确定性数据共享服务网络”互联互通，最终实现数据交易双方的数据流通和交易。

3、数据交易的参与方采用不同的部署方式：一方采用 SaaS 云化部署，另一方采用属地化部署。为了实现双方的互联互通和数据流通，云化部署用户通过 Internet 或“云”专线接入“政务云”，并利用“基于 CENI 的确定性数据共享服务网络”实现数据交易双方的高效数据流通和交易。

2.1.4 算力网

算力网在确定性网络体系中扮演着连接各城市算力中心与数据基础设施、连接器的重要角色，是实现算力与数据高效协同的关键纽带。在当今数字化时代，数据处理与计算需求日益增长，算力网能够将城市中的算力资源进行整合与优化配置，使其与数据的产生、存储和流通环节紧密结合。

依托试点城市算力网平台，实现对异构、异属、异域城市算力的统筹纳管。基于 CENI 确定性网络能力，可为千行百业打造安全可信、

灵活可控、质量确定、高性价比的传输网络，支撑数据汇聚和数据流通。通过算力网，数据基础设施和连接器产生的数据可以快速传输到相应的算力中心进行处理，而算力中心处理后的结果也能及时反馈回数据基础设施和连接器，实现数据与算力的无缝对接。例如，在人工智能模型训练场景中，数据基础设施收集到的大量训练数据通过算力网迅速传输到算力中心，利用算力中心强大的计算能力进行模型训练，训练完成后的模型参数又通过算力网传回到数据基础设施，为后续的应用提供支持。同时，引入了算力感知的路由算法，能够根据各算力中心的负载情况和网络状态，智能地选择最优的路径传输数据，提高算力资源的利用效率，保障数据处理任务的高效执行。

2.2 关键能力指标

2.2.1 时延分级模型（Level-1 至 Level-5）

时延分级模型将网络时延划分为五个级别，从Level-1 到 Level-5，时延要求逐渐降低，以满足不同快速响应场景的需求。

Level-1: 这是对时延要求最为苛刻的级别，主要应用于如远程手术、工业自动化中的高精度实时控制等场景。在远程手术中，医生的操作指令需要实时、准确地传输到手术器械端，任何微小的时延都可能导致手术操作的偏差，危及患者生命安全。因此，Level-1 要求网络时延能够控制在亚毫秒级，确保指令的瞬间传递，实现手术操作的精准同步。

Level-2: 适用于自动驾驶等场景。在自动驾驶过程中，车辆需要实时感知周围环境信息，如其他车辆的位置、速度等，并迅速做出决策。网络时延如果过大，车辆可能无法及时响应突发情况，引发交通事故。所以，Level-2 要求时延在 1-5 毫秒之间，保障车辆对环境变化的快速响应，确保行驶安全。

Level-3: 常见于高清视频实时互动、云游戏等场景。在高清视频实时互动中，如远程视频会议、在线教育直播等，参与者希望看到的画面和听到的声音能够实时同步，没有明显的延迟，以保证沟通的顺畅性和体验的沉浸感。云游戏则需要将玩家的操作指令快速传输到云端服务器，同时将服务器处理后的游戏画面及时反馈给玩家，Level-3 的时延控制在 5-10 毫秒，基本能够满足这类场景对实时性的要求。

Level-4: 对于一些对实时性有一定要求，但相对宽容的场景，如智能家居设备的远程控制等适用。用户通过手机APP控制家中的智能灯光、窗帘等设备时，虽然希望设备能够快速响应，但短时间的延迟并不会对使用体验造成严重影响。Level-4 的时延范围在 10 - 20 毫秒，能够较好地平衡网络成本与用户体验。

Level-5: 适用于一般性的数据查询、文件下载等对实时性要求较低的场景。在这些场景中，用户可以接受一定程度的等待时间，Level-5 的时延在 20 毫秒以上，能够在保证基本服务质量的前提下，更高效地利用网络资源。

2.2.2 抖动控制边界（ μs 级精度）

在工业控制场景中，抖动控制边界达到 μs 级精度至关重要。工业控制系统通常需要对生产过程进行精确控制，如在汽车制造的自动化生产线上，机械臂的运动轨迹需要严格按照预设程序执行，任何微小的抖动都可能导致产品质量问题。确定性网络通过一系列技术手段实现 μs 级精度的抖动控制。

一方面，在网络设备的硬件设计上，采用高性能的时钟同步芯片，确保各个网络节点的时钟精度达到纳秒级，减少因时钟不同步导致的抖动。例如，利用精确时间协议（PTP），通过网络传输精确的时间信息，使网络中的所有设备能够同步到同一时间基准，从而保证数据传输的定时准确性。

另一方面，在网络流量调度方面，采用先进的队列管理算法和流量整形技术。当网络中存在多种不同类型的流量时，通过对不同流量进行分类，并为每种流量分配专门的队列和带宽资源，严格按照预定的速率和时间间隔发送数据，避免因流量突发或争抢资源导致的抖动。例如，对于工业控制中的关键指令数据，给予最高优先级，确保其在传输过程中不会受到其他非关键流量的干扰，从而将抖动控制在极小的范围内，满足工业控制场景对高精度、稳定网络传输的要求。

2.2.3 安全隔离度（硬切片/软隔离）

在可信场景中，安全隔离度通过硬切片和软隔离两种方式保障

数据的安全与可信。

硬切片：硬切片是一种基于物理资源划分的隔离方式，如同在一条高速公路上划分出不同的专用车道。在网络中，通过专门的硬件设备和网络拓扑设计，为不同的业务或用户组分配独立的网络资源，包括独立的链路、网络设备端口、IP地址段等。例如，在金融领域，银行的核心业务系统与其他一般性业务系统之间采用硬切片技术进行隔离。核心业务系统涉及大量敏感的客户金融信息和资金交易数据，通过独立的物理网络链路和设备进行数据传输与处理，与其他业务系统完全隔离，确保核心业务数据的安全性和完整性，防止外部非法网络访问和恶意攻击对核心业务造成影响。

软隔离：软隔离则是基于软件技术实现的逻辑隔离方式。利用虚拟网络技术、访问控制列表（ACL）等手段，在共享的网络基础设施上为不同的业务或用户创建虚拟的隔离空间。以企业内部网络为例，企业的研发部门和销售部门可能使用同一套网络设备，但通过虚拟局域网（VLAN）技术将两个部门划分到不同的虚拟网络中，不同VLAN之间的通信受到严格的访问控制策略限制。只有经过授权的特定数据流量才能在不同VLAN之间进行传输，从而实现部门之间数据的软隔离，既保障了不同部门数据的安全性，又能在一定程度上实现资源共享，提高网络资源的利用效率。在一些对安全性和灵活性要求较高的可信数据共享场景中，软隔离与硬切片技术也可以结合使用，进一步提升安全隔离度，为数据的可信流通提供全方位的保障。

2.3 标准化进展

在确定性网络领域，IEEE和ITU-T等国际标准化组织积极推动相关标准化工作，取得了一系列重要进展。同时，未来网络与紫金山实验室在其中发挥了关键作用。

IEEE方面：IEEE在时间敏感网络（TSN）、确定性WiFi（DetWiFi）等技术标准制定上成果显著。未来网络试验设施（CENI）依托紫金山实验室的科研力量，为IEEE相关标准的实践验证提供了重要平台。TSN作为解决二层网络确定性保障问题的关键技术，IEEE制定了一系列相关标准。例如，IEEE 802.1ASrev精确时间同步协议，通过在CENI网络中的部署测试，确保网络中所有设备实现高精度的时间同步，为数据的确定性传输提供时间基准，其在实际网络环境中的运行效果反馈，助力IEEE对该标准不断优化完善。在IEEE 802.1Qbv标准定义的门控流量调度机制方面，紫金山实验室联合相关科研团队，基于CENI网络进行了大量实验，验证了该机制通过精确控制数据帧的发送时机，避免网络拥塞，实现零拥塞丢包传输的有效性，为该标准在实际应用中的推广提供了有力支撑。对于DetWiFi，IEEE正在制定相关标准以实现无线局域网中的确定性传输。紫金山实验室凭借在无线通信领域的深厚研究积累，参与到DetWiFi标准制定的研讨中，其提出的通过时钟同步、流量调度、帧抢占等技术手段保障WiFi网络在工业互联网、智能办公等场景下确定性服务质量的方案，被纳入IEEE相关标准制定的参考范畴，目前相关标准在不断完善与推进阶段，CENI网络也将持

续为其提供试验环境，加速标准的落地应用。

ITU-T方面：ITU-T在确定性网络标准制定上也发挥着重要作用。紫金山实验室积极参与ITU-T的标准化工作，与全球科研机构和企业协同合作。例如，由北京科技大学牵头，联合中国联通集团、之江实验室等多方共同制定的ITU-T国际标准Y.3126“IMT2020 及演进系统中支持局域确定性通信的互操作能力和服务质量要求及框架”，紫金山实验室在其中贡献了自身在网络架构、性能优化等方面的研究成果，推动该标准针对异构网络间协同支持确定性通信服务，明确相关的服务质量要求及框架，为工业互联网领域的网络技术发展提供重要规范，助力确定性网络在工业场景中的应用。此外，ITU-T持续开展面向未来网络的确定性网络技术标准研究，涵盖网络架构、性能指标、安全机制等多个方面。紫金山实验室凭借在未来网络技术研究上的前瞻性，参与到多项ITU-T标准研究项目中，如在网络架构标准研究中，其提出的新型网络架构理念，强调融合光网络与IP网络优势，实现高效的数据传输与资源调度，为构建全面、系统的确定性网络国际标准体系提供新思路，促进全球范围内确定性网络技术的统一与互联互通。随着这些标准化工作的不断推进，确定性网络技术将在全球范围内得到更广泛的应用与推广，为智能体可信数据空间等新兴应用提供坚实的标准支撑。

三、技术基石（二）：智能体可信数据空间体系

3.1 概念定义

智能体可信数据空间技术是支撑基于确定性网络技术的智能体可信数据空间实现其核心功能与价值的一系列技术集合，是构建该数据空间的底层技术框架与支撑体系。它以确定性网络技术为核心骨架，深度融合区块链、隐私计算、算网协同调度等多元技术，通过技术间的协同联动，为智能体在数据空间内的交互、数据的流通以及跨域协同提供全方位的技术保障。

从技术构成来看，该技术体系涵盖网络传输、信任构建、算力支撑、数据安全等多个维度。其中，确定性网络技术作为底层支撑，为智能体及数据的实时、稳定传输奠定基础；区块链技术通过分布式账本和智能合约，保障数据的不可篡改性和操作的可追溯性，构建起数据空间内的信任机制；隐私计算技术如联邦学习、TEE可信执行环境等，确保数据在“可用不可见”的前提下进行流通与共享，保护数据隐私；算网协同调度技术则实现算力与网络的协同分配，满足智能体在不同场景下的动态算力与网络需求。这些技术相互作用、相互补充，共同构成了智能体可信数据空间高效、安全、可信运行的技术基石。

3.2 关键能力指标

智能体可信数据空间技术的关键能力指标是衡量其技术性能与应用效果的重要标准，主要包括以下几个方面：

网络传输能力：端到端时延需 $\leq 10\text{ms}$ ，以保障智能体实时交互的及时性；抖动 $< 5\mu\text{s}$ ，确保网络传输的稳定性；丢包率 $< 0.001\%$ ，减少数据传输过程中的丢失，保证数据的完整性。同时，具备动态切片技术，能够根据智能体和数据的不同需求，灵活分配网络资源，适应高并发的数据交互场景。

信任保障能力：基于区块链技术，实现智能体身份认证的准确率达到 100%，确保接入数据空间的智能体身份真实可靠；数据权属界定的准确率 $\geq 99.9\%$ ，明确数据的归属，避免权属纠纷；操作行为溯源的完整性达到 100%，任何对数据的操作都能被完整记录和追溯，为责任认定提供依据。

隐私保护能力：采用隐私计算技术时，数据处理的准确率 $\geq 99\%$ ，在保护数据隐私的同时，不影响数据的有效利用；数据泄漏风险趋近于 0，通过严格的技术手段，防止数据在流通和共享过程中被非法获取和泄露。

算网协同调度能力：算力资源的分配响应时间 $\leq 1\text{s}$ ，快速满足智能体的动态算力需求；算力可用性在工业等关键场景下 $\geq 99.9\%$ ，保障智能体持续稳定运行；算力利用率 $\geq 80\%$ ，提高算力资源的使用效率，降低成本。

3.3 标准化进展

智能体可信数据空间技术的标准化工作对于推动其规范化发展和广泛应用具有重要意义，目前在多个领域和组织的推动下取得了一定进展：

网络传输方面：在确定性网络技术领域，相关国际标准化组织如IEEE正在推进TSN（时间敏感网络）系列标准的完善，针对网络传输的时延、抖动、丢包率等关键指标制定了明确的规范，为智能体可信数据空间的网络传输提供了相关的技术标准参考。同时，IETF在SRv6（分段路由IPv6）技术标准化方面也持续发力，致力于提升广域网网络的可编程性和灵活性，以适应智能体可信数据空间动态网络资源分配的需求。

信任与安全方面：区块链技术的标准化工作较为活跃，多个国际标准化组织和行业联盟如ISO、ITU-T以及Hyperledger等都在积极制定区块链相关标准，涉及分布式账本架构、智能合约规范、安全防护要求等内容，为智能体可信数据空间中信任机制的构建提供了标准依据。隐私计算领域，也有不少行业组织和研究机构在推动联邦学习、TEE等技术的标准化，明确技术应用的接口、流程和安全要求，促进隐私计算技术在数据空间中的合规应用。

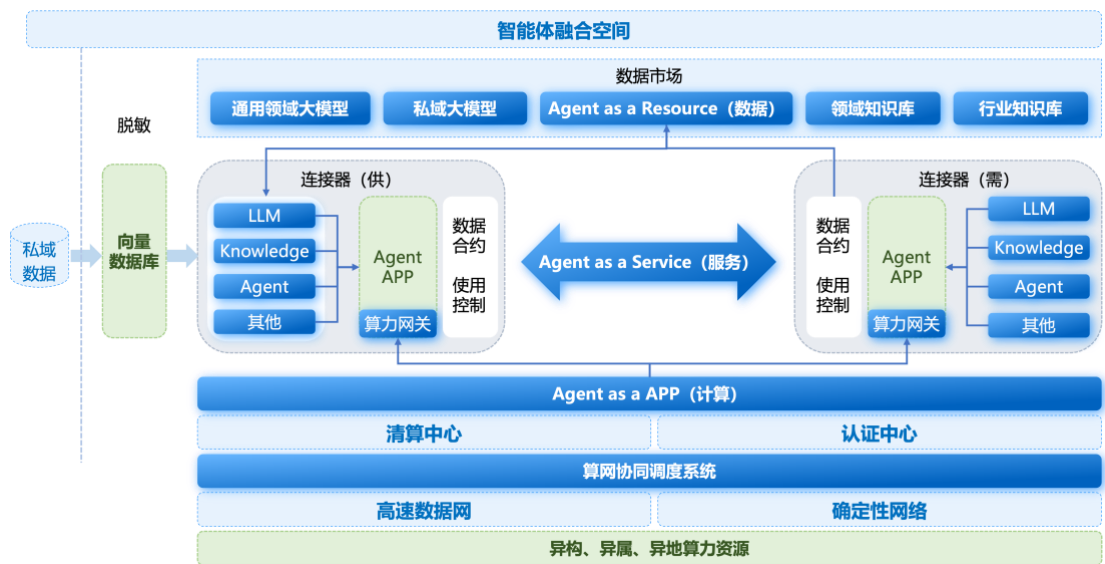
跨域协同方面：针对智能体可信数据空间的跨域协同需求，一些行业联盟和标准化组织正在开展数据空间互联互通标准的研究与制定。例如，在工业领域，相关组织致力于制定统一的数据格式、接口

协议和交互规范，以实现不同企业和部门的智能体可信数据空间之间的顺畅协同。同时，在数据权属、收益分配等方面的标准也在探讨中，为数据空间的可持续生态构建提供标准支撑。

然而，由于智能体可信数据空间技术涉及多个学科和领域，技术复杂且应用场景多样，目前标准化工作仍面临一些挑战，如不同技术领域之间的标准协调难度较大、新兴技术的快速发展使得标准制定难以跟上技术迭代速度等。未来，需要进一步加强跨组织、跨领域的合作与交流，加快标准的制定与更新，推动智能体可信数据空间技术的标准化体系不断完善。

四、基于确定性网络的智能体可信数据空间架构设计

4.1 系统框架



基于确定性网络的智能体可信数据空间旨在构建一个安全、可信、高效的数据交互与智能体服务环境，实现私域数据的安全利用和智能

体之间的协同服务，促进通用领域大模型、私域大模型等数据资源的高效流转与应用，满足不同用户对于数据处理和智能服务的需求。

4.1.1 数据层

数据层负责智能体相关数据的存储与区块链存证。一方面，采用分布式存储技术，将智能体数据分散存储在多个节点上，确保数据的高可用性和容灾能力；另一方面，利用区块链技术对数据的产生、流转、使用等过程进行存证，保证数据的不可篡改和可追溯性。

4.1.2 控制层

控制层涵盖可信数据空间相关的策略引擎、智能合约等层次。策略引擎根据预设规则对智能体行为、数据访问等进行动态管控，例如，基于智能体身份和数据敏感度制定差异化访问权限策略；智能合约则实现智能体之间约定事项的自动执行，当智能体达成数据交易或协同任务共识时，智能合约自动触发相应操作，提升智能体协作效率。

4.1.3 算力层

算力层为智能体运行提供所需的算力资源。依据智能体类型和任务负载，在云端、边缘端合理配置算力资源。对于需要处理海量数据和复杂计算的智能体，如人工智能训练智能体，分配强大云端算力资源；对于实时性要求高、靠近数据源的智能体，如物联网边缘智能体，就近提供边缘算力支持。

4.1.4 网络层

网络层实现确定性控制、传输管道功能。引入确定性网络技术，确保智能体数据传输具备低时延、低抖动、高带宽等特性，满足智能体实时交互业务需求。例如，在工业自动化生产线场景中，网络层为控制智能体与执行智能体之间的数据传输打造确定性传输管道，保障生产指令的精准下达和执行反馈的及时上传。

4.2 核心机制

4.2.1 智能体可信认证：

智能体可信认证基于数字身份的访问控制，为每个智能体创建唯一数字身份，该身份包含智能体基本信息、权限属性等内容，并采用加密技术对数字身份进行保护。当智能体请求访问数据或与其他智能体协同工作时，通过对数字身份的认证来判定其访问合法性。

4.2.2 智能体数据确权：智能体相关数据的权属标识与溯源追踪

智能体数据确权是对智能体相关数据的权属标识与溯源追踪。明确数据的归属主体，是数据拥有者还是数据生成者等，并记录数据的生成、流转、使用等全生命周期信息，以便在数据纠纷或安全事件发生时能够快速溯源。

4.2.3 智能体确权：智能体本身的权属标识与溯源追踪

智能体确权聚焦于智能体本身的权属标识与溯源追踪，确定智能体的开发者、所有者以及运营者等权属关系，并对智能体的开发、部署、运行等环节进行溯源，确保智能体的合法性和可控性。

4.2.4 算网协同：数据、智能体确权后，算网资源的协同

智能体可信数据空间中的算网协同是指在数据权属与智能体操作权限双重确权（基于区块链存证与智能合约实现权属清晰化、操作可控化及维权可溯化）的基础上，通过计算资源（云/边/端异构算力）与网络资源（5G/6G、SRv6 可编程路由）的深度融合调度机制，以任务需求（如 AI 训练、实时决策）为驱动核心，依托算网大脑（集成 DRL 强化学习引擎）动态适配最优算力节点与网络路径（实现“算随需动、网随算变”），并融合意图驱动网络（IDN）将业务语义转化为资源策略（如工业质检任务毫秒级响应需优先调度边缘 GPU 算力与低延时切片），同时在安全维度采用隐私计算（联邦学习/TEE）、数据沙箱保障原始数据“可用不可见”，通过网络切片与服务功能链（SFC）实现高敏感任务资源隔离与 SLA 合规性，最终构建“计算—网络—数据—智能体”四维一体的可信环境，形成数据增值→算力消耗→智能体进化→价值反馈（经分布式清算体系实时结算）的闭环生态，以技术重构信任机制，在确权与安全双约束下最大化资源效能，实现“数据流动不失控、智能协作不失序”的数字生态愿景。

4.2.5 QoS 保障：可信认知、确权过程中确定性网络 SLA 绑定

在智能体可信数据空间内，QoS（服务质量）保障是指通过确定性网络 SLA（服务水平协议）绑定机制，在数据与智能体完成可信认知（基于区块链存证与智能合约实现身份认证与行为审计）及双重确权（数据持有权与使用权分离）的前提下，将网络性能指标（如时延、带宽、可靠性）与算力调度策略（如边缘节点响应速度、GPU 算力分配）转化为可量化、可监测、可仲裁的 SLA 合约条款，并依托意图驱动网络（IDN）动态生成网络切片策略与服务功能链（SFC），实现“任务—资源—质量”的强一致性匹配：具体而言，在智能体执行协同任务（如联邦学习、实时决策）过程中，SLA 条款明确约束数据传输路径的端到端时延上限（如工业质检任务需 $\leq 10\text{ms}$ ）、算力节点可用性（如 $\geq 99.9\%$ ）、数据流安全隔离等级（如金融风控场景需独占切片）等关键参数，并通过动态信任评估模型实时交叉验证云端与客户端监测数据（如时延抖动、丢包率），结合隐私计算（TEE/联邦学习）保障原始数据“可用不可见”的同时，对 SLA 违例事件（如算力超时、带宽不足）触发自动清算与惩罚机制（如智能合约扣减信用积分或执行经济赔偿），最终形成“确权驱动 SLA 生成、SLA 绑定资源调度、动态验证闭环反馈”的 QoS 保障体系，确保智能体协作任务在安全可信、性能可预期、权责可追溯的框架内高效执行。

4.3 数网协同模型

4.3.1 云边端三级算力调度

云边端三级算力调度方案通过构建云端统筹、边缘协同、终端执行的一体化算力网络，实现算力资源的精准匹配与高效利用，为智能体应用提供弹性可靠的算力支撑。该方式打破传统算力孤岛格局，让算力像水电一样按需调配，满足不同场景的算力需求。

云端作为全局算力调度中心，负责全域算力资源的监控、分析与决策。边缘节点分布在园区、厂房、学校等靠近终端的位置，形成分布式算力集群，承担本地化数据处理与实时响应任务。终端设备布置在智能体应用现场，如政务大厅等，形成层次分明的算力梯队。

核心功能方面，方案具备智能感知、动态调度、协同计算三大能力。智能感知系统通过实时监测各节点的算力负载、网络带宽、能耗状态等关键指标，精准识别算力供需缺口。动态调度机制基于 AI 预测模型，在毫秒级时间内完成算力资源的最优分配，当边缘节点负载过高时自动向云端或邻近节点请求算力支援，终端设备则根据任务复杂度自适应调用本地或边缘算力。

通过优化的粒子群优化算法，实现全局算力分配的最优解，调度延迟控制在 50 毫秒以内。边缘计算框架支持容器化部署与微服务架构，可快速部署 AI 推理、数据过滤等本地化服务。云边协同协议采用轻量化设计，在任何网络环境下都能保持 99.9% 的通信可靠性。

4.3.2 高速数据网络

高速数据网络指面向数据流通利用场景，依托网络虚拟化、软件定义网络等技术，提供弹性带宽、安全可靠、传输高效的数据传输服务，具有高带宽、低延迟、高可靠性、高安全性、可扩展性、灵活性等特点。



高速数据网管理系统可集中配置私网地址映射规则，将可信数据空间中的连接器公网暴露 IP 转为内网私有地址。通过动态 NAT 技术，所有对外通信经网关公网接口中转，隐藏后端连接器真实 IP，规避公网扫描风险。同时系统支持一键部署地址转换策略，简化配置流程，在保障安全隔离的同时，确保数据流通链路的稳定性。

4.3.3 数算网协同

数算网协同以算力精准调度为核心、高速数据传输为纽带，构建“算力驱动—网络支撑—安全保障”的一体化运行体系，实现算力资

源与数据流通的动态适配。

算力网的三级调度架构依赖高速数据网络提供底层支撑。云边端三级算力节点的实时感知数据，需通过高速数据网络的高带宽通道传输至云端调度中心，使云端能基于全域算力负载、能耗状态等动态指标制定分配策略。云端的算力调度平台，需依托高速数据网络的低延迟特性，确保边缘节点负载过高时，算力支援请求与资源调配指令能即时传递，保障协同计算的时效性。

高速数据网络的安全机制为算力交互筑牢屏障。其动态 NAT 技术与私网地址映射规则，将边缘节点、终端设备的真实 IP 隐藏，通过网关中转实现算力节点间的匿名通信，规避公网扫描风险。这与算力网中跨节点数据交互需求深度适配，既保障云端对边缘、终端算力的远程调度安全，又确保本地化数据处理时的隐私隔离。

两者通过协议与技术协同提升整体效能。算力网的云边协同协议与高速数据网络的弹性带宽特性形成互补，在算力密集型任务执行时，网络自动扩容带宽，满足 AI 推理、数据过滤等服务的高频数据传输需求；而高速数据网络的一键部署策略，简化了算力节点接入流程，使边缘集群能快速融入全局算力网络。这种“算力调度—数据传输—安全防护”的闭环协同，最终实现算力像水电般按需调配，为智能体应用提供全场景数算支撑。

五、典型应用场景与需求

5.1 智能制造可信协同

5.1.1 痛点需求

在当前全球工业发展的背景下，智能制造逐渐成为推动工业转型升级的重要动力。随着新一轮科技革命和产业变革的深入推进，智能制造不仅体现在机械设备的智能化、信息化，更在于整体产业链与供应链的深度融合和协同。但是，传统制造业在数据治理、数据共享和数据利用方面仍然面临诸多挑战，严重制约了智能制造的全面实施。

首先，数据安全性与商业机密保护挑战大。智能制造过程中，企业的生产工艺参数、设备运行数据、客户订单信息、供应链数据等均属于核心商业机密。这些数据在企业内部各部门流转以及与上下游合作伙伴交互时，存在被窃取、泄露的风险。同时，随着工业互联网的发展，大量设备接入网络，网络攻击手段愈发复杂，传统的安全防护措施难以抵御针对智能制造系统的高级别攻击，数据安全面临严峻挑战。

其次，产业链数据孤岛制约协同效率。智能制造产业链涵盖原材料供应商、零部件生产商、整机制造商、分销商、服务商等多个环节。各环节企业的数据系统独立运行，数据格式、标准不统一，导致数据难以实现跨企业、跨环节的流通与共享。产业链数据孤岛使得整个产业链的协同效率低下，无法快速响应市场需求变化。

再次，数据权属与利益分配机制不明。智能制造数据的产生涉及设备制造商、生产企业、操作人员、软件服务商等多个主体，数据的权属界定十分复杂。例如，智能生产设备在运行过程中产生的设备状态数据，是属于设备制造商、使用企业还是两者共有，目前缺乏明确的界定标准。数据权属不清导致在数据共享和应用过程中，各方的利益难以得到有效保障，容易引发纠纷。此外，数据应用产生的收益如何在各参与主体之间进行合理分配，也缺乏相应的机制，影响了企业参与数据共享的积极性。

最后，数据质量与一致性难以保证。智能制造数据来源广泛，包括生产设备、传感器、ERP 系统、MES 系统等，数据类型多样，有结构化数据、非结构化数据等。由于不同设备的精度、传感器的灵敏度存在差异，以及数据采集过程中的环境干扰等因素，导致数据质量参差不齐，存在数据不准确、不完整、不一致等问题。例如，在产品质量检测环节，不同检测设备对同一产品的检测数据可能存在偏差，影响对产品质量的准确判断。低质量的数据无法为智能制造的决策优化提供可靠依据，制约了智能制造水平的提升。

5.1.2 解决方案

为了提升制造业的竞争力，企业需要构建开放、共享、可信的数据空间，以支持各环节之间的信息交互和协同决策，提升生产效率、降低运营成本，进而提升整体竞争力。

可信数据空间强化了数据的安全性与隐私保护，保障企业核心利

益。可信数据空间采用加密技术、访问控制、安全审计等多种安全机制，构建全方位的数据安全防护体系。对智能制造中的敏感数据进行加密处理，确保数据在传输和存储过程中的安全性；通过严格的访问控制策略，限制未经授权的用户访问数据，防止数据泄露；利用安全审计技术，对数据的操作行为进行全程记录，以便及时发现和追溯安全事件。这些措施能够有效防范数据安全风险，保护企业的核心商业机密和数据资产，保障企业的核心利益。

可信数据空间能够有效打破数据孤岛，促进各参与方之间的数据共享与交互，提升产业链协同水平。可信数据空间建立统一的数据标准和接口规范，推动产业链各环节企业的数据互联互通。通过构建数据共享平台，实现原材料供应、生产制造、物流运输、销售服务等环节数据的实时共享与协同。例如，原材料供应商可以通过可信数据空间将原材料的供应信息实时共享给制造商，制造商根据这些信息及时调整生产计划；制造商也可以将产品的生产进度和库存信息共享给分销商，分销商据此优化库存管理和销售策略。产业链数据的高效流通，能够显著提升整个产业链的协同效率和快速响应能力。

可信数据空间有助于明确数据权属与利益分配，激发数据价值。可信数据空间通过建立完善的数据权属界定机制和利益分配规则，明确各主体在数据产生、使用、共享过程中的权利和义务。利用区块链等技术对数据的权属进行确认和记录，确保数据权属的清晰可追溯。同时，根据各主体在数据价值创造过程中的贡献，制定合理的利益分配方案，保障各主体的合法权益。这将有效解决数据权属纠纷问题，

提高企业参与数据共享和应用的积极性，充分激发数据的价值。

可信数据空间通过提升数据质量，赋能企业智能决策。可信数据空间构建数据治理体系，对智能制造数据进行清洗、校验、整合和标准化处理，提高数据的准确性、完整性和一致性。通过建立数据质量评估模型和监控机制，实时监测数据质量，及时发现和纠正数据问题。高质量的数据能够为智能制造的生产优化、质量控制、供应链管理等提供可靠的决策支持。例如，基于准确的生产设备运行数据，企业可以预测设备故障，提前进行维护保养，减少生产停机时间；利用高质量的市场需求数据，能够更精准地进行生产计划制定，提高生产效率。

总而言之，建设可信数据空间不仅是智能制造转型的重要保障，更是实现产业链与供应链高效协同的核心。可信数据空间提升了整个智能制造生态系统的透明度与韧性，各方不仅可以实时监督生产与供应链状态，还能更快速地做出调整与决策，从而有效减少风险，提高市场适应能力，进一步提升产业的整体竞争力。

5.2 能源电力数据互联

5.2.1 痛点需求

能源电力行业关系国计民生，正经历着向“绿色、低碳、安全、高质量”转型的关键时期，这就要求能源电力行业内部的各企业主体之间实现数据的广泛互联，横向快速汇聚能源生产、消费、市场等数据，纵向深度融合电源、电网、储能、用户等数据，赋能新型能源业务，

加快实现能源产业数字化转型与深层次变革。但能源电力领域涵盖众多行业主体，涉及数据类型多种多样，长期存在数据分散标准不统一、企业间数据壁垒明显、数据供需难匹配难等问题，严重阻碍了能源电力企业之间的数据连接。

数据分散性与标准不统一，数据难以“讲同一种语言”。能源电力行业环节多，涵盖发电、输电、配电、用电、调度、交易等全产业链；主体多，包括发电集团、电网公司、售电公司、用户、设备厂商等；数据类型杂，包括结构化数据（SCADA/EMS 实时数据、电表读数、设备台账、生产报表、交易结算数据）、半结构化数据（日志文件、XML/JSON 配置文件）、非结构化数据（设备图像/视频、巡检报告、设计图纸、合同文档、气象数据、卫星遥感数据）等；由于各环节数据语义不统一、接口规范不一致、数据质量参差不齐，直接导致“数据烟囱”林立，严重制约了数据价值的挖掘。

企业间数据壁垒坚固，协同效率低下。能源电力行业的市场化改革尚未完全到位，企业间的竞争关系与数据安全顾虑形成了坚固的数据壁垒，阻碍了跨主体协同。行业内部，发电企业的成本数据（如煤耗、运维费用）属于核心商业机密，不愿向电网公司完全开放；电网公司的实时负荷预测数据因涉及电网安全，也仅向发电企业开放有限维度；工业用户担心用电数据泄露会暴露生产规模、开工率等商业信息等。跨行业数据壁垒更显著。能源企业与气象部门的气象数据、与交通部门的物流数据、与环保部门的排放数据缺乏共享机制。这些壁垒导致能源生态协同受限。

数据供需匹配失衡，价值转化通道不畅。能源电力行业的数据供需存在“显性短缺”与“隐性过剩”并存的矛盾，供需两端的信息不对称导致数据资源浪费。数据需求方（如新能源场站需要气象数据做功率预测，售电公司需要用户负荷数据做套餐设计）有时难以精准描述所需数据的范围、格式、时效性等具体要求；数据提供方（如气象局、电网公司）的响应流程可能冗长，审批复杂，难以满足灵活、快速、按需的数据获取需求。

5.2.2 解决方案

可信数据空间以统一的技术平台为底座，基于统一的标准规范，实现数据供需撮合对接，为能源电力企业之间的数据互联提供了最优解决方案。



聚焦“能源流-数据流-价值流”的深度融合，建设包括可信数据空间底座、数据资源服务、接入连接器、运营管理平台等层的能源电力行业可信数据空间，各层设计中嵌入行业专属的技术特征与业务逻辑。可信数据空间的技术底座层整合区块链、隐私保护计算、数据沙箱、

使用控制技术等促进数据合规使用的技术产品；数据资源服务层包括分时分区电碳因子库、电工装备碳足迹背景库、电网负荷与调控数据集、电力供需预测数据集、电力企业征信数据集等经过可信认证和合规认证的电力行业高质量数据集和行业数据；运营管理平台通过提供参与方入驻、目录展示、数据定价和资产评估等功能，是能源电力行业可信数据空间生态建设的核心。

可信数据空间有助于解决能源电力数据跨主体融合中存在的标准各异的问题。一是可以基于统一的能源行业数据标准和技术规范，实现数据高效查询和按需获取，降低沟通和运营成本；二是可以实现其他企业数据与自有数据有效关联融合，为场景化应用建立基础；三是基于统一的标准规范，能够快速实现跨空间互联互通，享受多个数据空间带来的数据流通红利，快速融入更广泛的数据生态。

可信数据空间有助于打破企业间的数据壁垒，促进系统和数据互联互通。可信数据空间提供了一套“通用”的技术平台，一是利用多主体互联的确定性网络，快速实现能源电力企业主体的“入网”，缩短主体连接的响应周期；二是利用数据空间构建的确定性网络，可以快速建立数据交换通道，无需针对每一个数据需求开发接口；三是提供了语义转换等技术服务，为不同主体在数据合作意向范围内开展数据共享交换建立统一渠道，实现不同主体间数据的快速集成和高效交互。

可信数据空间有助于强化供需精准对接，大幅降低找数取数成本。能源电力企业基于可信数据空间，一是可以便捷查询空间内的能源数

据，准确识别和对齐供需双方需求，快速达成合作；二是能够以空间运营方为“桥梁”，撮合供需双方建立有效联系，助力合作关系的形成；三是可以在数据空间内自行发布个性化需求，由数据提供方主动响应需求，从而实现供需双方的高度精准匹配对接，确保能源数据需求“找得到、发得出、对得齐”。

5.3 公共数据可信交互

公共数据可信交互在多个领域展现出巨大的应用潜力。例如，在社会治理方面，不同部门如公安、交通、应急等需要共享数据以实现跨部门的协同治理。公共数据可信交互通过建立统一的数据共享平台，确保不同部门数据的无缝对接和整合，同时保障数据的安全性和隐私性，防止数据泄露和滥用。这种机制能够提高城市安全的实时监控和应急响应能力，为社会治理提供科学决策依据。

在公共服务领域，公共数据可信交互能够优化资源配置，提升服务质量。以医疗为例，医疗数据的可信共享可以促进远程医疗和分级诊疗，提高医疗服务的可及性。通过建立数据互操作性标准，不同医疗机构之间的数据可以实现互通共享，同时在共享过程中严格保护患者的个人隐私，确保数据的匿名化和脱敏处理。此外，强大的数据处理和分析能力能够支持复杂的医疗诊断和决策，为患者提供更精准的医疗服务。

在城市规划与管理中，多源数据的融合分析有助于实现城市资源的优化配置和精细化管理。城市规划部门可以利用地理信息数据、人

口数据、经济数据等进行综合分析，制定更加科学合理的城市发展规划。公共数据可信交互确保这些数据的动态更新和实时性，反映城市发展的最新状况。结合大数据和人工智能技术，它还能提供智能决策支持，提升城市规划和管理的科学性，助力打造智慧城市。

在环境监测与保护领域，公共数据可信交互对于实现环境保护和污染治理至关重要。环保部门、气象部门、水利部门等需要共享数据，以实现空气质量、水质、土壤等环境要素的实时监测和综合分析。通过建立实时监测系统，公共数据可信交互能够确保环境数据的准确性和可靠性，及时发现和预警环境问题，并支持科学的环境决策。同时，它还促进了不同部门之间的跨部门协同，实现数据共享和联合行动，共同应对环境挑战。

在公共资源配置方面，公共数据可信交互可以确保资源分配的公平性、透明性和效率。以公共资源交易平台为例，通过共享和分析公共资源交易数据，该机制能够优化资源配置，提高公共资源的利用效率。它保证了公共资源交易数据的透明性，接受社会监督，并利用大数据和人工智能技术实现资源与需求的智能匹配和推荐。此外，公共数据可信交互还建立了防欺诈机制，确保公共资源交易的公正性和合法性，从而提升公共资源的管理效能。

5.4 智慧城市智能体交互

5.4.1 痛点需求

在新型智慧城市建设中，交通、气象等领域的智能体交互是实现城市精细化治理的核心支撑。当前跨领域智能体协同仍面临多重挑战，制约了智慧城市整体效能的发挥。

跨域数据安全与隐私保护风险突出。智慧城市智能体交互涉及海量敏感数据，包括交通卡口的车辆轨迹、气象监测的地理信息、市民出行的个人行为数据等。这些数据在交通信号控制智能体、气象预警智能体、应急指挥智能体等跨领域流转时，存在数据泄露、滥用的风险。同时，各类智能体接入网络的接口安全防护不足，易遭受恶意攻击，威胁城市运行安全。

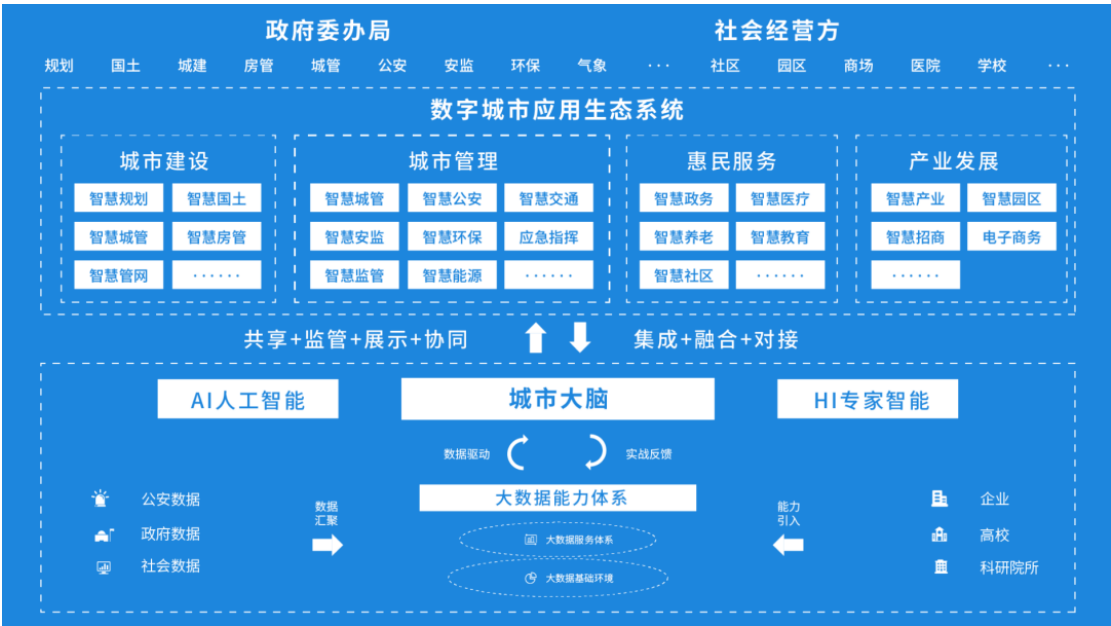
领域数据孤岛阻碍协同响应。交通、气象、城管、应急等部门的智能体系统独立建设，数据标准、接口协议、存储格式存在差异。例如，交通智能体的路况数据与气象智能体的降水预警数据格式不兼容，导致暴雨天气下无法快速联动调整交通信号配时；城管智能体的占道施工信息未能实时同步至导航智能体，造成市民出行规划偏差。数据孤岛使得城市级突发事件难以实现多智能体协同处置。

数据权属模糊与利益分配失衡。智慧城市数据产生主体多元，交通数据可能来自交管部门、网约车企业、车载终端等，气象数据涉及气象局、科研机构、监测设备厂商等。数据权属界定缺乏统一标准，例如交通流量数据的所有权归属采集部门还是城市管理主体，气象预

测数据的收益如何在数据提供方与应用方之间分配，这些问题导致各主体对数据共享持谨慎态度，影响智能体交互的深度。

数据质量参差影响决策精度。智能体交互依赖高质量数据支撑，但其数据来源广泛且采集条件复杂。交通摄像头因光线、遮挡导致数据失真，气象传感器因维护不当出现监测偏差，不同部门数据更新频率不一致造成时间维度错位。例如，交通智能体基于滞后的车流量数据调整信号时长，可能加剧拥堵；气象智能体使用低精度降水数据触发预警，易引发市民恐慌或应急资源浪费。

5.4.2 解决方案



构建智慧城市可信数据空间，是破解跨领域智能体交互难题、实现交通与气象等应用协同增效的关键路径，能够为城市治理提供安全、高效、可信的支撑体系。

可信数据空间筑牢跨域数据安全防线，保障智能体交互隐私。通

过部署数据加密、访问控制、安全沙箱等技术，对交通轨迹、气象敏感数据等进行全生命周期安全防护。建立基于角色的权限管理机制，严格限制智能体数据访问范围，例如气象智能体仅能获取交通智能体的匿名路况数据，无法追溯具体车辆信息。利用安全审计系统对智能体数据交互行为全程记录，实现异常操作实时预警与追溯，确保数据使用合规可控。

可信数据空间打破领域壁垒，提升智能体协同响应效率。统一交通、气象等领域的数据标准与接口规范，构建跨部门数据共享平台。通过标准化处理，实现交通流量、降水强度、道路施工等数据的互联互通，支持智能体实时调取所需信息。例如，暴雨天气时，气象智能体可通过可信数据空间将预警信息推送至交通智能体，触发信号灯动态调整、积水路段限行等联动策略；应急指挥智能体能够同步调用交通疏散路径数据与气象灾害扩散模型，制定科学救援方案。

可信数据空间明确权属与利益分配，激发协同动力。建立数据权属登记机制，利用区块链技术记录交通、气象等数据的产生主体、采集过程与使用权限，实现权属可追溯。制定差异化利益分配规则，根据数据贡献度确定收益分成比例，例如网约车企业提供的实时路况数据可按使用频次获得收益，气象部门的预测数据在商业导航应用中产生的价值可按约定比例返还。清晰的权责与利益机制，提升各主体参与智能体数据共享的积极性。

可信数据空间提升数据质量，强化智能体决策精度。构建全流程数据治理体系，对交通、气象等数据进行清洗、校验、融合与标准化

处理。建立数据质量评估模型，实时监测数据完整性、准确性、时效性，对异常数据自动标记并触发补采机制。例如，通过算法修正交通摄像头的遮挡数据，校准气象传感器的漂移误差，统一各部门数据更新频率。高质量数据支撑下，交通智能体可精准预测车流高峰，气象智能体可提高灾害预警精度，实现多智能体协同决策的科学性与有效性。

可信数据空间为智慧城市智能体交互提供了安全可信的“数据底座”，通过打通交通与气象等领域的协同壁垒，提升了城市治理的精细化水平与应急响应能力，推动智慧城市从“各自为战”向“协同共治”转型升级。

5.5 车联网可信生态

5.5.1 痛点需求

随着汽车产业进入以智能网联汽车为标志的下半场竞争，数据的价值愈发凸显。车辆通过车载感知设备和电气化，能产生包括自车状态数据、环境感知数据、事件类数据等大量数据，同时，随着车路云一体化的建设进程，路侧的智能化改造使得路侧能收集如信号灯态、道路事件、车辆轨迹、道路目标物等数据，海量的数据蕴含有大量价值亟待开发。然而，智能网联汽车在数据的收集、管理、分析和应用方面也面临着新的挑战。

首先，数据安全和隐私保护风险突出。车联网场景下，车辆传感

器、定位系统、车载终端等会产生海量数据，其中包含大量敏感信息，如车主身份信息、车辆实时位置、行驶轨迹、驾驶习惯等。这些数据一旦泄露或被恶意利用，可能导致严重后果。

其次，数据孤岛现象阻碍协同发展。车联网生态涉及车企、零部件供应商、交通管理部门、云服务提供商、保险公司等众多参与者，各主体出于商业利益、数据安全等因素考虑，往往将数据视为核心资产进行封闭管理，形成“数据孤岛”，数据孤岛使得车联网各环节无法实现高效协同，限制了车联网服务的创新和行业整体发展。

再次，数据质量与可信度不足。车联网数据来源广泛，包括不同品牌、型号的车辆，不同类型的传感器和设备，数据质量参差不齐。部分数据存在噪声、误差、缺失等问题，影响数据的可用性。同时，由于缺乏有效的数据校验和溯源机制，难以判断数据的真实性和可信度。低质量、不可信的数据无法为车联网应用提供有效支撑，阻碍了车联网技术的迭代升级。

最后，网络传输不确定性影响业务可靠性。车联网业务对网络传输的实时性、确定性要求极高。自动驾驶、车路协同等应用需要车辆与路侧设备、云端平台进行实时数据交互，毫秒级的延迟或数据丢失都可能引发安全事故。然而，现有网络存在带宽波动、传输延迟、丢包等不确定性问题，在车辆高速移动、复杂路况等场景下更为明显。网络传输的不确定性严重制约了车联网高级别应用的落地和普及。

5.5.2 解决方案

通过构建一个基于确定性网络的高效的汽车行业可信数据空间，推动各企业、机构和消费者之间的数据互联，促进汽车行业从传统模式向智能化、高效化的转型，助力打造一个更加安全、可靠、互联的未来智能网联生态系统。



保障数据安全与隐私，增强行业信任。可信数据空间通过采用加密技术、隐私计算、区块链等技术，构建多层次的数据安全防护体系。对敏感数据进行加密处理，确保数据在传输、存储和使用过程中的安全性；利用隐私计算技术实现“数据可用不可见”，在数据共享分析时保护原始数据不泄露；借助区块链的不可篡改特性，对数据流转全过程进行记录，实现数据溯源。这些措施有效降低了数据安全风险，保护了用户隐私，增强了消费者、行业参与者对车联网的信任，为行业健康发展奠定基础。

打破数据孤岛，促进协同创新。可信数据空间建立统一的数据标

准和接口规范，推动各主体数据的互联互通。通过制定数据共享规则和权限管理机制，明确数据共享的范围、方式和责任，促进车企、交通管理部门、服务提供商等主体之间的数据流通。例如，车企与交通管理部门共享车辆行驶数据和路况信息，可共同优化智能交通系统；保险公司基于车辆驾驶行为数据制定个性化保险方案，实现精准定价。数据的高效共享打破了行业壁垒，促进了跨领域协同创新，催生了更多车联网新业态、新模式。

提高数据质量，赋能行业升级。可信数据空间通过建立数据治理体系，对数据进行清洗、校验、标注等处理，提高数据质量。利用数据溯源技术，确保数据的真实性和可追溯性，为数据使用者提供可靠的数据来源。高质量的数据为车联网技术创新提供了有力支撑，例如，基于精准的车辆运行数据，车企可以优化车辆设计和制造工艺；利用海量的路况数据，交通管理部门可以制定更科学的交通规划方案。数据质量的提升推动了车联网行业向智能化、精细化方向发展，加速了行业的升级迭代。

确定性网络提升网络传输确定性，保障业务可靠运行。可信数据空间依托确定性网络技术，如时间敏感网络（TSN）、网络切片等，为车联网业务提供稳定、可靠的网络传输环境。通过为不同业务类型分配专属的网络资源，保障关键业务的实时性和低延迟。例如，为自动驾驶业务分配高优先级网络切片，确保车辆与路侧设备、云端的实时数据交互不受其他业务干扰。网络传输确定性的提升，为自动驾驶、车路协同等高级别应用的落地提供了关键支撑，提高了车联网业务的

可靠性和安全性。

5.6 元宇宙在线教育

5.6.1 痛点需求

在元宇宙沉浸式在线教育蓬勃发展的进程中，技术创新与教育模式变革深度融合，催生了全新的学习体验。在元宇宙教育环境中，数据不仅是教学过程的记录载体，更是驱动个性化学习、虚拟实验、教育资产化的核心生产要素，然而当前其流通利用面临多重瓶颈：

首先，数据安全与隐私保护风险加剧。元宇宙教育涉及用户身份信息、学习行为数据、虚拟环境中的交互数据（如手势、表情识别信息）等敏感内容，这些数据若未妥善保护，可能被用于行为分析或商业滥用。传统安全防护手段难以应对元宇宙中多源异构数据的动态流转需求，亟须构建多层次的安全防护体系。

其次，跨平台数据孤岛与互操作性壁垒。各元宇宙教育平台采用独立的数据标准与接口规范，导致教学资源、用户数据无法跨域共享，形成封闭的数据壁垒。例如，某高校开发的虚拟实验室数据无法与企业培训平台兼容，造成资源重复建设。数据孤岛不仅阻碍教育资源的优化配置，还限制了跨机构协作与个性化学习服务的拓展。

再次，数据权属与知识产权保护机制缺失。元宇宙教育中，教学课件、虚拟场景、数字孪生模型等内容的版权归属复杂。例如，教师创作的虚拟教案与平台提供的基础框架之间的权属划分缺乏明确规

则。虚拟资产（如数字徽章、虚拟道具）的所有权确认与交易溯源问题突出，制约了元宇宙教育生态的价值循环。

最后，网络传输不确定性影响沉浸体验。元宇宙教育对实时性与稳定性要求极高，如多人协作实验、虚拟课堂互动等场景需确保毫秒级响应。然而，现有网络环境下，带宽波动、延迟抖动等问题频发，导致虚拟场景卡顿、交互中断。例如，在 VR 远程实训中，网络延迟可能使学生操作与反馈不同步，影响实训效果。网络传输的不确定性已成为制约元宇宙教育规模化应用的关键瓶颈。

5.6.2 解决方案

可信数据空间作为新型数据基础设施，通过“技术+规则”双轮驱动，以隐私计算筑底安全、区块链贯通孤岛、智能合约激活资产，彻底重构数据流通的信任基座，构建起安全可控的数据流通生态。

构建全生命周期数据安全防护体系。可信数据空间通过加密技术（如国密算法 SM 系列）对传输与存储的数据进行高强度加密，确保用户隐私信息在交互过程中不可窃取。结合区块链技术，实现数据操作全程可追溯，任何对教学内容、用户行为的篡改均能被精准定位。通过隐私计算技术（如联邦学习）支持跨机构数据联合分析，在不泄露原始数据的前提下优化教学模型，实现“数据可用不可见”。

破解数据孤岛与跨平台互操作性难题。可信数据空间通过制定统一数据标准，整合多源异构数据，实现教学资源、用户画像、虚拟资产的跨平台流通。例如，某高校与企业合作开发的虚拟实训平台，通

过标准化接口实现设备运行数据与教学管理系统的无缝对接，提升实训效率 30%以上。同时，智能合约技术自动执行数据共享规则，确保数据使用权限与收益分配透明化，激发各方参与数据协作的积极性。

强化知识产权保护与价值流通。可信数据空间为元宇宙教育内容提供数字版权确权服务，通过 NFT(非同质化通证)技术为虚拟教案、数字模型等赋予唯一标识，明确创作者权益。此外，区块链的不可篡改特性为版权纠纷提供司法取证支持，降低维权成本。

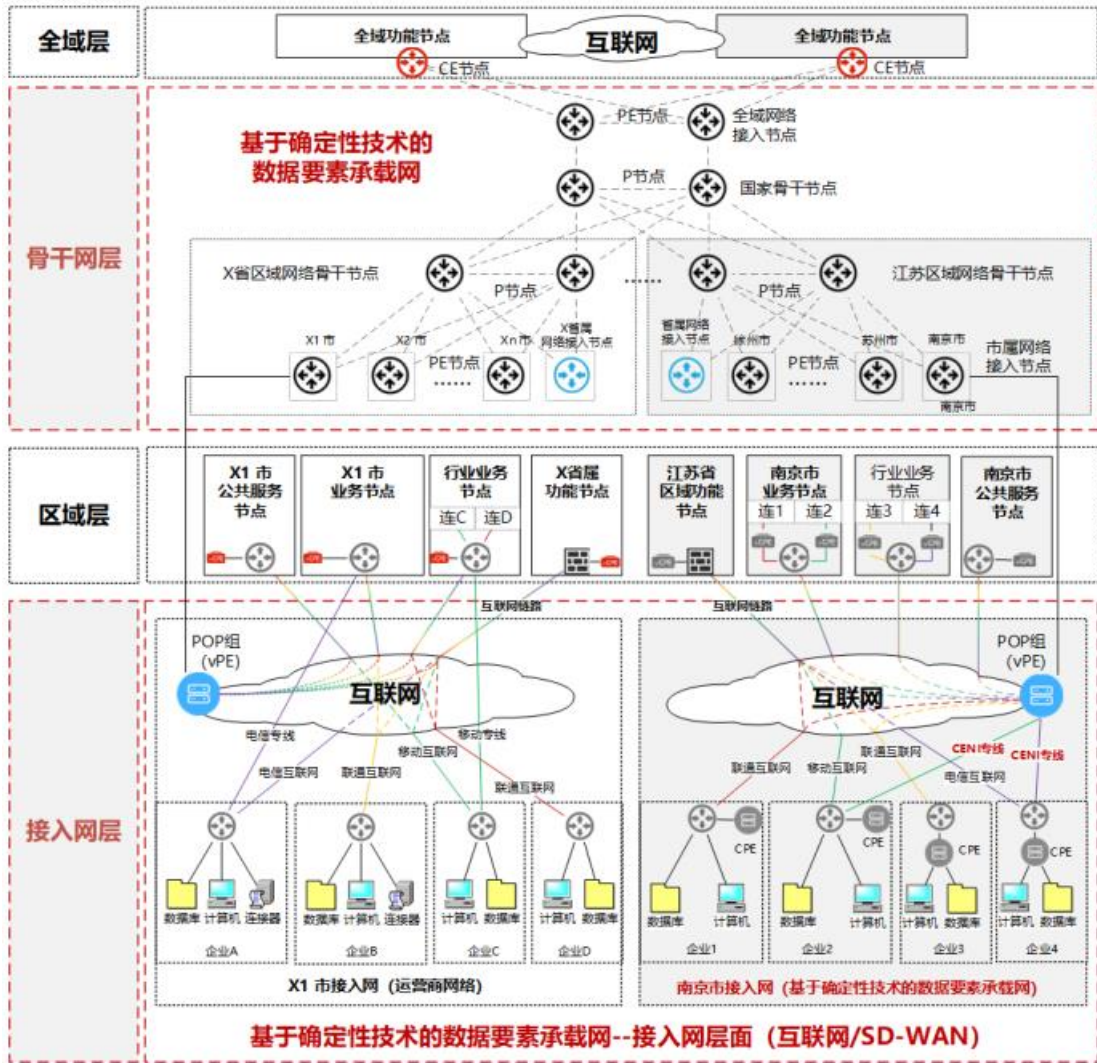
确定性网络传输保障教学沉浸体验。结合光电融合广域确定性网络技术、时间敏感网络（TSN）、网络切片等新兴网络技术，可信数据空间为元宇宙教育分配专属网络资源，确保实时交互场景（如虚拟课堂直播、多人协同编程）的端到端时延低于 20ms，网络可靠性达到 99.99%以上。例如，某 VR 语言学习平台通过网络切片技术隔离娱乐流量与教学数据，使语音交互延迟降低 60%，显著提升口语训练效果。

六、关键技术实现路径

6.1 确定性网络部署

基于“三大运营商资源和 CENI 确定性网络技术”构建数据要素承载网，具备高速传输、低延迟、高可靠性及安全性等特性。优化数据流通体系，提升数据传输效率与安全特性，确保“三统一”信息同

步，支持业务灵活流量调度，满足用户多样化接入和高性价比需求。



1、骨干网：全域功能节点与区域业务/功能节点通过互联网/专线结合 SD-WAN 技术，接入数据要素承载网，实现平台节点间的高速、安全数据传输及“三统一”信息同步的增强服务，保障业务互联互通。

2、接入网：基于运营商互联网基础能力与 SD-WAN 技术，打造“互联网+虚拟接入专网”服务方案，为接入主体提供灵活多样的数据传输方式。接入主体依据数据安全传输需求，通过区域业务节点平台选择“虚拟接入专网服务”并完成服务注册，即可快速实现安全、高效的数据交易组网与传输。

基于“三大运营商资源和 CENI 确定性网络技术”构建数据要素承载网，具备高速传输、低延迟、高可靠性及安全性等特性。优化数据流通体系，提升数据传输效率与安全特性，确保“三统一”信息同步，支持业务灵活流量调度，满足用户多样化接入和高性价比需求。

1、高效网络加速：专用网络与高效路径优化，实现网络传输加速，提升数据传输效率。

2、数据加密传输：专网隔离与端到端加密，解决“公网”数据暴露风险，保障数据传输安全。

3、智能故障定位：采用分层网络设计与智能监控诊断工具，快速定位并修复故障，降低对全局影响，提升网络可靠性与稳定性。

4、使用成本效益：通过优化网络资源配置提供高效数据传输，降低使用成本，使接入主体在享受高性能与高可靠性服务的同时，实现更高性价比。

6.2 算力协同部署

算力协同部署在南京市数据基础设施项目中，致力于整合城市内分散的算力资源，实现算力与数据的高效协同，提升城市整体的算力服务能力。

算力资源整合：整合各类算力资源，涵盖高校科研计算资源、企业数据处理算力以及政府部门的政务数据统计分析算力等。通过数据基础设施的算力网络，将这些分散在不同机构、不同领域的算力资源进行统一管理调度。例如，在某大型科研项目中，高校的科研计算

集群算力不足时，可通过数据基础设施的算力协同机制，调用企业闲置的云计算资源，实现算力资源的跨机构共享，避免了资源的浪费，提高了整个城市算力资源的利用率。同时，对不同类型的算力，如通用计算、智能计算、超级计算等进行分类整合，根据不同业务场景的需求，灵活调配相应的算力资源，提升算力服务的针对性与有效性。

算力网络构建：构建专门的算力网络，连接城市中的算力中心与数据基础设施、连接器。基于光电融合技术，通过“IP+光”的融合路径，打造出低时延、低抖动、高通量、高可靠的网络链路。基于 IPv6 的扩展协议为每一个接入算力网的设备分配独立的 IP 地址，确保数据传输的准确性与高效性。结合软件定义网络（SDN）技术，对网络流量进行灵活调控，根据不同业务对算力和网络的需求优先级，合理分配网络带宽资源，保障关键业务数据的传输质量，为算力与数据的交互提供稳定、高速的网络通道，实现数据快速传输至算力中心处理，以及处理结果及时反馈回数据基础设施和连接器。

协同机制建立：建立完善的算力协同机制，包括算力调度机制、资源分配机制以及收益分配机制等。在算力调度方面，引入算力感知的路由算法，能够根据各算力中心的负载情况和网络状态，智能地选择最优路径传输数据和调度算力，提高算力资源的利用效率。资源分配机制根据业务的实时需求，动态分配算力资源，确保紧急、重要的业务优先获得足够的算力支持。收益分配机制则鼓励各参与方积极贡献算力资源，通过合理的利益分配，调动高校、企业等机构参与算力协同的积极性，保障算力协同部署的持续推进与高效运行，推动南京

市数据基础设施项目在算力支撑下实现数据的深度挖掘与价值创造。

6.3 数据空间可信引擎

数据空间可信引擎作为智能体可信数据空间的核心技术支撑，其构建需要综合运用多种技术手段以实现数据的安全、可信与高效流通。首先，在可信计算与认证方面，通过建立可信根，利用可信执行环境（TEE）等技术，确保智能体身份的真实性和可靠性，为数据空间打造坚实的信任基础。同时，采用智能体身份认证与授权机制，精准控制智能体对数据的访问权限，防止未授权访问和数据泄漏风险。其次，数据加密与隐私保护至关重要。运用先进的加密算法对数据进行加密处理，确保数据在存储和传输过程中的机密性。结合密钥管理与分发技术，使授权智能体能够安全地解密和使用数据。此外，引入差分隐私与同态加密等前沿技术，在保护数据隐私的前提下，实现数据的可用性，满足不同场景下的数据共享需求。再者，智能合约与规则引擎的应用为数据空间的可信协作提供了有力支持。基于区块链的智能合约技术可以自动执行预设的规则和条件，实现数据共享、交易等操作的自动化和可信化。同时，规则引擎能够根据预先定义的策略和规则，对数据的访问、使用等行为进行实时监控和管理，确保数据的合规使用。最后，数据存证与溯源功能为数据空间提供了完整的数据生命周期管理。通过区块链等技术对数据进行存证，确保数据的不可篡改和可追溯性。当出现数据争议或需要审计时，可以利用溯源追踪机制，快速定位数据的来源和流向，为数据的安全和可信提供有力保障。

6.4 智能体协同协议

智能体协同协议是实现智能体之间高效、可信协作的关键技术。在数据交互层面，协议需要统一智能体之间的数据格式与语义，确保数据能够被准确理解和解析。通过制定标准化的数据表示形式，以及对数据语义进行清晰的定义和规范化，减少因数据不一致导致的误解和错误。同时，数据传输协议的设计要充分考虑基于确定性网络的特点，对数据包的时序进行严格控制，保障数据的可靠传输。采用诸如确定性网络（DetIP）等技术，确保数据在传输过程中的时延、抖动等关键指标满足业务要求，为智能体之间的实时交互提供稳定的数据传输通道。在智能体协作方面，不同的协作模式与流程需要被明确地定义和规范。智能体之间的协作任务需要进行合理的分解与分配，以充分发挥各个智能体的优势和能力。通过编排和管理协作流程，确保智能体之间的协作任务能够有序、高效地执行。任务调度与资源分配是智能体协同的关键环节。根据业务需求的动态变化，采用智能的任务调度策略，将任务合理分配给合适的智能体。同时，对算力资源和网络资源进行动态分配和优化配置，确保智能体在执行任务时能够获得足够的资源支持，提高整体协同效率。在安全与可信方面，智能体之间的身份认证与授权是保障协同安全的基础。采用基于属性的访问控制等机制，对智能体的访问权限进行细粒度的管理，确保只有经过授权的智能体能够参与协作。数据与通信安全是智能体协同的重要保障。通过加密与解密机制对数据进行保护，防止数据在传输过程中被窃取。

或篡改。同时，加强通信过程的安全防护，采用安全审计与监控手段，及时发现和处理潜在的安全威胁，确保智能体协同过程的安全可靠。最后，在互操作性与扩展性方面，智能体协同协议需要考虑不同智能体之间的互操作性。制定统一的标准和接口适配机制，实现异构系统之间的无缝对接和数据的双向映射，确保智能体能够在不同的系统环境中协同工作。此外，协议的扩展性设计至关重要。随着技术的发展和业务需求的变化，协议需要能够平滑地引入新的功能和特性，同时保持向后兼容性，确保智能体协同系统能够持续演进和发展。

智能体协同协议规范智能体之间的通信、交互和协同工作流程。在通信层面，定义智能体之间的数据传输格式、编码规则和通信协议栈，确保智能体之间能够准确无误地收发数据。例如，采用轻量级的消息队列遥测传输（MQTT）协议实现智能体之间的高效消息传递，在物联网场景下，传感器智能体通过 MQTT 协议将采集到的数据发送给数据处理智能体。

在交互层面，设计智能体之间的交互模型和接口，包括请求—响应模型、发布—订阅模型等。在协同工作流程方面，明确智能体之间协同完成任务的步骤和规则。以智能物流系统为例，仓储智能体、运输智能体和配送智能体依据协同协议，首先由仓储智能体根据库存信息规划货物出库顺序并向运输智能体发送货物交接请求；运输智能体按照约定的交接时间和地点接收货物，并实时向配送智能体反馈运输状态；配送智能体依据运输智能体提供的信息规划最优配送路线，完成货物配送任务。

七、产业实践案例

7.1 “江宁政企通 2.0”

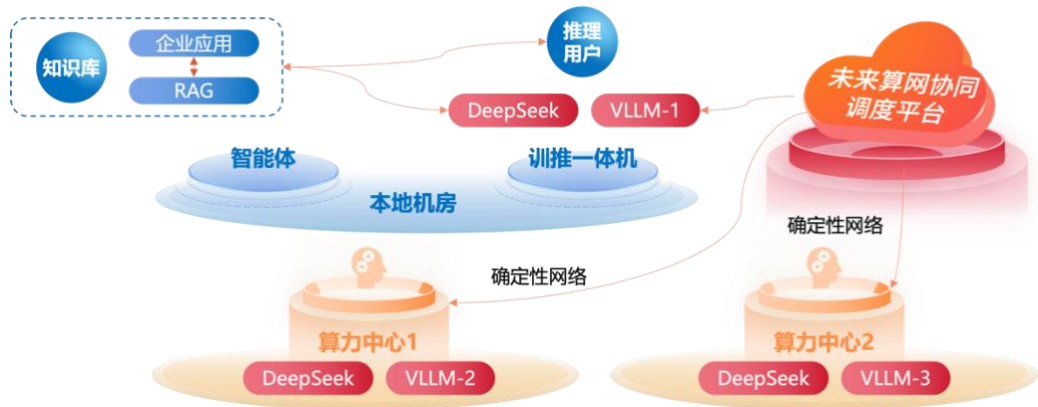
在数字化转型的浪潮中，AI 技术的快速迭代，使得中小企业面临诸多困境，严重制约其发展。

算力资源获取成本高：中小企业普遍面临算力资源匮乏且成本高昂的难题。一方面，受限于资金和技术实力，企业难以独立构建大规模算力设施，导致在处理大模型训练等复杂任务时，算力严重不足，业务推进缓慢。另一方面，传统的算力租赁模式价格高昂，按使用量计费的方式使得中小企业在业务高峰时算力成本剧增。

AI 应用技术门槛高：市场上通用大模型难以满足企业个性化需求，而定制开发大模型成本高、周期长，超出中小企业承受范围。同时，大模型的部署和维护需要专业技术团队，中小企业技术人才短缺，难以有效管理和优化模型，无法充分发挥大模型的效能。如何利用自身数据与基础大模型匹配，形成本地知识库，是中小企业面临的技术难题。

江宁政企通 2.0 打造算网智一体化数据基础设施，旨在助力中小企业突破数字化转型困境，针对算力资源获取成本高的问题，通过确定性网络整合市一省/区域一国家多级算力资源，借助算网协同调度平台，实现算力灵活调用，让中小企业能按需获取算力，降低获取成本与使用门槛，满足复杂任务的算力需求，加快业务推进速度。在应

对 AI 应用技术门槛高的挑战上，帮助企业进行基础大模型选型与适配，并与企业自身数据深度融合，形成本地知识库，为企业提供一站式 AI 智能体服务。

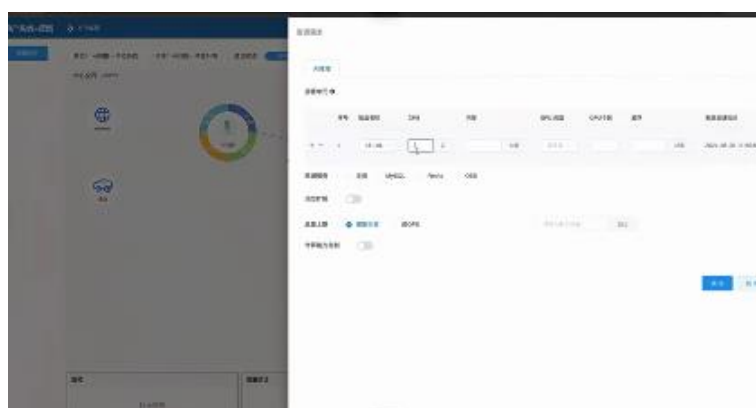


整体架构如图，打造未来算网协同调度平台，通过确定性网络连接本地一体机资源和云端算力资源，各节点适配不同版本 DeepSeek R1 模型，形成云边一体化的算网智数据基础设施。通过底层算网资源整合与协同运作，企业应用并发量小时使用本地资源，并发量大时跳转云端算力。同时，通过整合企业的历史数据，构建本地 RAG 知识库，形成企业特色的 AI 智能体应用。



通过未来网络基础设施及其多元异构算力直连网构建 1ms 时延的城市算力网、5ms 时延区域一体化网络、20ms 时延的国家“东数西算”新总线。该网络连接企业本地算力与市一区域一国家级算力，为

算力整合和调度奠定技术基础。

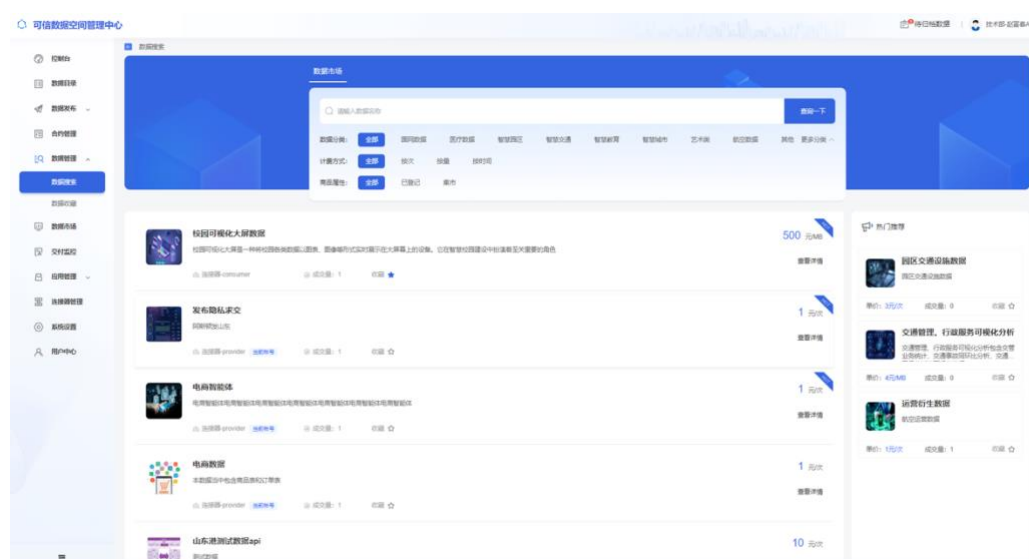


通过确定性网络接入的算力资源，企业可在平台上查看不同算力中心的实时报价，点击算力购买可跳转到算网智一体化调度平台，根据企业自身通算、智算、超算的不同需求，进行详细定制。定制完毕后，该平台通过编策略自动排序算网资源，企业用户点击即可实现资源实时开通，降低算力资源部署难度。



企业本地部署 DeepSeek 70B 版本大模型，满足日常应用需求，快速响应本地数据处理需求，云端部署 DeepSeek 671B 满血版，可实现复杂业务运算。

同时，支持使用企业的历史数据打造本地 RAG 知识库，通过 TXT、PDF、DOCX 等多种格式原始文档导入识别，使用噪声清洗等技术剔除干扰信息，提供自动分块以及按分段标识分块技术，提高知识检索与应用的针对性，对分块文档进行向量化处理，打破传统基于关键词匹配的局限，实现基于语义的深度理解与检索。



预留可信数据空间连接器，采用“数据不出域、可用不可见、可控可计量”的应用模式。方便企业快速接入行业可信数据空间获取数据资源，训练自身业务大模型，或发布流通自身脱敏数据，实现数据价值产业链打造。

7.2 菲尼克斯云化 PLC 智能体

在工业自动化领域，传统 PLC（可编程逻辑控制器）虽然在控制逻辑、稳定性和可靠性方面有着显著优势，但随着智能制造和工业 4.0 的发展，其系统封闭、扩展性差、灵活性不足、维护成本高等局限性和问题也逐渐显现，这些问题促使工业企业寻求更高效、灵活和智能

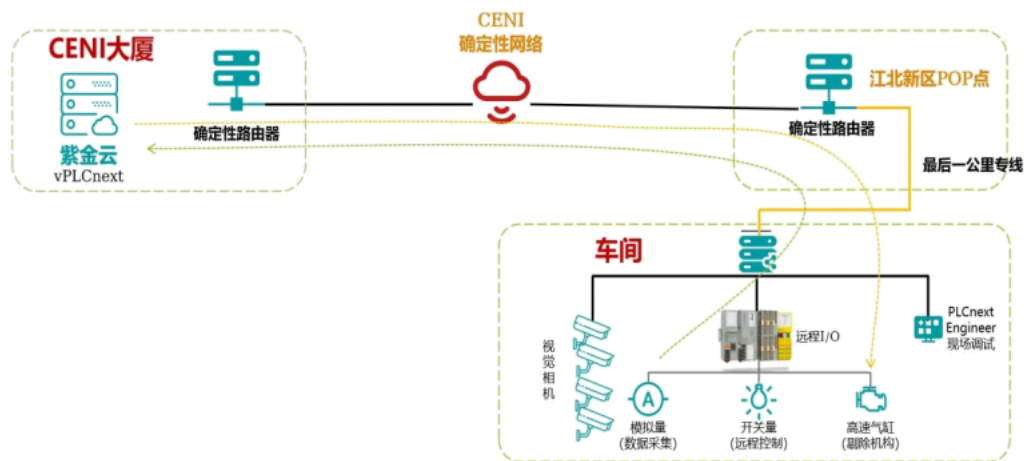
的解决方案。云化 PLC 作为工业控制系统的新兴形态，以其开放性、灵活性和智能化的特点，引领着智能制造的新潮流。云化 PLC 是将传统 PLC 的处理控制功能虚拟化后部署到云端，本地保留分布式控制单元和 I/O 端子，通过软硬解耦的方式增强 PLC 的兼容性与适配性，为工业自动化带来前所未有的灵活性和效率。

在制造业领域，云化 PLC 的应用场景非常广泛。首先，云化 PLC 可以实现生产线的实时监控与远程管理。通过传感器采集到的数据云化 PLC 可以实时监测设备的运行状态、产品的质量指标等，并将这些数据上传到云端，供管理人员随时查看和分析。同时，云化 PLC 还可以通过云端下发指令，实现对设备的远程控制和调节，提高了生产线的灵活性和可控性。

确定性网络是云化 PLC 的“神经中枢”，满足工业控制对通信的实时性、可靠性和同步性的极致要求。传统网络的“尽力而为”传输无法满足毫秒级甚至微秒级时延需求，也难以控制抖动，会导致指令与设备动作不同步。确定性网络通过时间同步、流量调度和资源预留机制，确保控制数据在固定窗口传输；借助冗余机制、网络切片和双链路热备提升可靠性，避免中断或数据丢失；通过微秒级时间同步支持多设备协同作业。确定性网络为云化 PLC 构建了一条媲美本地总线的虚拟控制通道，不仅满足工业控制对网络性能的严苛要求，还推动工业自动化向柔性化、智能化演进，为智能制造提供底层支撑。

菲尼克斯作为国内领先的 PLC 自动化厂商，与未来网络联合打造了基于确定性网络的云化 PLC 智能体解决方案，通过融合确定性网

络通信、PLC 虚拟化控制逻辑以及自主决策能力，构建“实时感知—智能决策—精准执行”的闭环，实现复杂场景下的高效协同与动态优化。该方案在某电子元器件产线部署落地。



在车间产线上，部署工业质检相机，通过 AI 机器视觉质检实现电阻外观缺陷检测（如并环、端环、气泡等），并将检测结果数据通过确定性网络传输至云化 PLC 智能体，用于触发控制产线侧的高速气缸，实现不良品的自动剔除，形成“感知（视觉）—决策（智能体）—执行（PLC）”的闭环融合，确定性网络则是确保这一融合高效运转的“神经中枢”，最终实现工业系统从“被动控制”向“主动优化”的智能化升级。同时，云化 PLC 智能体可整合 AI 机器视觉的历史数据与实时检测结果，优化控制策略，实现“自适应质检+预测性控制”。另外，中心 AI 训练平台通过调用标注过的异常/错误样本数据对模型进行再训练和评估，以提高模型的准确性和泛化能力。然后将新模型通过确定性网络快速推送部署回边缘设备，更新推理模型，使得模型学习到的最新知识能够立刻应用于生产，实现 AI 模型“边用边学、常用常新”。

云化 PLC 作为智能制造的关键技术之一，其发展不仅关乎企业的技术进步，更关系到国家工业的长远发展。确定性网络赋能的云化 PLC 智能体，正推动制造业向“集中控制、无线柔性、AI 驱动”范式演进。其价值不仅体现为成本与安全的优化，更深层的是打破 OT 层封闭性，为工业互联网提供“一网到底、算控一体”的数字基座。未来，云化 PLC 智能体将朝着更加智能化、集成化、绿色化的方向发展，为制造业的高质量发展提供坚实的技术支撑。

7.3 杭州市“城市大脑”公共数据智能体应用项目

杭州市“城市大脑”项目是公共数据智能体应用的典型案例。该项目构建了智能体可信数据空间，整合多领域公共数据，创建各类智能体实现城市精细化管理。

案例背景：杭州市“城市大脑”项目旨在通过公共数据的开发利用，提升城市管理效率和市民生活质量。项目整合了交通、医疗、环保、城管等领域的公共数据，构建了一个智能体可信数据空间。

智能体应用：数据治理智能体负责对各部门上报的原始公共数据进行清洗、分类和标注。例如，对交通摄像头采集的车辆通行数据去除重复记录，纠正车牌识别错误信息，将处理后的结构化数据存储于数据层。交通优化智能体实时获取道路车流、公交地铁运行等数据，运用机器学习算法预测交通流量变化，自动优化信号灯时长配置，提高车辆通行效率。医疗协同智能体对接医院挂号、就诊、检查检验等信息系统，实现医疗资源智能调度，缩短患者候诊时间。

技术亮点：杭州市“城市大脑”项目采用可信认证，所有智能体均基于数字身份证书进行身份认证，确保通信双方身份合法性。利用区块链技术对数据和智能体进行确权，实现数据权属标识和溯源追踪，确保智能体的合法性和可控性。根据智能体任务需求，在云端和边缘端合理分配算力资源，实现智能体的高效运行。

应用效果与价值：杭州市“城市大脑”项目打破了部门间数据壁垒，公共数据在智能体可信数据空间中得以安全流通和深度利用。数据价值充分释放，为城市数字经济创新发展提供了有力支撑。为城市公共数据开发利用打造了可信、可控、协同的环境，吸引了更多企业、科研机构等参与城市数据应用创新，形成了良性发展的数据生态。

八、发展建议与展望

8.1 产业生态构建

基于确定性网络的智能体可信数据空间的产业生态构建，将围绕“技术协同深化、场景价值释放、生态壁垒打破”三大主线，推动芯片、算力、网络、可信空间、密态计算等核心环节形成深度耦合的创新体系，为智能体跨域协同与数据要素流通提供全栈支撑。

在芯片层面，专用化与异构化成为核心发展方向。面向确定性网络的低时延需求，将涌现融合时间敏感网络（TSN）协议加速引擎的边缘芯片，实现微秒级时钟同步与任务调度；针对可信数据空间的安

全需求，集成硬件级加解密模块、安全启动与远程证明功能的安全芯片将成为标配，支撑数据全生命周期的可信根基。同时，芯片设计将深度适配智能体场景，形成“云端高性能通用芯片+边缘轻量异构芯片+终端低功耗专用芯片”的三级架构，通过统一指令集与接口标准，实现算力资源的无缝调度。

算力生态将向“智能调度+绿色集约”的模式升级。云边端三级算力网络与确定性网络的融合不断深化，基于 AI 的动态调度算法将实现算力需求与网络带宽的实时匹配，确保智能体高优先级任务的算力响应延迟控制在毫秒级以内。分布式算力集群将通过可信数据空间实现跨域协同，依托粒子群优化、联邦学习等技术，在保障数据隐私的前提下完成全局算力最优分配。同时，算力网络将融入绿色节能设计，通过智能功耗调节与资源虚拟化技术，提升单位能耗的算力产出，支撑“双碳”目标下的产业可持续发展。

网络技术将迈向“确定性增强+安全内生”的新阶段。确定性网络将实现从“时延可控”到“全链路可预期”的突破，通过 6G 空口技术与光传送网的深度融合，构建端到端时延抖动小于 10 微秒的确定性通道；网络切片技术将与可信数据空间联动，为不同智能体场景定制“带宽—时延—安全”专属网络切片，例如工业智能体的高可靠切片、交通智能体的低时延切片。此外，网络安全将从“外挂防护”转向“内生免疫”，通过动态 NAT、零信任架构与可信计算技术的集成，实现网络节点身份可信、数据传输加密、行为操作可追溯的全程防护。

可信空间将走向“标准化+开源化+跨域化”。行业级可信数据空

间标准体系将逐步完善，涵盖数据接口、安全协议、权属界定等关键环节，推动金融、制造、城市等领域的可信空间互联互通。开源社区将成为生态创新核心载体，提供标准化的可信空间中间件与开发工具，降低企业部署门槛。跨域可信联盟将广泛形成，通过区块链技术实现数据权属链上存证、利益分配智能合约自动执行，打破“数据孤岛”与“信任壁垒”，让智能体在医疗、交通等敏感场景实现安全高效的数据交互。

密态计算技术将实现“全场景适配+易用性提升”。作为数据“可用不可见”的核心支撑，密态计算将与联邦学习、安全多方计算深度融合，形成覆盖数据采集、传输、存储、计算的全流程隐私保护方案。面向智能体实时交互需求，轻量级密态计算算法将突破性能瓶颈，在边缘节点实现毫秒级加密计算响应。同时，密态计算将与开发工具链深度集成，通过可视化编程界面与预制算法模板，降低企业应用门槛。

未来，芯片的算力支撑、网络的确定性保障、可信空间的协同载体、密态计算的安全防护将形成“四位一体”的产业生态闭环。在政策引导与市场驱动下，产学研用将深度协同，培育出一批具备核心技术的领军企业、开源社区与行业联盟，推动基于确定性网络的智能体可信数据空间成为数字经济的核心基础设施，为千行百业的智能化转型注入强劲动能。

8.2 标准体系推进

在智能体可信数据空间标准体系推进上，与信通院等相关机构紧

密合作。联合信通院制定智能体身份认证标准，规范智能体数字身份的创建、管理、认证流程和接口，确保不同厂商开发的智能体能够在统一的身份认证框架下实现互认。协同信通院构建智能体数据确权与溯源标准，明确数据确权的原则、方法和溯源的技术要求，为智能体数据的合法流通和使用提供标准依据。

8.3 未来方向

基于确定性网络的智能体可信数据空间的未来发展，将深度融入国家战略与前沿技术创新浪潮，通过“东数西算”战略落地，构建更具韧性、安全与效率的数字基础设施，为智能体跨域协同与数据要素流通开辟全新路径。

“东数西算”战略的推进将与确定性网络形成“算力调度—网络支撑—可信流通”的协同体系，推动智能体可信数据空间实现跨区域资源优化配置。确定性网络将成为“东数西算”的“算力高速公路”，通过端到端时延确定性保障与动态带宽调度能力，支撑东部实时算力需求向西部枢纽节点的弹性迁移。例如，东部智能制造场景的智能体可通过确定性网络，将非实时的数据分析任务调度至西部算力枢纽，而本地边缘节点依托低时延特性保障生产控制指令的实时执行，实现“东部算实时、西部算非实时”的高效分工。

可信数据空间将为“东数西算”中的数据流通提供合规载体，通过统一的数据权属界定、安全审计与利益分配机制，破解跨区域数据共享的信任壁垒。在确定性网络支撑下，东部企业的敏感数据可在加

密状态下传输至西部算力中心进行计算，数据“可用不可见”的密态处理模式将广泛应用。同时，智能体将成为“东数西算”的“动态调度中枢”，通过感知东西部算力负载、网络状态与数据需求，基于 AI 预测模型实现算力资源的跨区域最优分配，使东部数据要素与西部算力资源的匹配效率提升 30%以上，推动形成“算力跟着数据走、数据贴着需求流”的良性循环。

未来，“东数西算”的资源优化，将推动基于确定性网络的智能体可信数据空间进入“全域协同、全域安全”的新阶段。这一融合创新不仅将夯实数字经济的基础设施底座，更将为千行百业的智能化转型提供“算力可调度、数据可流通、安全可信赖”的核心支撑，加速构建更具活力与韧性的数字生态。

附录 A：术语与缩略语

中文名称	英文缩写	英文全拼
可编程逻辑控制器	PLC	Programmable Logic Controller
时间敏感网络	TSN	Time-Sensitive Networking
可信数据空间	TDS	Trusted Data Space
软件定义网络	SDN	Software-Defined Networking
网络功能虚拟化	NFV	Network Function Virtualization

服务水平协议	SLA	Service Level Agreement
意图驱动网络	IDN	Intent-Driven Networking
未来网络基础设施	CENI	China's Emerging Networking Infrastructure
弹性以太网	FlexE	Flexible Ethernet
IPv6 分段路由	SRv6	Segment Routing IPv6
可信执行环境	TEE	Trusted Execution Environment
通用公共许可	GPL	General Public License
全球移动通信系统	GSM	Global System for Mobile Communications
增强型数据速率 GSM 演进技术	EDGE	Enhanced Data Rates for GSM Evolution
长期演进	LTE	Long Term Evolution
5G 增强技术	5G-Advanced	5G Advanced
第六代移动通信技术	6G	6th Generation Mobile Communication Technology
多协议标签交换	MPLS	Multi-Protocol Label Switching
网络地址转换	NAT	Network Address Translation
用户驻地	CPE	Customer Premises Equipment

设备		
虚拟专用网	VPN	Virtual Private Network
域名系统	DNS	Domain Name System
动态主机配置协议	DHCP	Dynamic Host Configuration Protocol
简单网络管理协议	SNMP	Simple Network Management Protocol
光传送网	OTN	Optical Transport Network
同步数字体系	SDH	Synchronous Digital Hierarchy
密集波分复用	DWDM	Dense Wavelength Division Multiplexing
粗波分复用	CWDM	Coarse Wavelength Division Multiplexing
互联网协议	IP	Internet Protocol
传输控制协议	TCP	Transmission Control Protocol
用户数据报协议	UDP	User Datagram Protocol
地址解析协议	ARP	Address Resolution Protocol
反向地址解析协议	RARP	Reverse Address Resolution Protocol
网际控制报文协议	ICMP	Internet Control Message Protocol
边界网关协议	BGP	Border Gateway Protocol
开放最短路径优先	OSPF	Open Shortest Path First

路由信息 协议	RIP	Routing Information Protocol
虚拟路由 冗余协议	VRRP	Virtual Router Redundancy Protocol
链路聚合 控制协议	LACP	Link Aggregation Control Protocol
生成树协 议	STP	Spanning Tree Protocol
快速生成 树协议	RSTP	Rapid Spanning Tree Protocol
多生成树 协议	MSTP	Multiple Spanning Tree Protocol
认证授权 计费	AAA	Authentication, Authorization and Accounting
动态主机 配置协议	DHCP	Dynamic Host Configuration Protocol
简单邮件 传输协议	SMTP	Simple Mail Transfer Protocol
邮局协议 版本 3	POP3	Post Office Protocol - Version 3
互联网消 息访问协 议版本 4	IMAP4	Internet Message Access Protocol - Version 4
超文本传 输协议	HTTP	Hypertext Transfer Protocol
超文本传 输安全协 议	HTTPS	Hypertext Transfer Protocol Secure
文件传输 协议	FTP	File Transfer Protocol
安全文件	SFTP	Secure File Transfer Protocol

传输协议		
远程登录 协议	Telnet	Telecommunication Network
安全外壳 协议	SSH	Secure Shell
网络时间 协议	NTP	Network Time Protocol
精确时间 协议	PTP	Precision Time Protocol
用户数据 报协议	UDP	User Datagram Protocol
实时传输 协议	RTP	Real-time Transport Protocol
实时控制 协议	RTCP	Real-time Control Protocol
流媒体协 议	RTSP	Real Time Streaming Protocol
移动边缘 计算	MEC	Mobile Edge Computing
雾计算	FC	Fog Computing
云计算	CC	Cloud Computing
边缘计算	EC	Edge Computing
人工智能	AI	Artificial Intelligence
机器学习	ML	Machine Learning
深度学习	DL	Deep Learning
联邦学习	FL	Federated Learning
强化学习	RL	Reinforcement Learning
自然语言 处理	NLP	Natural Language Processing
计算机视 觉	CV	Computer Vision

机器人流程自动化	RPA	Robotic Process Automation
数字孪生	DT	Digital Twin
物联网	IoT	Internet of Things
工业互联网	IIoT	Industrial Internet of Things
车联网	V2X	Vehicle to Everything
元宇宙	Metaverse	Metaverse
区块链	BC	Blockchain
智能合约	SC	Smart Contract
非同质化代币	NFT	Non-Fungible Token
分布式账本技术	DLT	Distributed Ledger Technology
哈希算法	Hash	Hash Algorithm
对称加密	Symmetric Encryption	Symmetric Encryption
非对称加密	Asymmetric Encryption	Asymmetric Encryption
数字签名	Digital Signature	Digital Signature
数字证书	Digital Certificate	Digital Certificate
公钥基础设施	PKI	Public Key Infrastructure
零信任网络架构	ZTNA	Zero Trust Network Architecture
网络安全	Network Security	Network Security
信息安全	Information Security	Information Security
数据安全	Data Security	Data Security
隐私计算	Privacy Computing	Privacy Computing
差分隐私	DP	Differential Privacy
同态加密	HE	Homomorphic Encryption
安全多方	SMPC	Secure Multi-Party

计算		Computation
数据脱敏	Data Desensitization	Data Desensitization
数据加密	Data Encryption	Data Encryption
数据备份	Data Backup	Data Backup
数据恢复	Data Recovery	Data Recovery
数据治理	Data Governance	Data Governance
数据质量管理	DQM	Data Quality Management
数据生命周期管理	DLM	Data Lifecycle Management
数据仓库	DW	Data Warehouse
数据湖	Data Lake	Data Lake
数据集市	Data Mart	Data Mart
大数据	Big Data	Big Data
实时数据处理	Real-time Data Processing	Real-time Data Processing
批处理	Batch Processing	Batch Processing
流处理	Stream Processing	Stream Processing
数据挖掘	Data Mining	Data Mining
数据可视化	Data Visualization	Data Visualization
应用程序编程接口	API	Application Programming Interface
微服务	Microservice	Microservice
容器化	Containerization	Containerization
Kubernetes	K8s	Kubernetes
Docker	Docker	Docker
服务网格	Service Mesh	Service Mesh
持续集成 / 持续部署	CI/CD	Continuous Integration/Continuous Deployment
DevOps	DevOps	Development and Operations

云计算平台即服务	PaaS	Platform as a Service
基础设施即服务	IaaS	Infrastructure as a Service
软件即服务	SaaS	Software as a Service
函数即服务	FaaS	Function as a Service
存储即服务	STaaS	Storage as a Service
数据库即服务	DBaaS	Database as a Service
网络即服务	NaaS	Network as a Service
安全即服务	SECaaS	Security as a Service
人工智能即服务	AIaaS	Artificial Intelligence as a Service
机器人即服务	RaaS	Robot as a Service
边缘即服务	EaaS	Edge as a Service
区块链即服务	BaaS	Blockchain as a Service
灾备即服务	DRaaS	Disaster Recovery as a Service
桌面即服务	DaaS	Desktop as a Service
通信即服务	CaaS	Communication as a Service
监控即服务	MaaS	Monitoring as a Service

务		
测试即服务	TaaS	Testing as a Service
知识即服务	KaaS	Knowledge as a Service
统一资源定位符	URL	Uniform Resource Locator
统一资源标识符	URI	Uniform Resource Identifier
可扩展标记语言	XML	eXtensible Markup Language
JavaScript对象简谱	JSON	JavaScript Object Notation
简单对象访问协议	SOAP	Simple Object Access Protocol
表征状态转移	REST	Representational State Transfer
移动应用	Mobile App	Mobile Application
网页应用	Web App	Web Application
原生应用	Native App	Native Application
混合应用	Hybrid App	Hybrid Application
渐进式网页应用	PWA	Progressive Web App
前端开发	Front-end Development	Front-end Development
后端开发	Back-end Development	Back-end Development
全栈开发	Full-stack Development	Full-stack Development
数据结构	Data Structure	Data Structure
算法	Algorithm	Algorithm
数据库	Database	Database
关系型数据库	Relational Database	Relational Database

非关系型数据库	NoSQL Database	Not Only SQL Database
结构化查询语言	SQL	Structured Query Language
分布式数据库	Distributed Database	Distributed Database
云数据库	Cloud Database	Cloud Database
数据中心	Data Center	Data Center
服务器	Server	Server
存储设备	Storage Device	Storage Device
网络设备	Network Device	Network Device
终端设备	Terminal Device	Terminal Device
传感器	Sensor	Sensor
执行器	Actuator	Actuator
嵌入式系统	Embedded System	Embedded System
操作系统	OS	Operating System
Linux 操作系统	Linux	Linux
Windows 操作系统	Windows	Windows
macOS 操作系统	macOS	macOS
Android 操作系统	Android	Android
iOS 操作系统	iOS	iOS
鸿蒙操作系统	HarmonyOS	HarmonyOS
麒麟操作系统	Kylin OS	Kylin Operating System

欧拉操作系统	openEuler	openEuler
龙蜥操作系统	Anolis OS	Anolis Operating System
深度操作系统	Deepin	Deepin
红旗操作系统	Red Flag Linux	Red Flag Linux
中兴新支点操作系统	NewStart OS	NewStart Operating System
中标麒麟操作系统	NeoKylin	NeoKylin Operating System
银河麒麟操作系统	Kylin Galaxy	Kylin Galaxy Operating System
统信操作系统	UOS	Union Operating System
处理器	CPU	Central Processing Unit
图形处理器	GPU	Graphics Processing Unit
张量处理器	TPU	Tensor Processing Unit
神经网络处理器	NPU	Neural Processing Unit
现场可编程门阵列	FPGA	Field-Programmable Gate Array
专用集成电路	ASIC	Application-Specific Integrated Circuit
内存	Memory	Memory
随机存取存储器	RAM	Random Access Memory

只读存储器	ROM	Read-Only Memory
高速缓冲存储器	Cache	Cache
硬盘驱动器	HDD	Hard Disk Drive
固态硬盘	SSD	Solid State Drive
光盘驱动器	ODD	Optical Disc Drive
通用串行总线	USB	Universal Serial Bus
高清多媒体接口	HDMI	High-Definition Multimedia Interface
显示端口	DP	DisplayPort
以太网	Ethernet	Ethernet
无线保真	WiFi	Wireless Fidelity
蓝牙	Bluetooth	Bluetooth
ZigBee 协议	ZigBee	ZigBee
LoRa 技术	LoRa	Long Range
5G 技术	5G	5th Generation Mobile Communication Technology
4G 技术	4G	4th Generation Mobile Communication Technology
3G 技术	3G	3rd Generation Mobile Communication Technology
2G 技术	2G	2nd Generation Mobile Communication Technology
1G 技术	1G	1st Generation Mobile Communication Technology
卫星通信	Satellite Communication	Satellite Communication

光纤通信	Optical Fiber Communication	Optical Fiber Communication
微波通信	Microwave Communication	Microwave Communication
毫米波通信	Millimeter Wave Communication	Millimeter Wave Communication
太赫兹通信	Terahertz Communication	Terahertz Communication
量子通信	Quantum Communication	Quantum Communication
可见光通信	VLC	Visible Light Communication
电力线通信	PLC	Power Line Communication
无线传感器网络	WSN	Wireless Sensor Network
无线自组网络	Ad Hoc Network	Ad Hoc Network
移动自组网络	MANET	Mobile Ad Hoc Network
无线网状网络	WMN	Wireless Mesh Network
认知无线电网络	CRN	Cognitive Radio Network
软件定义无线电	SDR	Software Defined Radio
物联网网关	IoT Gateway	IoT Gateway
工业以太网	Industrial Ethernet	Industrial Ethernet
现场总线	Fieldbus	Fieldbus
Profibus	Profibus	Process Field Bus

协议		
Modbus 协议	Modbus	Modbus
CAN 总线	CAN	Controller Area Network
LonWorks 协议	LonWorks	Local Operating Network Works
DeviceNet 协议	DeviceNet	DeviceNet
EtherCAT 协议	EtherCAT	Ethernet for Control Automation Technology
PROFINET 协议	PROFINET	Process Field Net
Sercos 协议	Sercos	Serial Real-time Communication System
CC-Link 协议	CC-Link	Control & Communication Link
自动化金字塔	Automation Pyramid	Automation Pyramid
企业资源计划	ERP	Enterprise Resource Planning
制造执行系统	MES	Manufacturing Execution System
Supervisory Control And Data Acquisition	SCADA	Supervisory Control And Data Acquisition
可编程自动化控制器	PAC	Programmable Automation Controller
分布式控制系统	DCS	Distributed Control System
机器视觉	Machine Vision	Machine Vision

运动控制	Motion Control	Motion Control
机器人学	Robotics	Robotics
工业机器人	Industrial Robot	Industrial Robot
服务机器人	Service Robot	Service Robot
特种机器人	Special Robot	Special Robot
协作机器人	Collaborative Robot	Collaborative Robot
智能制造	Intelligent Manufacturing	Intelligent Manufacturing
工业 4.0	Industry 4.0	Industry 4.0
工业互联网平台	Industrial Internet Platform	Industrial Internet Platform
数字工厂	Digital Factory	Digital Factory
智能工厂	Smart Factory	Smart Factory
黑灯工厂	Dark Factory	Dark Factory
柔性制造	Flexible Manufacturing	Flexible Manufacturing
精益生产	Lean Production	Lean Production
敏捷制造	Agile Manufacturing	Agile Manufacturing
绿色制造	Green Manufacturing	Green Manufacturing
可持续制造	Sustainable Manufacturing	Sustainable Manufacturing
增材制造	Additive Manufacturing	Additive Manufacturing
3D 打印	3D Printing	3D Printing
工业大数据	Industrial Big Data	Industrial Big Data
工业人工智能	Industrial AI	Industrial Artificial Intelligence
工业数字	Industrial Digital Twin	Industrial Digital Twin

孪生		
工业区块链	Industrial Blockchain	Industrial Blockchain
工业信息安全	Industrial Information Security	Industrial Information Security
工业网络安全	Industrial Network Security	Industrial Network Security
工业控制系统安全	Industrial Control System Security	Industrial Control System Security
工业物联网安全	Industrial IoT Security	Industrial Internet of Things Security
工业机器人安全	Industrial Robot Security	Industrial Robot Security
智能制造标准	Intelligent Manufacturing Standard	Intelligent Manufacturing Standard
工业 4.0 标准	Industry 4.0 Standard	Industry 4.0 Standard
工业互联网标准	Industrial Internet Standard	Industrial Internet Standard
数字工厂标准	Digital Factory Standard	Digital Factory Standard
智能工厂标准	Smart Factory Standard	Smart Factory Standard
柔性制造标准	Flexible Manufacturing Standard	Flexible Manufacturing Standard
精益生产标准	Lean Production Standard	Lean Production Standard
敏捷制造标准	Agile Manufacturing Standard	Agile Manufacturing Standard
绿色制造标准	Green Manufacturing Standard	Green Manufacturing Standard

可持续制造标准	Sustainable Manufacturing Standard	Sustainable Manufacturing Standard
增材制造标准	Additive Manufacturing Standard	Additive Manufacturing Standard
3D 打印标准	3D Printing Standard	3D Printing Standard
工业大数据标准	Industrial Big Data Standard	Industrial Big Data Standard
工业人工智能标准	Industrial AI Standard	Industrial Artificial Intelligence Standard
工业数字孪生标准	Industrial Digital Twin Standard	Industrial Digital Twin Standard
工业区块链标准	Industrial Blockchain Standard	Industrial Blockchain Standard
工业信息安全标准	Industrial Information Security Standard	Industrial Information Security Standard
工业网络安全标准	Industrial Network Security Standard	Industrial Network Security Standard
工业控制系统安全标准	Industrial Control System Security Standard	Industrial Control System Security Standard
工业物联网安全标准	Industrial IoT Security Standard	Industrial Internet of Things Security Standard
工业机器人安全标准	Industrial Robot Security Standard	Industrial Robot Security Standard