

2025

中国AI Agent 行业研究报告（二）

目录

CONTENTS

Part 01

AI Agent的全球认知与发展演进

Part 02

AI Agent的技术突破与行业重构

Part 03

AI Agent的商业实践与场景突破

Part 04

AI Agent的未来趋势与挑战

AI Agent 进化之路：大模型点燃智能体的变革引擎，加速AI走向应用

- Agent（代理）一概念起源于哲学，描述了一种拥有欲望、信念、意图以及采取行动能力的实体。在计算机科学和人工智能领域，“Agent”（智能体）是一个具有自主性、感知能力和决策能力的实体。智能体能够通过传感器感知其所处的环境，并根据其内部状态和预设的目标，通过执行器对环境进行影响。智能体的目标通常是在给定的环境中实现特定的任务或目标。大型语言模型（LLMs）的出现为智能代理的进一步发展带来了希望

AI Agent发展历程



人工智能领域存在AI Agent与 AI Workflow，其存在区别：

- **AI Workflow（工作流）**：指的是一系列预先定义好的大模型调用步骤，像是在“轨道上”运行，步骤固定，可预测。每一步骤都有明确的输入和输出
- **AI Agent（智能体）**：AI Agent 更加自主，由大模型自行决定执行多少步骤，直到问题得到解决。AI Agent会持续循环，例如与客户沟通或迭代代码修改，步骤数量不固定

大模型激活AI Agent发生质变提升

大模型持续进化

- 大模型赋能的新特性：强大的语言理解和生成能力
- 认知智能的突破：更接近人类思维的推理能力

"大脑级"基础设施

- AI Agent概念的重重新定位：从工具到数字助手的进化
- 大模型引爆AI Agent讨论：大模型的突破，让AI Agent从实验室走向实际应用

大模型推动AI Agent的普惠化：让AI Agent从学术讨论走向实际应用

大模型搭台，AI Agent能力进阶，撬动产业重构并浇筑生态



AI Agent 破茧：从被动听命的工具附庸到主动出击的智能先锋

通过自主感知与决策能力提升，颠覆传统 AI 定位，全方位重构人机协作崭新生态

- AI Agent通过自主感知和决策能力，实现从被动响应到主动任务启动的转变和动态策略生成。它提升了产业效率，广泛应用于金融和健康等多个场景，并重构生态系统，包括智能体开发平台和硬件。在大模型的支持下，AI Agent正从“工具”转变为“协作者”，引发生产关系的变革

自主能力定义：感知—决策全链路闭环

动态推理

基于目标的逻辑推演与冲突解决
MIT “认知内核” 理论框架

多模态感知

环境/语音/文本实时解析
Google DeepMind的SIMA
游戏Agent

AI Agent
能力组成

自主决策

非预设路径的弹性行动生成
微软AutoGen多Agent协作系统

持续进化

交互数据驱动的策略迭代
OpenAI GPT-4自我反思机制

与传统AI工具的颠覆性差异

传统AI工具

AI Agent

任务触发

人类指令触发
(如Siri问答)

环境感知自主启动
(如特斯拉FSD预判刹车)

决策机制

规则驱动
(if-else逻辑树)

目标驱动
(LLM生成动态策略树)

交互模式

单次请求-响应

长期记忆支持的连续对话与协作

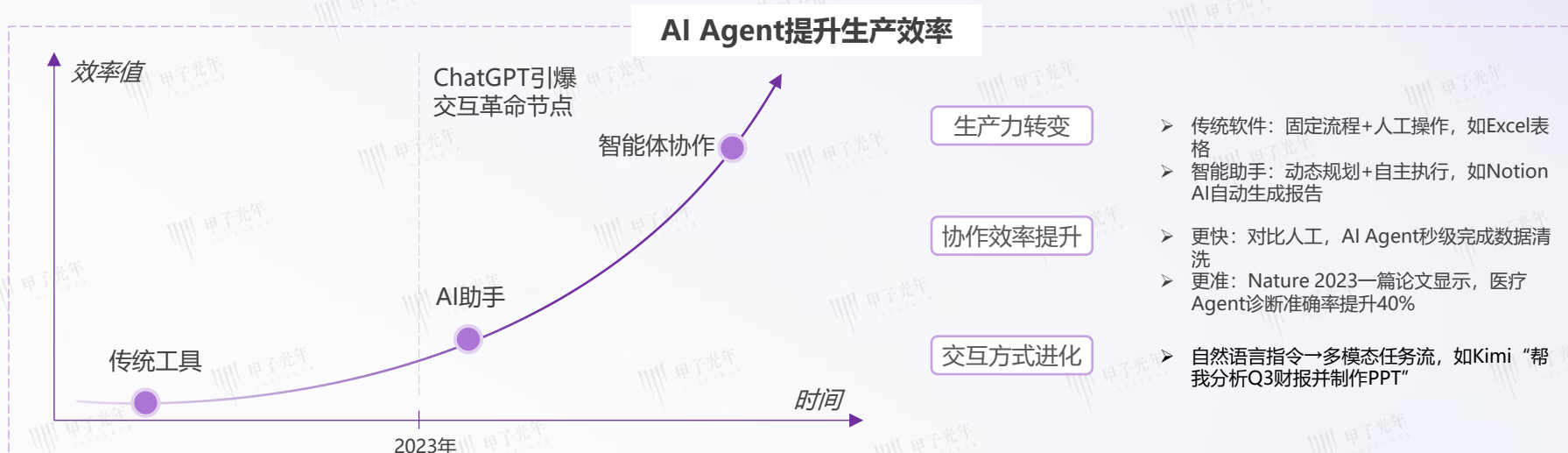
能力边界

限定场景封闭系统

跨领域经验迁移
(如医疗Agent转金融风控)

AI Agent的产业价值：重塑人机协作方式，推动效率变革

从效率工具到智能协作者的范式升级，AI Agent成新时代的革命性生产力



现阶段构建法则

简单起点+量化验证

- 例：从会议纪要生成→逐步扩展至全流程项目管理
- 测量指标：任务完成率/错误率下降曲线

护城河绑定模型进化

- 反例：仅做Prompt包装的产品将被淘汰
- 正例：AutoGPT构建工具调用生态

AI Agent思维培养

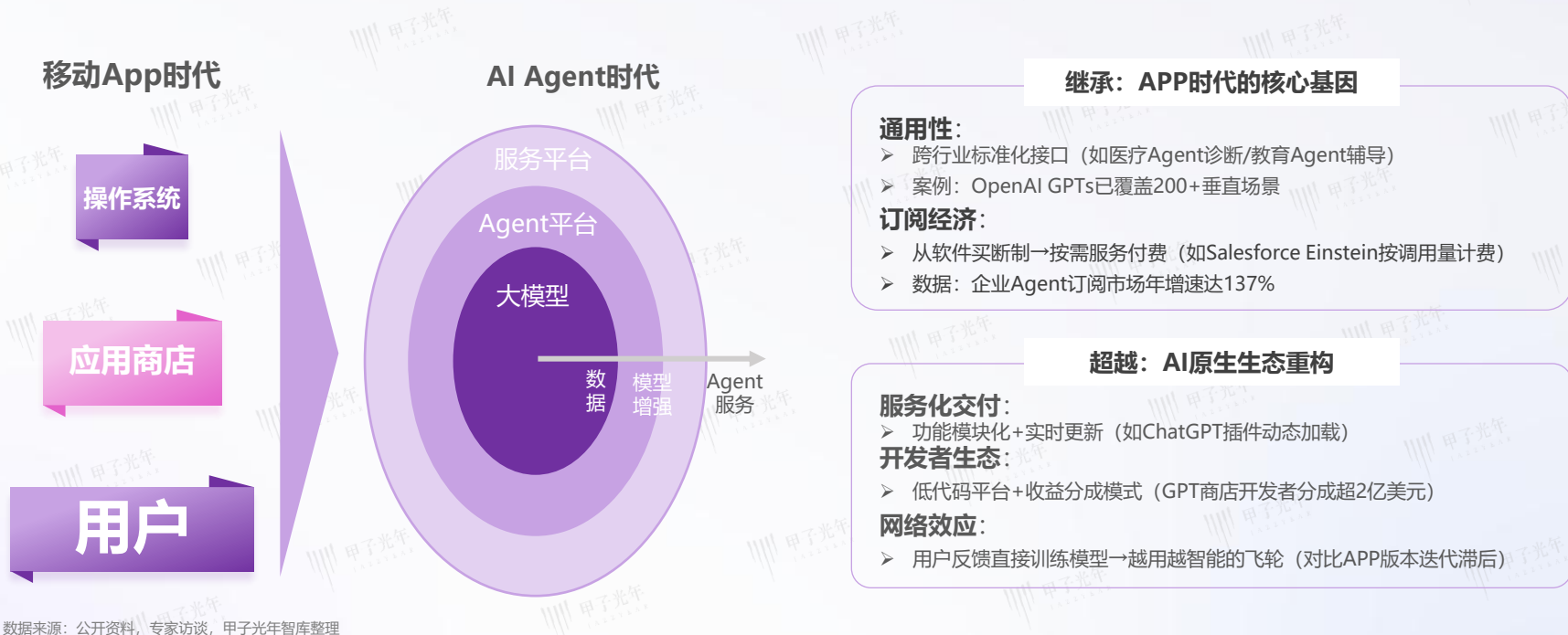
方法论：

- 用“目标-推理-验证”框架替代传统功能清单

AI Agent的商业模式：移动时代APP的继承与超越

从“应用商店”到“智能体”平台的转型升级，推动AI生态的快速重构与创新发

- **从应用到智能体服务的升维：**AI Agent继承APP的规模化分发能力，但通过大模型实现三个突破——服务动态进化、收益与价值实时匹配和开发者 - 用户 - 模型协同进化。预计到2027年40%的企业服务将由AI Agent组合交付，这不仅是技术升级，更是软件经济规则的重构



大模型能力持续进化，推动AI Agent从任务执行者（copilot）向决策主体跨越

- AI Agent正通过认知能力的三重重建建立竞争壁垒：在感知层打破模态边界，在决策层构建动态规划，在进化层实现终身学习。这使其超越Copilot的工具定位，成为真正的‘数字员工’。到2026年认知型Agent将覆盖70%的企业复杂决策场景，重新定义生产力革命

技术演进：大模型重塑AI本质



竞争分水岭：Copilot→Agent的跨越



大模型能力提升：基于大模型的AI Agent可颠覆现有的工作范式

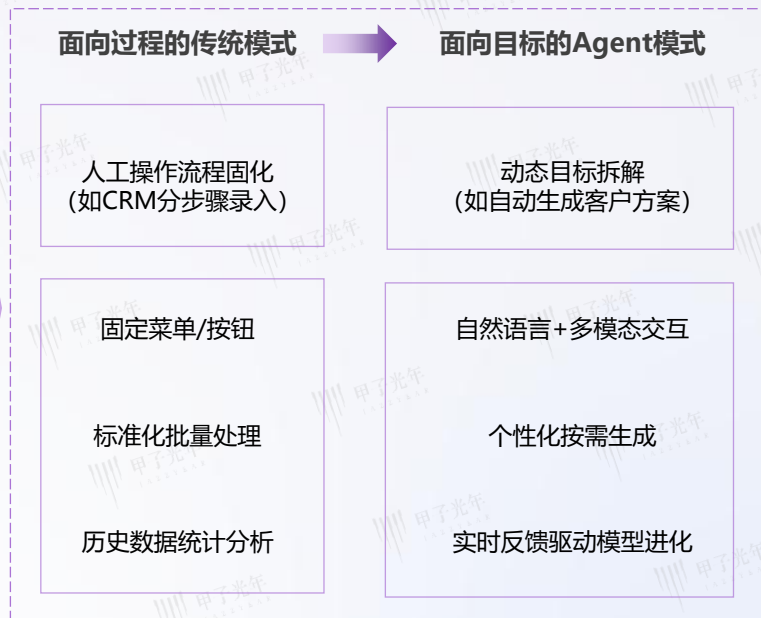
从工具执行到自主决策的能力升维，最终实现Agent从“四肢”到“大脑”的进化

- AI Agent正引发生产力范式的双重革命：在能力维度，通过记忆感知（L4）和数字人格（L5）实现人类意图的深度理解；在产业维度，推动 workflow 从‘操作说明书式’过程执行转向‘结果导向’的智能编排

基于大模型AI Agent不同自动化程度所需要的能力简要分析

	关键特征	代表用例
L1 (简单步骤跟随)	代理通过遵循用户或开发者预先定义的确切步骤来完成任务。	“打开 Messenger” “打开邮箱中第一封未读邮件并读取内容”，“给爱丽丝打电话”
L2 (确定性任务自动化)	基于用户对确定性任务的描述，代理在预定义的动作空间中自动完成步骤。	“查询北京今天的天气”
L3 (战略任务自动化)	基于用户指定的任务，代理自主使用各种资源和工具规划执行步骤，并根据中间反馈迭代计划直至完成。	“给爱丽丝打视频电话”
L4 (记忆和上下文感知)	代理感知用户上下文，理解用户记忆，并有时主动提供个性化服务。	“告诉扫地机器人今晚打扫房间”，“告诉爱丽丝我明天的日程安排”
L5 (数字人格)	代理代表用户完成事务，代表用户与他人交互，确保安全和可靠性	“找出最近适合旅行的城市”

AI Agent的能力提升促进工作范式转移



从“流程固化”到“任务智能”，企业软件从‘工业化’到‘智能化’的质变

- AI Agent正通过**三层重构**颠覆企业服务：交互层（自然语言取代复杂界面）、逻辑层（目标导向替代流程固化）、价值层（从‘人适应系统’转向‘系统服务人’）。到2026年60%的企业将部署AI Agent，其核心价值不仅是效率提升，更是通过**降低数字化摩擦**释放组织创新潜能

传统软件VS AI Agent的破局对比

传统企业软件

流程数字化，如ERP/SAP刚性规则

平均3个月员工培训

仅覆盖30%高频场景

版本迭代周期≥6个月

AI Agent解决方案

任务目标驱动，如动态拆解KPI

自然语言指令，零学习门槛

解决70%非标需求

实时在线学习（周级模型微调）

VS



AI Agent实践案例

供应链管理

传统企业软件

SAP需手动配置参数，
平均响应72小时

AI Agent

沃尔玛：动态预测缺货风险，
自动生成补货方案（时效压缩
至15分钟）

客户服务

传统企业软件

CRM预设话术，首
次解决率≤40%

AI Agent

Zendesk：通过情感识别+知
识图谱，解决率提升至78%

AI Agent生产力：打造企业级“数字员工”，重塑生产力边界的智能范式

数字员工正在成为行业标配，提供自动化、高效、准确的工作支持

- 数字员工正逐步成为各行业的标配，通过自动化和智能化的支持，显著提升工作效率和准确性。它不仅帮助企业降低成本，还通过数据分析为决策提供支持，推动个性化服务与国际化扩展。未来，企业将更加依赖这一新型“数字员工”，以保持竞争优势和市场适应性

核心价值主张

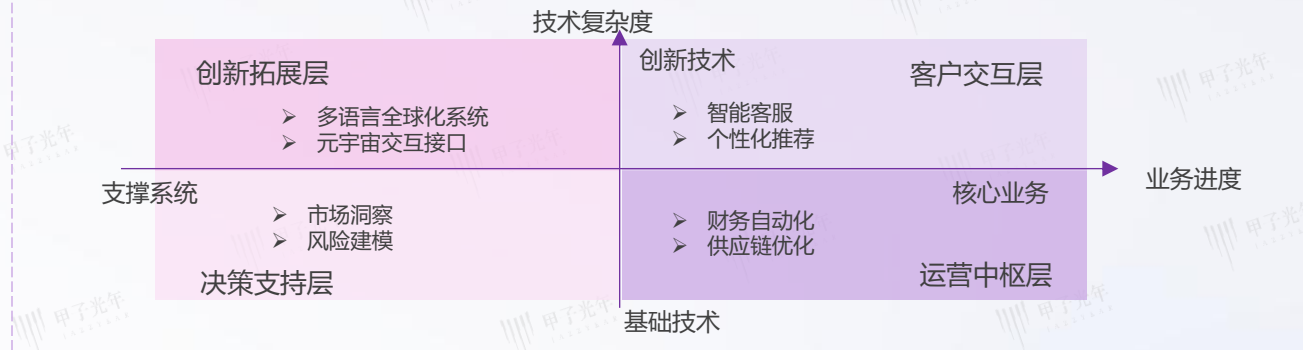
定义进化：

- 具备自主任务处理能力的AI系统集群，覆盖“感知-分析-决策-执行”全链路

战略价值：

- **人效提升**：RPA+AI实现业务流程自动化率超80%
- **决策精度**：机器学习模型使运营决策准确度提升65%
- **成本结构**：三年期ROI达400%，人力密集型场景降本45%

AI Agent场景化应用矩阵

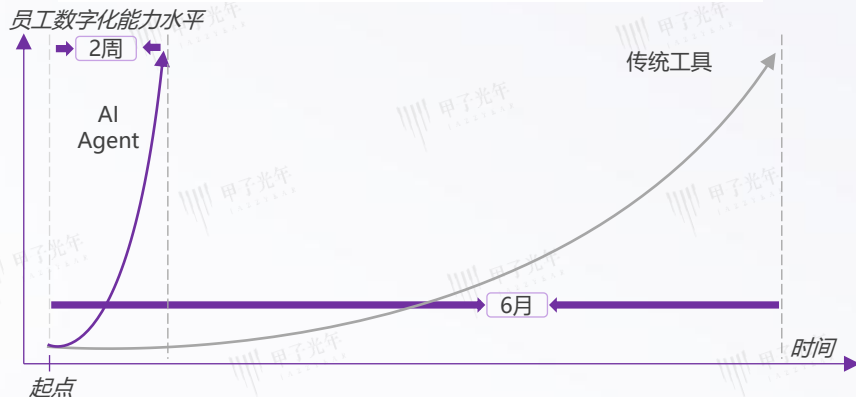


AI Agent技术支撑场景应用与拓展



AI Agent加速员工数字化水平提升，重塑人机协作的知识平权 and 专业化进程

AI Agent能力升维，提升员工数字化水平



传统困境

技术门槛：

- 非IT员工需学习复杂系统，平均培训成本¥20,000/人

知识断层：

- 20%关键岗位人员掌握80%数字化技能

AI Agent破局

教练模式：

- 实时工作流指导，如Microsoft 365 Copilot文档优化建议



助手模式：

- 自动生成分析报告，如Salesforce Einstein案例：
- 平权效应：
- 自然语言交互使技能获取效率提升5倍



相比传统，AI Agent个性化赋能员工

传统培训体系

AI Agent赋能体系

知识传递

单向灌输
(课程→考核)

场景化浸润
(工作流实时反馈)

技能应用

脱离实际
业务场景

任务驱动的自适应学习，
如AWS Q优化运维决策)

进化速度

年度更新周期

实时模型微调
(周级知识库迭代)

VS

AI Agent是AGI的载体：AI Agent是具备能动性的“图书馆”

- AI是包含所有多媒体形式存储的知识的“图书馆”，那么AI Agent是、具备能动性、能与物理世界互动、并改变物理世界的“图书馆”
- 能动性是将智力转化为实际价值的催化剂，是一种比智力本身更具决定性的品质。在相同条件下，高能动性者往往能比高智力者取得更显著、更持久的成就

AI的纯智力与AI Agent的能动性

Intelligence

智力
(Intelligence):
思考、分析、
学习和解决问
题的能力

VS

Agency

能动性(Agency):
主动采取行动、做出决
策并影响环境的能力,
体现为:

- 主动设定目标并坚
定追求
- 在面对障碍时寻求
解决方案
- 内在控制点(认为自
己掌控命运)
- 自我效能感、决心
与责任感的综合体

AI Agent的能动性优于AI的纯智力

Intelligence

Agency

AI Agent 在真实物理世界条件下强于纯人工智能 (AI)

能动性 (Agency) 价值大于纯思考 (Intelligence)

- 再高的智力不付诸行动也只是潜能，而中等智力配合高能动性却能创造实际价值。

稀缺性差异

- 高智力的大模型相对常见，而真正具备高能动性的AI Agent却极为稀缺。

能动性能够调动并放大智力

- 具备能动性的AI Agent会积极寻求提升自己智力的方法，而高智力的AI模型却不必然导致更强的行动力。

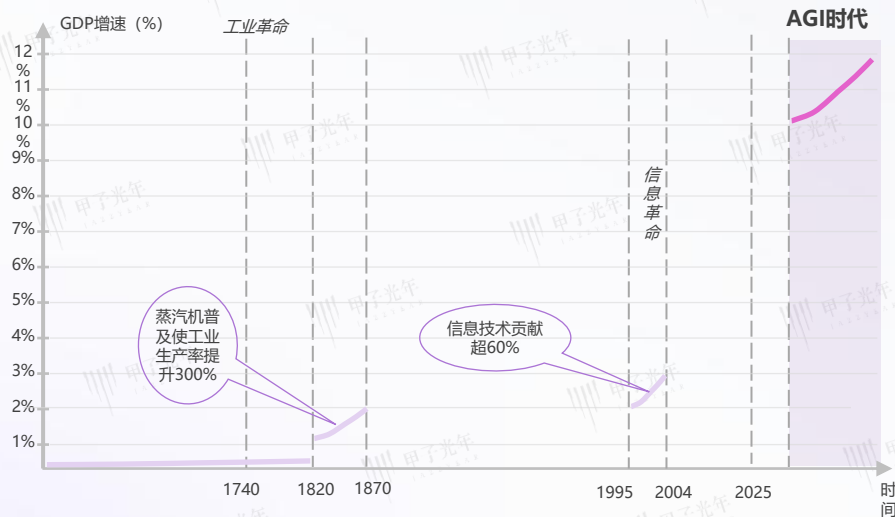
社会结构偏差

- 社会教育体系和社会评价体系过度强调智力测量（对AI也是如此），却很少关注和培养能动性，导致能动性在AI Agent市场中更为稀缺。

当AI推动经济达到10%增长，才是AGI时代，而AI Agent是将会是AGI重要载体

- Satya Nadella为AGI时代的到来设定了一个明确的经济量化标准：唯有当AI能推动全球经济实现10%的增长率时，才算真正迈入AGI时代
- 这一标准的提出建立在对当前经济现状的深刻洞察之上 - 发达国家GDP年增长率仅约2%，若考虑通胀因素，实际增长几近于零。因此，若AI要引发堪比工业革命的变革，至少需要带动发达国家实现5-7%的实际增长率。具体而言，以当今100万亿美元的世界经济规模为基准，10%的增长意味着每年将创造10万亿美元的新增价值，这一指标巧妙地将抽象的技术进步转化为可衡量的经济增长目标

不同时期技术革命对GDP增速的影响



数据来源：Satya Nadella、《英国工业革命中的技术变革》，美国劳工统计局，甲子光年智库整理

突破AGI的核心指标

	现在	AGI时代	
发达国家GDP增速	约2% (实际增长近零)	5%-7%实际增长	工业革命期英国年均增速2-3%
全球经济增量	窄AI贡献约0.1%-0.3%	年增10万亿美元 (10%增速)	工业革命200年累积增长10倍
技术渗透率	AI覆盖 < 10%职业 (OpenAI)	覆盖80%职业与经济活动	电力普及率达90% 耗时40年

量子计算有望
加快渗透

基于LLMs的AI Agent推动下，AGI时代有望在十年内到来

➤ 当前，AGI（通用人工智能）尚未形成统一标准，行业领袖从不同维度提出定义：认知能力、科学发现与经济创造。Anthropic CEO阿莫代主张AGI需具备“多领域人类顶尖水平”，如AI Agent在医疗、法律等场景中完成诺贝尔奖级任务；谷歌DeepMind CEO哈萨比斯则认为AGI的核心是“信息稀缺下的理论创造”，例如Project Astra通过多模态融合自主设计量子算法，接近爱因斯坦式科学突破；而OpenAI与微软则聚焦经济价值，特斯拉FSD等AI Agent通过全自动驾驶每年节省全球物流成本超3000亿美元，验证了“千亿美金系统”的潜在标准

不同维度下的AGI标准和预期到来的时间

	代表者	AGI标准	预测时间
认知能力	Anthropic CEO Dario Amodei	✓ 多领域全才型智能（如诺贝尔奖级跨学科能力） ✓ 人类水平认知泛化（无需领域微调）	2026-2027年
科学发现	Google DeepMind CEO Demis Hassabis	✓ 信息稀缺下的理论创新（如发明相对论） ✓ 自主创造复杂系统（如设计新棋类规则）	2030年代初期
经济创造	OpenAI Sam Altman Microsoft CEO Satya Nadella	✓ 单系统创造千亿美元价值 ✓ 推动GDP年增10%（发达国家）	2027-2030年

AI Agent的多元实践正推动AGI从技术概念走向现实：认知能力不断扩展，科学发现需突破多模态创造力，经济价值倒逼规模化落地。

数据来源：Satya Nadella、Sam Altman、Dario Amodei、Demis Hassabis、甲子光年智库整理

模型优化与普及浪潮下的算力黑洞与破局路径，技术单点优化与系统性指数扩张

- AI技术的能效悖论已然显现：当单个智能体能效提升30%时，全球算力需求却激增50%，揭示出典型的杰文斯陷阱。据国际能源署，2030年AI或将消耗全球5%电力
- AI Agent在普及过程中还需要：重构技术架构削减冗余计算，云边端动态调度化解能耗峰值，共享算力经济遏制资源空转，此外量子计算也可以解决AI Agent面临的数据能力和能源消耗所带来的挑战。这场能效革命标志着AI发展逻辑的根本转向——从参数军备竞赛转向单位能耗智能产出的效能竞争

杰文斯（Jevon’s）悖论

	工业革命	信息革命	AI革命
核心资源	煤炭、钢铁	电力、数据	算力、数据
技术驱动	瓦特改良蒸汽机	摩尔定律	大模型能力不断提升
矛盾表现	单台机器耗煤量降低30%，但总消耗量增加10倍	单芯片能耗降低50%，但数据中心总耗电量增加400%	单任务能耗降低30%，但全局算力需求增速达50%/Y
触发机制	规模化生产需求激增	网络效应与用户扩张	智能泛在化部署
解决路径	石油替代煤炭	能效标准+低功耗芯片	算法革新+架构革命
演进特点	单维度能源消耗	能源+数据双重消耗	算力+数据需求大增，量子计算取得突破

破局之道



Part 01

AI Agent的全球认知与发展演进

Part 02

AI Agent的技术突破与行业重构

Part 03

AI Agent的商业实践与场景突破

Part 04

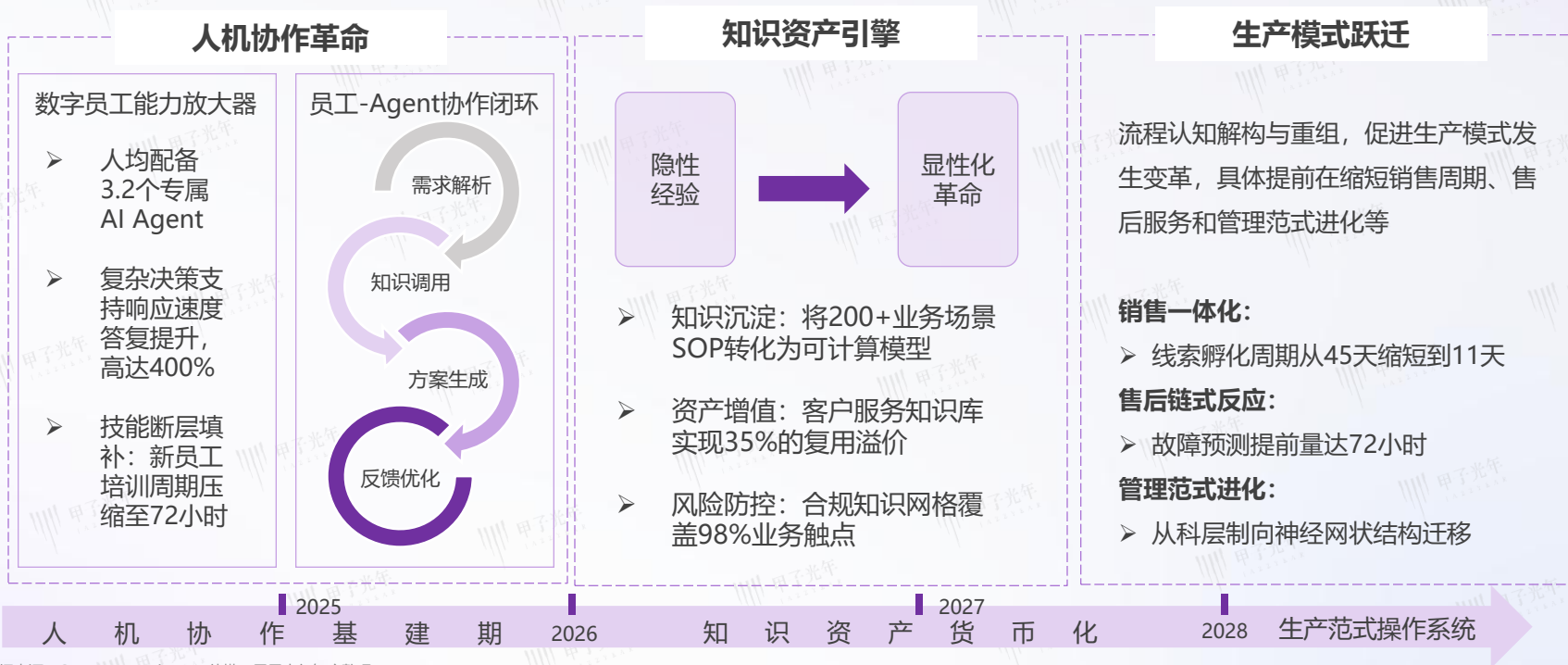
AI Agent的未来趋势与挑战

目录

CONTENTS

重构人机边界·激活知识资本·重塑生产范式，从数字助力到认知重构的企业操作系统

- 当AI Agent渗透率突破40%临界点，企业将经历从‘工具使用’到‘认知共生’的范式迁移。这不仅带来58%的运营效能提升，更将重构企业DNA——知识资产成为新资产负债表核心科目，流程智能化为新的核心竞争力，最终实现组织从机械执行体向认知有机体的进化

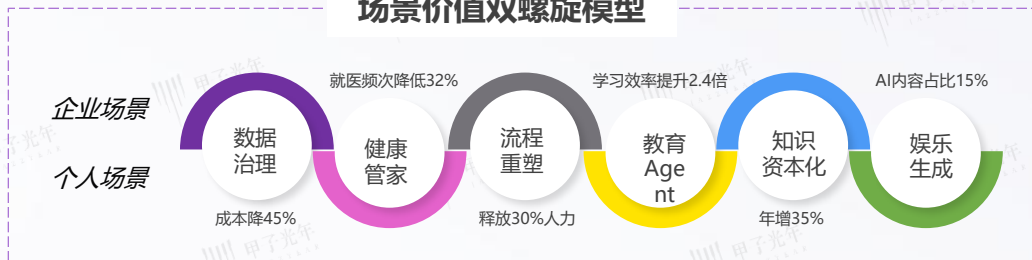


不同领域的场景化突破：企业级场景与个人场景全面覆盖

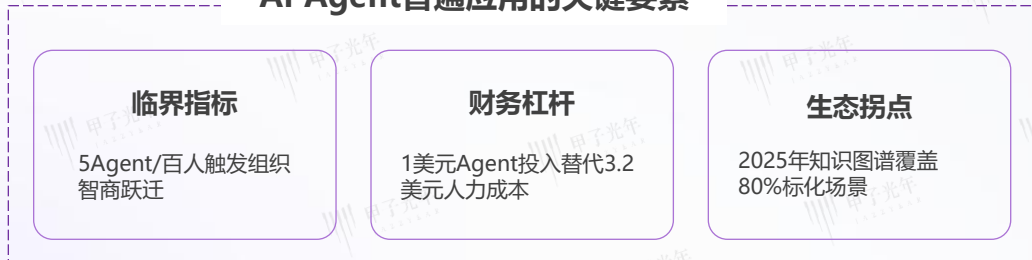
研发、设计、采购、物流等企业生产经营与个人工作生活娱乐全场景覆盖

- AI Agent的应用潜力进行全场景分析：行业渗透率方面金融/医疗/工业较高，其次为消费/教育，之后是文旅/建筑；在企业级AI Agent场景成熟度方面研发/供应链高于人力/财务；在个人级AI Agent场景成熟度方面，健康/学习高于娱乐等
- 应用潜力较高的场景为：专业领域的自动化助手&生活化的个性化陪伴伙伴可能最先突破，尤其是金融、法律、医疗等专业等领域

场景价值双螺旋模型



AI Agent普遍应用的关键要素



典型场景



金融、医疗、教育、工业制造、文旅率先突破，赋能全场景价值链

- 金融、医疗、教育、工业制造、文旅五大行业凭借技术融合与政策支持，已进入规模化应用拐点。其全链条场景覆盖能力将重塑产业生态，成为经济增长的核心引擎



具体应用场景

行业	具体应用场景
金融	数字化支付、区块链、智能风控加速渗透
医疗	AI辅助诊断、远程医疗、精准医疗技术突破
教育	个性化学习平台、虚拟现实（VR）教学场景落地
工业制造	工业互联网、智能工厂、数字孪生技术应用
文旅	沉浸式体验、智慧景区、IP衍生经济崛起

AIGC产业格局重构：大模型竞争进入“生态+场景”下半场

未来决胜关键——开放生态、垂直深耕与数据闭环能力

- 大模型竞争已从技术“军备竞赛”转向**生态协同与场景落地效率**的比拼。产业竞争焦点已从单纯的技术突破，转向了更复杂的生态系统构建与商业价值实现。成功的关键在于如何将技术创新转化为可持续的商业模式，并在特定垂直领域形成不可替代的竞争优势



在大模型竞争下半场一些典型案例

	落地策略	案例
开放生态	开发者激励计划、模型微调工具包	百度文心“千帆生态”接入超800家企业
高质量数据应用	行业知识库构建、数据隐私合规解决方案	科大讯飞医疗大模型与三甲医院数据合作
商业化能力	按需付费模式（API调用量）、订阅制SaaS	阿里通义千问推出企业专属模型版本
社区共创	用户反馈驱动迭代、开源社区贡献奖励机制	Hugging Face模型众包优化案例

AI Agent产业厂商动态：动作越来越频繁，行业竞争趋于白热化

- AI Agent产业在2024年第四季度至2025年初呈现快速迭代态势，从技术竞争转向生态价值重构。通信运营商、科技巨头和专业厂商的多元竞争，推动该领域从单点突破走向"模型-工具-生态"的协同创新
- 企业竞争焦点已从**通用能力**转向**场景深耕与生态整合**，尤其在企业管理、代码编程等高频场景构建数据闭环优势。通过降低开发门槛、开放API接口，加速形成"技术-应用-反馈"的正向循环，这将重塑产业格局与价值分配

2024 年 9 月 至今AI Agent 领域行业动态

时间（年月）	产品/技术	参与者	意义
2024年9月	BetterYeah AI Yeah客服	BetterYeah AI	基于原有企业级AI Agent开发平台，发布首款官方AI应用「Yeah客服」
2024年9月	容联云容犀Copilot & Agent	容联云	为企业在营销和客服领域提供全面的AI解决方案，有效提升企业营销转化率，降低客诉率。
2024年10月	微软Dynamics 365集成自主AI Agent	微软	增强企业管理软件的智能化水平，实现多业务领域的自动化，提高企业运营效率。
2024年10月	卓世科技“AI家庭医生”智能体	卓世科技	通过深度强化学习优化医疗健康、政务、文教传媒、能源制造行业复杂推理，降低模型部署成本，打造全链路AI解决方案。
2024年10月	中国移动灵犀消息智能体	中国移动	推动AI在通信领域的应用，提升用户通话等场景中的体验，拓展智能体在通信场景中的应用边界。
2024年12月	谷歌Gemini 2.0驱动AI Agent原型	谷歌	拓展AI Agent在多领域的应用，推动多模态AI Agent的发展，为用户提供更全面、智能的服务。
2024年12月	中国电信星辰智能体	中国电信	通过自主规划和工作流两大模式解决大模型落地痛点，快速搭建“会展助手”智能体，提升工作效率。
2024年12月	字节跳动MarsCode	字节跳动	为国内开发者提供一款功能强大的AI代码编程工具，提高编程效率，推动国产AI编程工具的发展。
2025年1月	Claude 3.5 Sonnet升级版	Anthropic	提升AI在代码开发和计算机操作模拟方面的能力，为开发者提供更智能的辅助工具，推动AI在软件开发领域的应用。
2025年1月	AI Agent Operator	OpenAI	拓展AI Agent的功能边界，为用户提供更强大的自动化任务执行和知识生成能力，推动AI Agent在多领域的应用。
2025年1月	阿里云推出通义千问Qwen2.5 - Max模型	阿里云	提升国内大模型在多模态交互和复杂任务处理方面的能力，为AI Agent的开发提供更强大的基础模型支持。
2025年1月	拓尔思拓天大模型AI Agent工具链	拓尔思	降低AI Agent的创建门槛，推动AI在多个行业的应用落地，为行业智能化转型提供有力工具。具备任务规划、流程编辑与自动执行功能，已在金融、政务、媒体和智库等多个行业场景落地。
2025年2月	GitHub Copilot Agent模式	GitHub	提升AI在代码开发中的自主性和智能性，推动软件开发模式的变革，提高代码开发的效率和质量。
2025年2月	DeepSeek - R1	幻方量化	降低AI Agent开发门槛，推动开源生态与行业应用的结合，为国内AI Agent的发展提供新的技术支撑和开源资源。
2025年2月	视语坤川智能体应用平台	中科视语	基于视觉大模型实现工业柔性产线与交通管理智能化，端云协同加速传统行业AI渗透。
2025年3月	Manus	Monica.im	工具链整合能力的规模化跃升迎来中国AI Agent重大突破时刻，推动AI Agent从对话智能升级为生产力操作系统。

DeepSeek的出现实现了从“暴力计算”到“精准效能”的技术跃迁

- AI Agent正经历从**中心化到泛在化的历史转折**：小模型突破冯·诺依曼瓶颈（模型体积缩小80%）、低能耗重构算力经济（单位智能成本下降99%）、跨场景释放长尾价值、多模态重塑人机接口（语音/视觉/触觉融合）。这场变革的本质是将智能从‘云计算神殿’带入‘现实毛细血管’。此外，DeepSeek验证了开源模型超越专有模型的可能性，其技术路径或将成为AI Agent从实验室走向产业的核心推手

未来技术四维演进

维度	技术突破	标杆实践
小模型	TinyML技术 (<10亿参数)	微软Phi-3: 手机端运行, 医疗 诊断准确率98% 
低能耗	能效比提升50倍 (MoE架构)	谷歌Gemini Nano: 单设备推理 功耗<1W 
跨场景	元学习迁移框架 (场景切换耗时 <5分钟)	特斯拉Dojo: 工厂→家庭机器 人无缝迁移 
多模态	神经符号系统 (文本→3D场景 生成)	OpenAI Sora: 物理引擎实时渲染 

技术对产业的重构

技术重构

- 隐私计算：联邦学习使医疗数据不出城
- 轻量化：DeepSeek-R1 API价格仅为行业均值的5%，推动企业级部署成本下降90%
- 精准认知：支持金融/医疗等长尾场景多模态需求

商业价值重构

- 以DeepSeek R1模型为例，通过开源协作与高效架构设计，推理成本相比传统模型大幅降低，使中小企业可负担高精度AI Agent部署
- 以DeepSeek为例，在零售电商、金融保险等复杂场景的独立解决率得到提升，减少人工干预需求

DeepSeek的出现

技术升维： deepseek

- 通过轻量化（大幅降低成本）与精准化（准确率明显提升），突破“暴力计算”时代能效天花板

生态重构：

- DeepSeek开源战略催生开发者社区热度，推动智能从“中心化云”向“边缘节点”渗透

伦理觉醒：

- 推理路径可视化与主动伦理框架，重塑企业级AI信任基线

产业爆发：

- 在工业（能效管理）、消费（多模态硬件）、开源（个人开发者）三大阵地验证“普惠智能”可行性。预计2027年60%企业将采用DeepSeek类方案

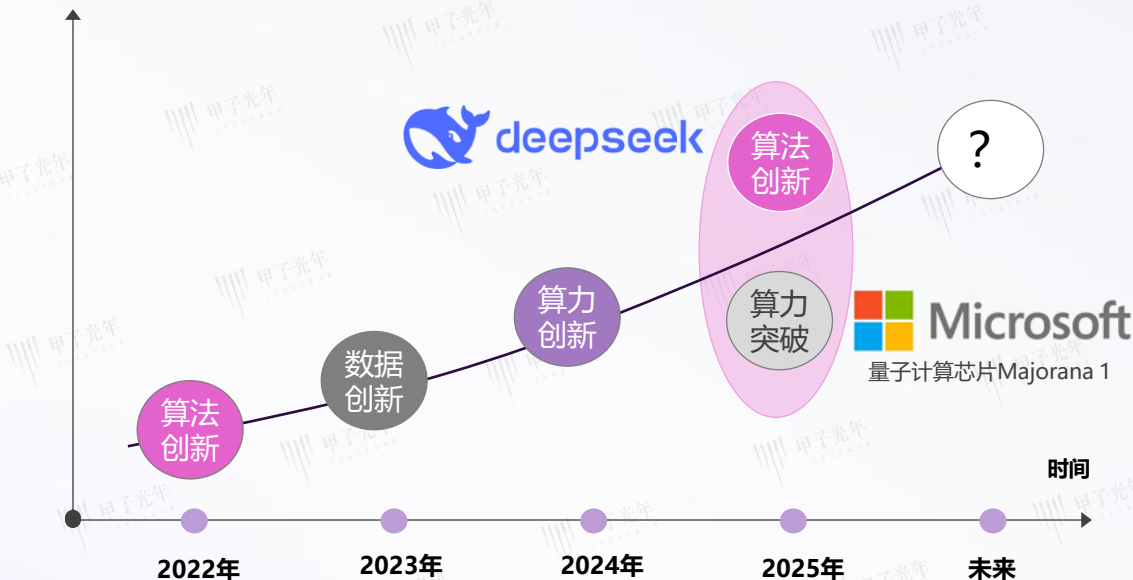
AI Agent技术路径的循环：算法创新+算力突破再次成为新的突破点

技术创新一直围绕着核心三要素，2025年再次进入算法创新+算力突破新阶段

每年AI技术创新发展的方向围绕三要素迭代展开

AI技术成熟度

核心三要素的创新循环



- 算力、数据、算法的三角创新体系，在动态循环之中再次进入算法创新阶段
- 2022年：算法创新为主，ChatGPT发布，引发Transformer架构的风潮迭起
- 2023年：数据创新为主，数据合成、数据标准等成为高质量数据集建设的热点方向
- 2024年：算力创新为主，算力迈向超万卡时代，算力运营商等产业新物种诞生
- 2025年：再次进入算法创新与算力突破阶段

DeepSeek算法变革推动AI普惠应用，加速AI Agent普及和应用

DeepSeek的“高性价比”有望解锁AI Agent的理解、推理及普遍应用

- DS基于算法工程方面的优化，DS能够实现性价比更高的模型推理能力（价格低、效率高、性能强、可部署在端侧平台）
- 大模型的价格快速下降。OpenAI 的 o1 每输出 100 万令牌收费 60 美元，而 DeepSeek-R1 只需 2.19 美元。这将近 30 倍的价差，让算力成本不再是模型门槛，正在让基础模型层“平民化”。推理成本的颠覆性降低，将会推动C端产品在大多数应用场景得到落地。尤其是在星云象限和星团象限之中的应用场景，将会得到全面的落地

DeepSeek的性价比&效率优势，有望加速具身智能技术发展普及

低成本和高效率对于实现规模化应用和商业化至关重要

降低训练成本

- 以较低的成本训练出高质量的模型

加速研发速度、加速迭代速度、降低开发门槛

降低推理成本

- 性能更强的中小模型蒸馏
- 更低的计算成本在真实硬件上运行

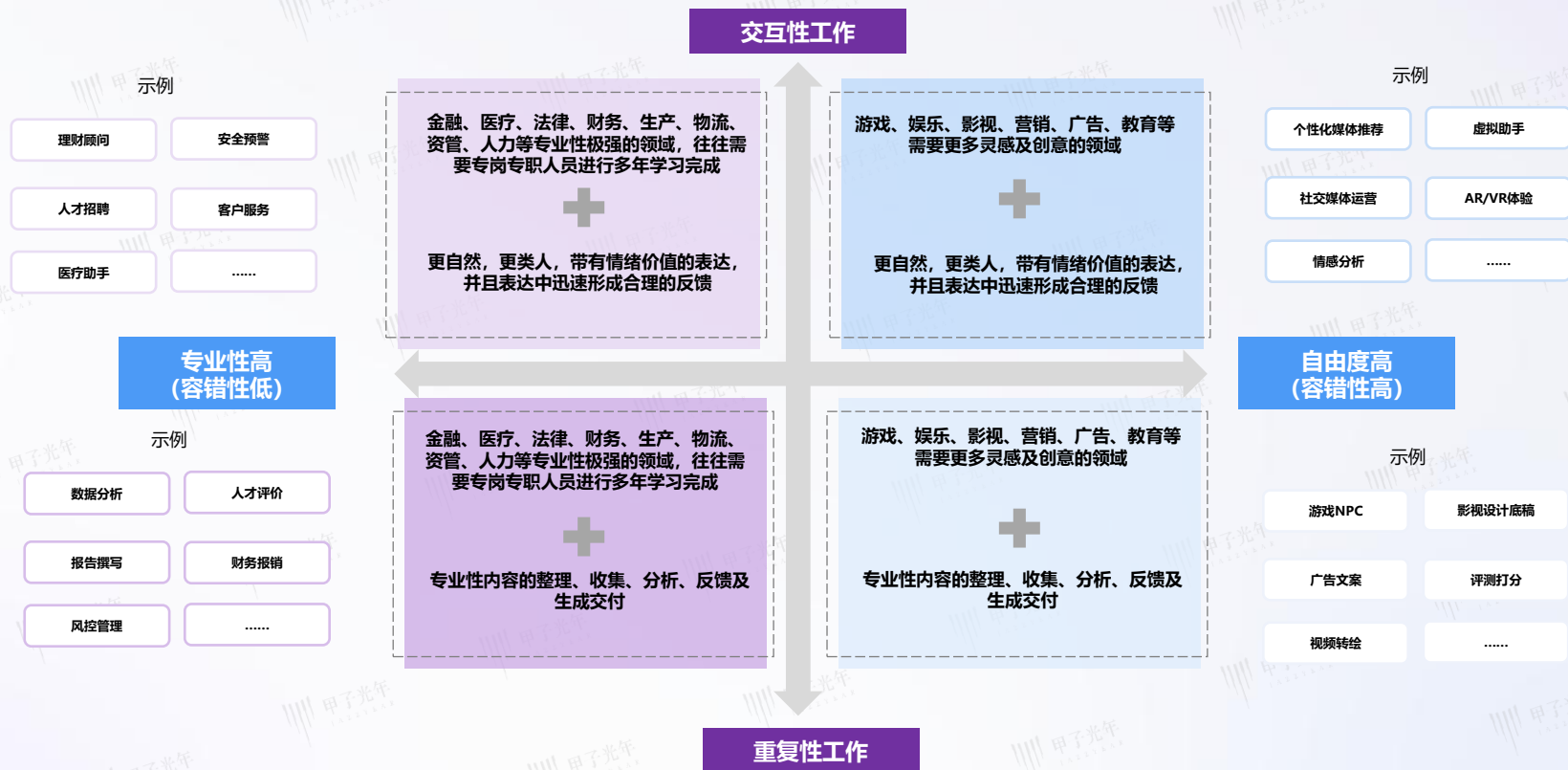
端侧平台部署、提升反应速率、降低计算能耗

图：甲子星空坐标系—生成式AI在C端应用场景的商业潜力评估



AI Agent的场景化应用：大模型走向行业落地的第一步

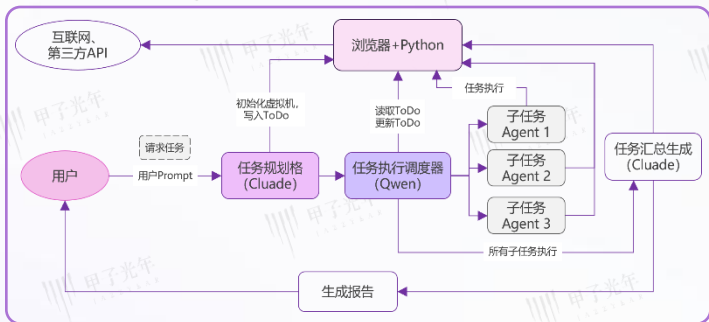
所有行业都值得用AI重新做一遍，AI Agent是实现这一目标的关键形式



Manus在交互及用户体验上有大创新大突破，但受限于模型与数据，护城河暂未能构筑

- 2025年将成为AI Agent商业化应用元年。对于现阶段 AI 产品而言，护城河主要为模型 + 算力、数据、用户体验。头部玩家以不同路径筑墙：OpenAI有强大的模型基座，Google深耕数据搜索，而新锐产品（Perplexity、Cursor和Manus）则有大量用户数据沉淀后的用户体验
- Manus 的工作流程呈现清晰的分层协作架构：用户发起需求后，模型首先进行任务拆解与规划，生成结构化待办清单；调度器随即分配子任务至专用Agent群，驱动虚拟机中的浏览器/Python环境执行数据抓取、API调用等操作；执行结果实时回传并由Claude 二次介入，整合多源数据生成最终报告。该架构通过高低阶模型协同与工具链（调用6-8个工具）深度绑定构建出从需求输入到成果交付的完整自动化链路
- 与其他AI产品（GPT/Claude）相比Manus的护城河在于生态占位+数据飞轮：通过早期发布抢占企业自动化中枢生态位，沉淀用户场景数据（如合同审核流程偏好），形成“越多人用→越懂需求→体验越精准”的闭环。其分层架构（Claude规划/Qwen调度/Agent执行）虽可复刻，但业务流寄生性（用户核心流程深度绑定）与动态知识图谱（实时优化私有化 workflow）构成迁移壁垒

manus 工作原理



Manus是中国AI Agent领域的现象级产品，其阶段性突破的核心在于工具链整合能力的规模化跃升，但技术护城河也相对薄弱。在Manus发布后次日便出现了OpenManus

Manus 与其他AI产品比较

	Manus	GPT/Claude
核心能力	主动调用浏览器、代码编辑器等工具直接完成任务	通过文本对话提供建议，无法直接操作外部工具
运行环境	云端独立计算环境，无需用户监督	依赖用户提供的运行环境（如本地设备）
协作模式	类人类同事：中途可调整需求，支持偏好记忆（如“以后都这样做”）	工具型交互：需逐步指导，偏好重复说明
主要优势	自动化执行复杂任务-多领域任务融合处理-迭代式成果优化	即时问答-创意文本生成-简单数据处理
适用场景	批量文件处理、深度调研分析、跨平台数据整合与可视化	信息查询、内容创作、基础代码协助、简单任务指导
用户交互特点	简单提示即可输出完整内容	需详细分步指导-每次对话需重新说明需求
任务执行特性	后台自主运行（委托-交付模式），支持中途干预调整策略	需要持续对话引导，复杂任务易中断
学习进化能力	通过用户反馈持续优化工作模式	对话历史记忆有限，需重复训练
成果交付形式	直接生成最终成果文件（报告/可视化图表/处理后的数据包等）	提供文本/代码建议，需人工复核执行

Part 01

AI Agent的全球认知与发展演进

Part 02

AI Agent的技术突破与行业重构

Part 03

AI Agent的商业实践与场景突破

Part 04

AI Agent的未来趋势与挑战

目录

CONTENTS

AI激起的浪花，促进AI Agent迅速成为潮流

- AI Agent技术架构正从单点技术突破转向“模型-工具-生态”协同进化升级。未来竞争将聚焦于场景深耕聚焦医疗、金融等高壁垒领域，通过专业化数据闭环构建竞争力；企业竞争核心从技术领先转向“场景理解+生态协同”，需在通用底层使能者与垂直场景整合者间做出战略选择、开放生态的开发者粘性

AI Agent产业技术架构



AI Agent产业技术演进趋势

实时感知与自主决策升级

随着大模型能力提升和硬件水平进化，从“指令-响应”转向主动规划

多链与跨模态融合

D.A.T.A框架解决跨链数据交互，多模态模型（如Gemini 2.0）增强环境感知

社区共创

LangChain等框架降低开发门槛，开源社区（如Hugging Face）推动工具生态扩展

AI Agent领域成为实现AI价值的重要赛场，不同类型企业各显身手

AI Agent产业图谱

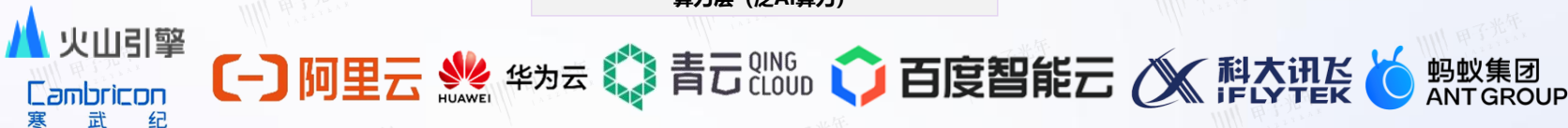
行业应用层



平台框架层



算力层 (泛AI算力)



注：生态格局图时间截止2025年2月底，由于版面所限，仅通过部分示例企业展示行业应用生态特点。

国内重点厂商及产品服务——中科视语

视语坤川智能体应用平台，面向行业提供全方位的智能体生态链服务

中科视语（北京）科技有限公司，**是中国科学院自动化研究所项目孵化企业**。成立于2018年4月，作为通用视觉大模型领域国家队企业，国家级专精特新“小巨人”企业，**自研技术勇立国际前沿，致力于引领通用视觉大模型技术**。公司成立以来历经工业、交通等数十个国家级重大项目的检验，核心标杆成果多次荣获顶级智库典型应用案例。



中科视语
object eye

依托大模型赋能行业智能进化，构建知识驱动，多维协同的智能体平台，助力业务精准决策与高效创新

视语坤川智能体应用平台通过融合外部工具、知识工程与中科视语行业小模型的深厚积淀，构建贯通感知、规划、决策、执行与记忆的智能闭环，快速打造面向行业特定场景的高阶智能体，为用户提供前沿的大模型决策引擎与执行赋能

行业智能体：能理解、会思考、懂规划、做决策、去执行

机车外观设计智能体
政务智能问答智能体

对话式数据分析智能体
交通隐患分析智能体

能源安全生产智能体
建筑专家对话智能体

基于逻辑推理的语言理解，精准处理复杂任务；先验知识引导的视觉模型，高效适应多场景；混合专家机制统一多任务，展现卓越跨领域智能协同

融合多模态数据，运用深度语义分析、视觉引擎与跨模态关联技术，精准提取信息并智能决策，适配复杂场景，实现高效认知与协作

中科视语坤川通用视觉大模型、DeepseekV3、R1等模型全搭载，为企业打造专属定制模型，快速调优，精准适配业务需求

多模态内容生成

多模态内容理解

模型全家桶

视语坤川智能体
应用平台

智能助手

工作流编排

智能分析

结合LLM+RAG技术和Agent的长短期记忆功能，能够高效利用私域知识，深入理解用户意图，提供精准回应，显著降低大模型的幻觉问题，确保AI应用的准确性与可靠性

内置强大的工作流引擎和丰富的工具插件，用户通过拖拽组件，灵活编排工作流，轻松应对复杂业务场景，提升开发效率

实现自然语言对话即分析，通过日常对话的方式即可获得可信的数据，极大降低数据消费门槛，引领数据分析新范式

感知推理能力

用户意图理解
多模态信息融合感知与推理

规划决策能力

需求和任务拆解
执行流程规划

自主学习反思能力

自主问题反思
自我学习技能提升

长短期记忆能力

实时对话记忆
长期历史行为记忆

交互式信息挖掘能力

交互式意图引导
多轮引导信息挖掘

工作流场景适配能力

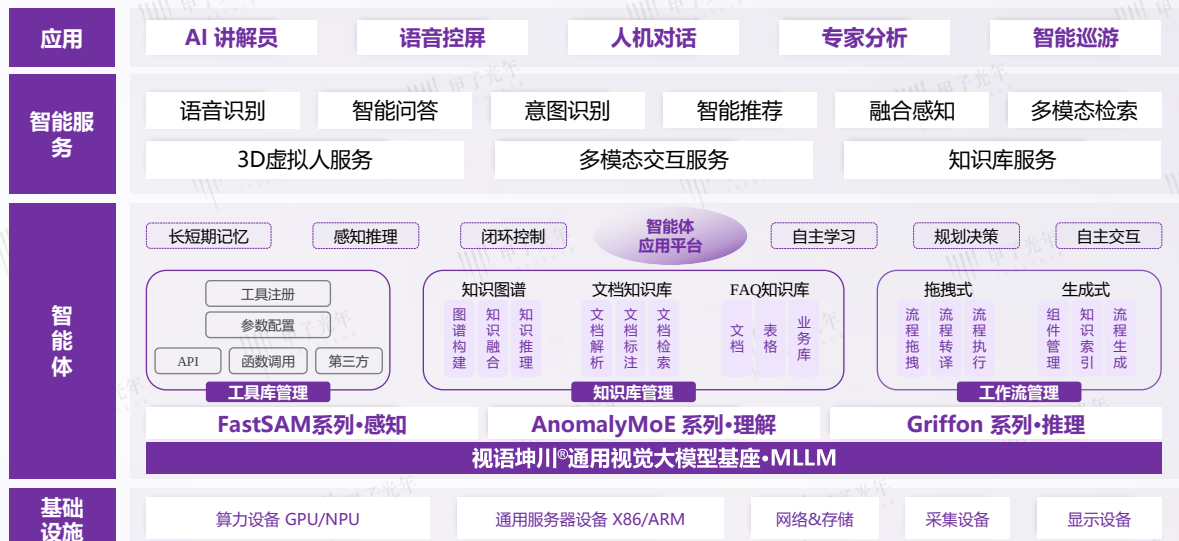
工具与函数调用完成任务执行
任务执行反馈闭环

中科视语：智能网联云控平台，重塑交通管理新格局

中科视语智能网联云控平台融合视语坤川通用视觉大模型、数字人交互、C-V2X通信等技术，构建新一代智能化智慧交通体系。平台以车辆、道路、环境的动态数据为核心，结合多源感知，实现协同感知、决策、控制，推动车路协同管控与智能调度。视语坤川通用视觉大模型提供精准环境感知与目标识别，提升智能驾驶与交通监管能力；数字人基于多模态交互，赋能远程管控、智能指挥与辅助决策。平台支持设备远程管理、车辆监测、网联信息发布、高精地图、数据分析共享等功能，实现信息融合、智能调度、精准发布，助力智慧交通高效、安全发展。



中科视语
Object Eye



语音对话
数字人讲解及智能



势分析
交通事件播报及趋



车指引
智慧停车及自主泊

项目成果

建设成效

- 通过智能化的信息交互与协同控制提效交通协同管控，降低交通事故发生率、优化交通流，减少拥堵，提高行车效率
- 智能虚拟助手提供直观、生动的交通信息展示，通过智能化的数据分析，为交通管理提供决策支持，提升响应速度和决策效率

项目亮点

- 新型协同控制：**基于智能体，融合融合AI、车路协同、语音识别与合成等多领域先进技术，实现针对垂类场景的新型AI+高效协同控制
- 人机交互新体验：**打造高度智能化虚拟助手，提供接近真人交流的互动控制，提高用户交互体验，提效业务处理流程

技术亮点

- 智能体技术：**深度融合多模态语音识别与意图分析，打造个性化且上下文敏感的交互环境，实现平台级高效协调控制
- 3D虚拟人技术：**结合高逼真度渲染和自然语言处理技术，实现栩栩如生的3D虚拟人形象和智能对话

国内重点厂商及产品服务 —— BetterYeah AI

专注提供企业级AI Agent平台，助力实现AGI for Organization

- 斑头雁（杭州）智能科技有限公司，是国内企业级AI Agent智能体头部厂商，致力于为企业提供AI Workforce
- BetterYeah AI 专注企业场景，打造专业的生产级AI Agent开发平台，并围绕企业客服、销售、营销、产研等场景，提供丰富的AI Agent应用，保障企业AI战略迅速落地。已服务联想、百丽、追觅、添可、啄木鸟等数百家头部企业，已落地的企业AI场景丰富深入、价值明显，团队具备丰富的落地经验和行业know-how



核心产品：国内最早发布、领先的企业生产级AI Agent开发平台

BetterYeah AI Agent开发平台

- 行业领先**：国内最早发布的企业级AI Agent开发平台，具备行业先发优势
- 专业高效**：平台功能丰富，提供从Agent建设到管理的一体化基础设施
- 市场认可**：平台每月数千万次任务调用，市场认可度极高



AI Agent应用&模版市场

- 实践丰富**：国内落地场景最多的企业级Agent模版市场之一
- 场景赋能**：来源客服、销售、营销等真实场景，快速复用
- 简单易用**：支持开箱即用，或基于模版快速打造个性化应用，迅速实现AI价值闭环

技术实力：聚焦企业AI场景，引领技术创新

易用

- 多角色协同**：满足技术、产品、业务多角色在平台上顺畅协同
- 行业模版**：丰富的企业级Agent模版，全部基于真实场景，快速复用
- 自动化构建**：Agent Copilot，辅助的Code生成工具，库表AI字段补齐备注
- 清晰直观的Flow Editor**，结构化和图形化的Prompt Editor，降低学习成本

专业

- 专业构建工具**：首家同时支持GUI-Flow, Web Code IDE, Py/Node SDK多种开发构建方式
- AI APP DevOps**：针对AI应用开发设计的CI/CD，多套开发环境，版本管理，批量单元测试
- 多套RAG算法**，Self-RAG, Self-Planning能力，提高准确率

灵活

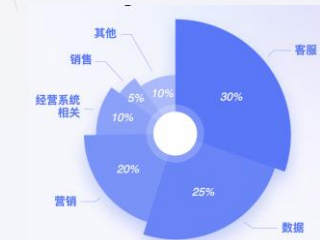
- 丰富的集成能力**：提供多端的集成能力，API和Chat SDK集成能力
- 支持多维数据同步**：非结构化数据，关系型数据，批量同步API
- 满足多种企业AI任务**：定时任务处理，批任务处理，Webhook任务

高性能

- 高并发**：支持上万QPS访问，每两周进行大容量并发压测
- 稳定性**：基于模型节点和区域性能的负载均衡算法，保证模型稳定性和响应速度
- 可观测**：提供了丰富的监控和报表能力，实时评估AI应用稳定性，性能，和线上质量，包括监控业务指标达成率

实践丰富：深入企业经营系统并直接提供生产力

- 某时尚鞋服集团**：以BetterYeah平台为AI基础设施，构建货品、店铺、营销等800+ Agent，深入业务场景
- 某互联网平台**：打造物流、订单及服务场景等agent，单日任务调用量45万次
- 某家电头部品牌**：客服agent赋能公司内客服团队300+人，人力成本降低20%
- 某人才招聘公司**：400+招聘Agent，7*24小时实时运行，提效35%



企业基于BetterYeah平台搭建的agent场景

标杆客户



国内重点厂商及产品服务 —— BetterYeah AI

BetterYeah AI Agent平台作为百丽集团AI应用一体化基础设施，全面支撑企业核心复杂场景AI落地



AI Agent已深入复杂经营场景，实现价值闭环

AI 货品助手

围绕“货”这个企业生命线，贯穿订货、入库、铺货、辅料、抽样、库存等 22 个关键模块 250 余个节点，覆盖总部货品、地区货品、电商货品、加盟货品、门店、仓库、工厂质检中心、供应商，以AI助手推进相关业务执行，协助跨组织信息连接和流程自动化处理，极大提升货品流转效率及流程优化

店铺 AI 助手

聚焦在全国上万家最小经营单元店铺中的店长、店员等角色，以及上下游区域、品牌总部发生的店铺终端管理、陈列管理、渠道管理、营销管理、巡店管理等关键模块，350 余个节点，通过 AI 完成店铺相关的业务操作及运营管理

AI 内容生成助手

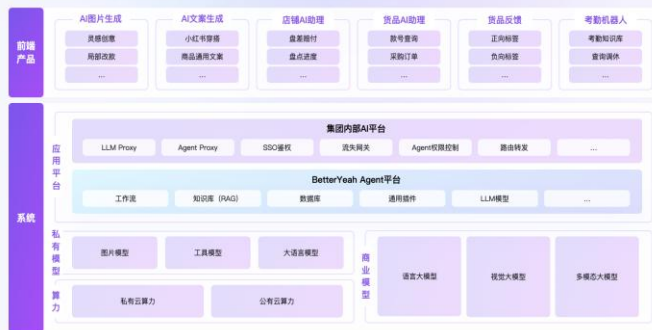
通过BetterYeah AI 知识库、flow 工作流的能力，将百丽旗下 20 余个品牌的全量 SKU 商品详情，当季潮流时尚、流行元素进行入库、AI 处理，并结合 LLM、多模态模型能力，原子化生成在小红书、抖音等9大平台的标题、tag、正文、脚本等内容，极大提升一线运营人员的效率

AI VOC助手

自动处理、洞察分析小红书等公域平台、淘宝天猫京东等电商平台的终端用户评论，辅助商品等迭代优化，以供给更加优质的商品，提升消费者体验

方案特色

- 迅速落地验证想法：** BetterYeah平台模块化功能+预置模版，帮助百丽2周内落地首个Agent货品反馈AI助手，低成本快速实现价值验证
- 加速解锁更多生产力场景：** 基于平台轻松搭建AI应用，百丽快速解锁营销文案生成、店铺AI助理等更多Agent场景，1年内规划800+ AI场景并逐步建设上线
- 企业级复杂场景开发环境：** BetterYeah平台提供多套开发环境、权限体系、安全能力，满足集团各类复杂开发协同诉求，降低集成开发成本
- 生产级稳定性保障：** BetterYeah AI平台覆盖AI应用生命周期，持续监控AI应用效果，保障线上质量，快速构建AI应用，响应集团各子业务需求变化



百丽时尚集团与BetterYeah合作，以BetterYeah AI Agent平台作为百丽集团AI平台基础设施，支撑百丽时尚集团近千人开发团队，实现AI应用高效开发和迅速落地实践。

开发团队从“VOC分析”和“内容生成助手”入手，逐步扩展到企业的核心业务——货品全生命周期管理，并为10000+门店不同角色提供服务的 AI 助手。

已迅速规划800+个AI场景并逐步上线，以AI应用推动跨组织信息连接和流程自动化处理。

- 企业级高扩展性：** 支持与ERP、CRM、OA等企业系统无缝集成，跨平台业务联动，满足集团多业务线协同及管理需求
- 生产级稳定性：** 聚焦企业级复杂场景，深入核心业务（货品流、店铺流等）直接提供AI生产力，满足集团10000+人、10000+次调用量
- 敏捷工程能力：** 模块化功能+预置模版，轻松构建各类个性化Agent，从场景规划到落地仅需2周，快速落地AI价值。
- 企业级开发环境：** 平台提供多套开发环境、权限体系、数据安全管控，充分满足集团的AI业务的复杂开发需求

以行业大模型驱动产业智能化，引领AI普惠新未来，提升全民健康福祉

- 卓世科技是一家国家级高新技术企业、国家级专精特新“小巨人”企业，于2018年底在北京成立。公司核心团队来自百度人工智能团队，兼具顶尖技术研发能力与成熟的AI产品商业化落地经验，公司一直秉持“AI-普惠”的理念，深耕“AltoB”赋能产业数智化，以自研AI大模型“璇玑玉衡”为核心，深度打造MaaS和Agent双引擎平台，全场景AI大模型覆盖医疗健康、政务企服、文教传媒和工业制造等领域，深度聚焦医疗健康行业大模型产品及应用，为客户提供人工智能综合解决方案



核心优势

全栈式行业大模型：“璇玑玉衡”大模型信创兼容



行业深度
定制化服务

商业化落地领先优势

参与项目

- 卓世科技联合**科技部、工信部**参与国家级科研攻关，与**清华大学精准医学研究院**等顶尖高校共建实验室，推动AI+医疗创新
- 携手**三大运营商、卫健委、浪潮、青岛软通、北京康养、新能源**等企业开发大模型、智能体、数字员工、智慧政务等解决方案，覆盖医疗、工业、政务、教育等领域，实现技术研发与商业落地的深度协同

产品体系



科研成果

- 累计申请发明专利102项，覆盖大模型架构（MoE）、模型微调（LoRA/QLoRA）、数据工程（RAG增强）等核心技术
- 登记软件著作权40项，涵盖医疗健康、工业制造等领域智能应用

获得奖项

- 自主研发MoE（混合专家）架构大模型，获AAMAS国际自主智能体竞赛冠军
- 国家级专精特新“小巨人”企业（2024年）
- 国家网信办大模型首批备案企业（2024年）
- 康养行业大模型标准牵头制定单位（2024年）
- 工信部“2024年度重点实验室大模型工作组优秀单位”

卓世科技部分产品

1. 璇玑玉衡大模型
 璇玑玉衡
FABIAN SUANJUYUHENG-20240221
2. MaaS+Agent双引擎平台
 - MaaS平台
 - Agent平台
3. 医疗健康解决方案
 - AI家庭医生
 - 北京市养老千亿大模型
4. 行业大模型及智能体
5. 一体机/智能硬件/数字人
 - AI人大屏一体机
 - DeepSeek软硬融合一体机



国内重点厂商及产品服务 —— 卓世科技

率先为各级医疗机构提供多模态通用医疗AI解决方案，助力医疗高质量高水平发展

- 卓世科技依托**璇玑玉衡大模型（MoE架构）**，融合多模态交互与知识图谱技术，为医疗、康养、工业、政务提供全场景AI解决方案；适配多家国产算力，其模型压缩技术可使模型推理成本下降68%；服务客户累计超1000家
- 医疗领域**AI家庭医生提升基层工作效率200%，覆盖北京、天津、深圳、福建、河南等省市；**康养行业**牵头制定行业标准；**政务、教育**等行业应用落地效果大大提升。获工信部“实验室大模型优秀单位”认证，入选《2024中国AI产业图谱》，树立AI赋能实体标杆



卓世科技全景产品体系，构筑全链路AI能力高地



创新点

- 卓世科技**璇玑玉衡大模型**基于**MoE混合专家架构**，适配国产算力（华为昇腾），推理效率提升30%-50%，模型体积压缩减少72%，支持低成本部署。通过RAG技术动态调用行业知识库（如中医药、工业参数），生成专业建议，检索准确率超95%。赋能医疗、工业、政务、教育等场景：AI家庭医生提升基层工作效率200%，工业大模型数字顾问优化生产30%，政务智能问答集成2000+政策。牵头制定《康养行业大模型标准》，服务累计超1000家企业，成为AI普惠化标杆

卓世科技“AI家庭医生”智能体



创新点

- 卓世科技AI家庭医生系统基于**璇玑玉衡大模型（MoE架构）**，支持多模态交互（语音/文本/图像），响应<800ms，问答准确率>95%，模型体积压缩68%，适配国产算力。覆盖健康咨询至慢病管理全流程，效率提升40%；赋能基层医疗，签约率提升30%，响应提速200%。集成跨学科虚拟团队，动态更新权威知识库，提供政策咨询、健康宣教、智能问答、用药指导、家医签约、慢病随访等一站式健康管理服务。支持方言与适老化设计，计划2025年覆盖全国4000+基层机构，牵头制定《康养行业大模型标准》，成为AI+医疗标杆

Part 01

AI Agent的全球认知与发展演进

Part 02

AI Agent的技术突破与行业重构

Part 03

AI Agent的商业实践与场景突破

Part 04

AI Agent的未来趋势与挑战

目录

CONTENTS

算法演进：与行业Know-how深度结合，从通用模型到行业专属模型

基于模型实现从通用智能到行业专属AI Agent的跃迁，加速场景应用

算法专业化演进路径

领域知识深度集成

- 行业专属Agent架构 = 基础大模型 + 领域规则引擎 + 私有知识库
- 知识注入范式演进：静态规则库 → 动态知识图谱 → 自演进知识网络
- 典型应用价值：关键业务场景决策自动化率明显提升

垂直领域模型架构

- 分层决策架构：通用语义理解层 → 行业逻辑推理层 → 企业定制适配层
- 多模态行业适配模块：跨文本/图像/时序数据的领域特征提取器



边缘化部署技术突破

轻量化技术矩阵

- 模型压缩黄金三角：参数量减少+，推理速度明显提升，内存占用明显降低
- 混合精度量化 + 自适应计算框架 = 边缘设备响应延迟优化至毫秒级

动态优化体系

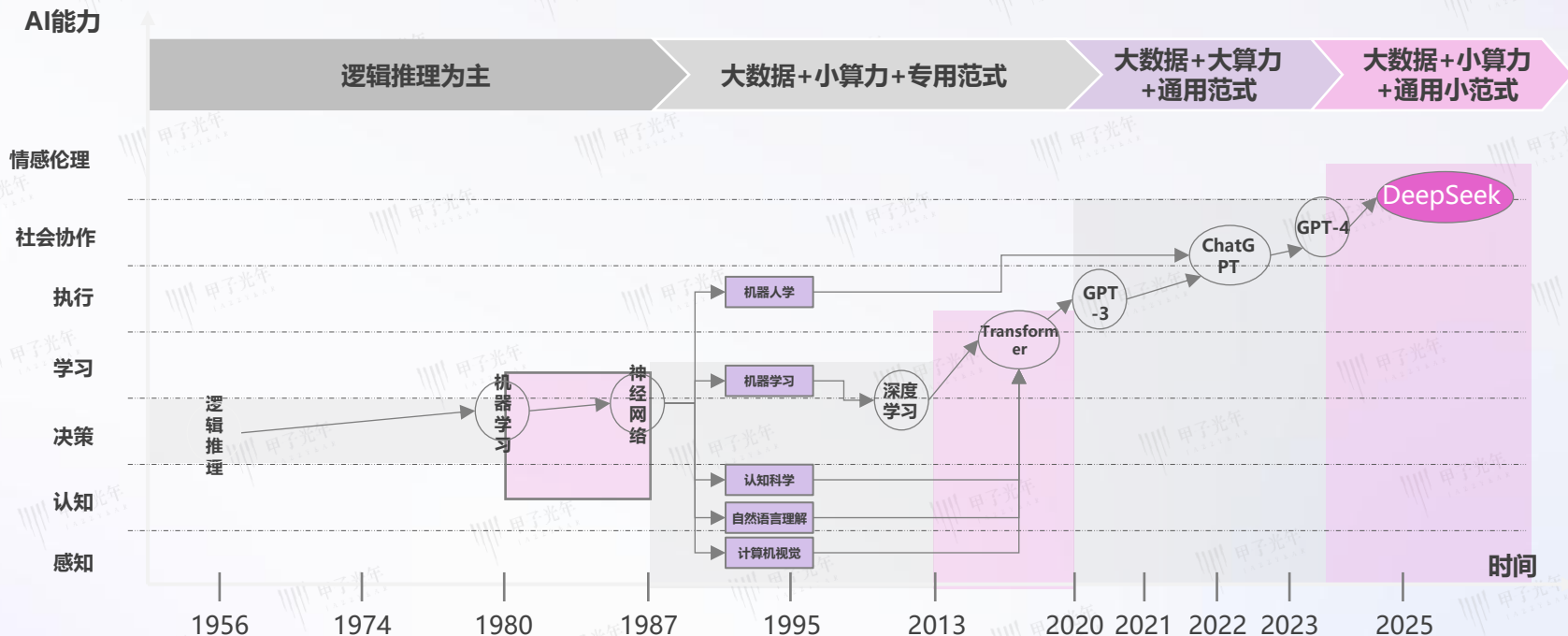
- 联邦学习支持设备端模型持续迭代，周更新率占比大幅提高
- 边缘缓存 + 增量学习实现低带宽环境下的模型热更新

AI Agent成为新一轮产业变革的核心驱动，将推动从垂直领域单一环节到跨行业跨领域全生命周期的智能化升级。

AI Agent的未来探索：小模型、低能耗、跨场景、多模态

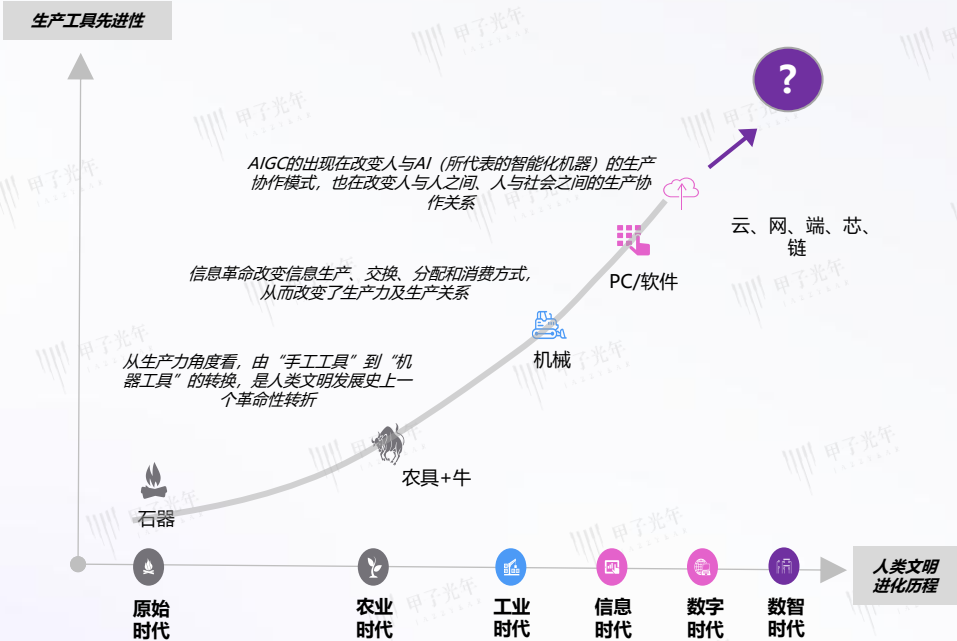
基于大数据+小算力+通用小范式大模型的AI Agent成为趋势

AI能力的进化路线



从集中式智能到泛在化智能的架构革命，重构AI Agent技术及产业体系

- 2025年技术拐点将聚焦混合训练框架实现云边协同进化，神经符号系统突破终端因果推理瓶颈。未来三年，构建弹性算力网络推动AI Agent服务从"中心辐射"向"毛细血管渗透"转型，通过云-边-端动态协同实现隐私安全、实时响应、全局优化的智能升维



AI Agent的算力分布正在重构智能体系

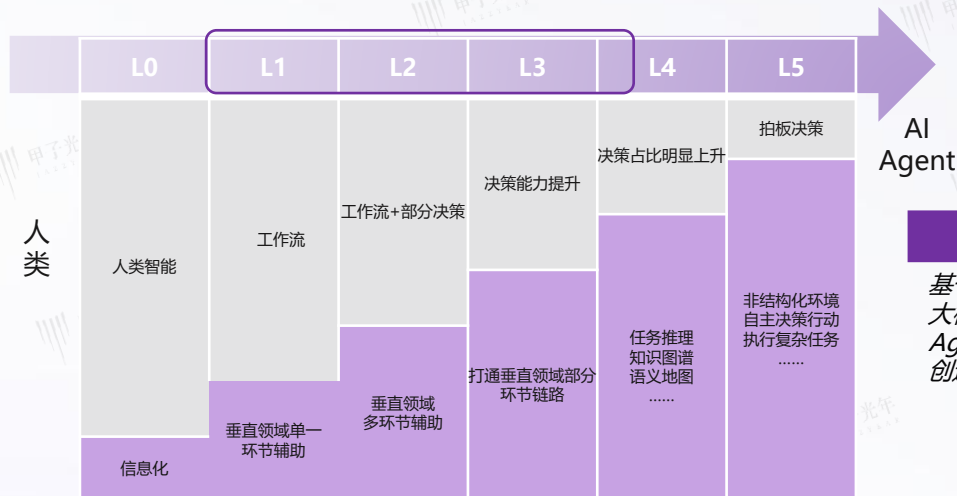
云端	高性能智能中枢	支撑千亿参数级模型的分布式训练与推理	混合专家系统（MoE）、多模态融合框架
边缘	实时响应中枢	实现毫秒级决策	动态模型切片、增量学习与边缘联邦学习
终端	隐私敏感型智能触手	本地化推理	混合精度量化、设备自适应计算框架

- 云边端协同架构：通过任务分级与资源动态调配，实现从集中式智能到泛在化服务的跃迁
- 隐私与效能平衡：终端本地化推理解决数据主权问题，边缘实时计算突破响应瓶颈，云端持续进化全局智能

社会影响：价值由人和AI Agent共同创造

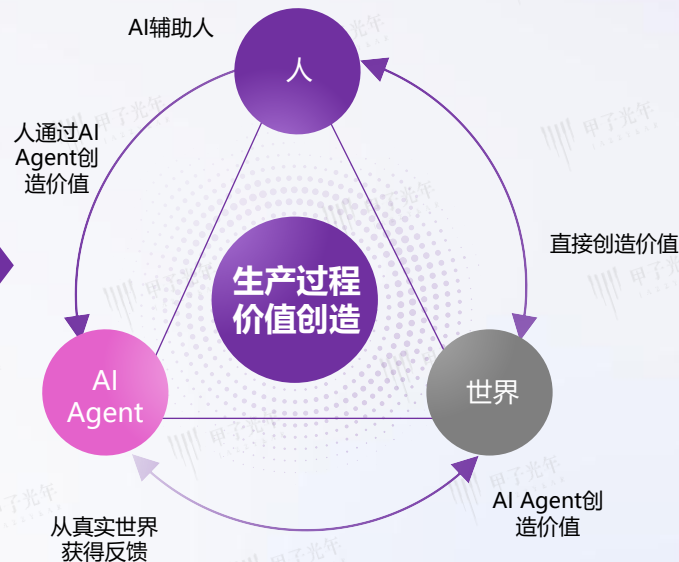
- 随着AI Agent技术能力升级，AI Agent从“辅助”到“自主”的定位与角色转变，逐步实现由边缘支持向任务主导的层级跃迁

从L0到L5，AI Agent的自主性随智能化程度持续发展



基于高水平大模型的AI Agent同人类创造价值

生产过程的价值由人和AI Agent共同创造



AI Agent的发展在技术、应用和治理/伦理方面面临的挑战

技术

算力基础设施瓶颈

- **计算资源不足**：大模型训练与推理需求激增
- **边缘端部署限制**：终端设备算力有限
- **能耗矛盾**：轻量化技术降低单任务能耗30%，但全局算力需求增速达50%/年，形成“能效陷阱”

数据获取与处理难题

- **高质量数据稀缺**：医疗、金融等敏感数据因隐私限制难以获取并应用
- **多模态数据融合损耗**：数据转换时易丢失细节，影响决策准确性
- **动态知识更新滞后**：模型知识库更新周期长，无法适应实时场景需求

应用

跨场景协作能力不足

- **工具链封闭性**：现阶段更多是工作流，无法灵活整合自主决策
- **数字-物理环境割裂**：大模型在真实物理场景中训练成本高，导致AI Agent工业与医疗等领域的落地

可解释性与用户信任危机

- **黑箱决策机制**：大模型内部逻辑不透明，用户难以理解AI决策依据，导致对基于大模型的AI Agent信任缺失
- **幻觉与误判风险**：AI Agent在开放场景下，可能输出错误信息和决策，需建立实时纠错与人工复核机制

伦理 & 治理

责任归属与合规风险

- **自主性带来的法律空白**：AI Agent高度自主的决策难以追溯责任主体（开发者/用户/算法等）
- **监管框架滞后**：现有法规（如欧盟《AI法案》）尚未覆盖多Agent协同、去中心化决策等复杂场景

伦理与社会公平失衡

- **算法偏见固化**：训练数据中的隐性偏差（如性别、种族歧视）可能被放大，加剧社会不公
- **技能鸿沟扩大**：AI自动化替代低技能岗位速度远超职业培训体系适应能力，可能引发结构性失业