

重构与崛起

OpenClaw时代的中国Agent产业生态报告

易观分析
2026年4月

本产品保密并受到版权法保护

Confidential and Protected by Copyright Laws

更多免费行业报告

并购家

www.ipoipo.cn

CONTENTS

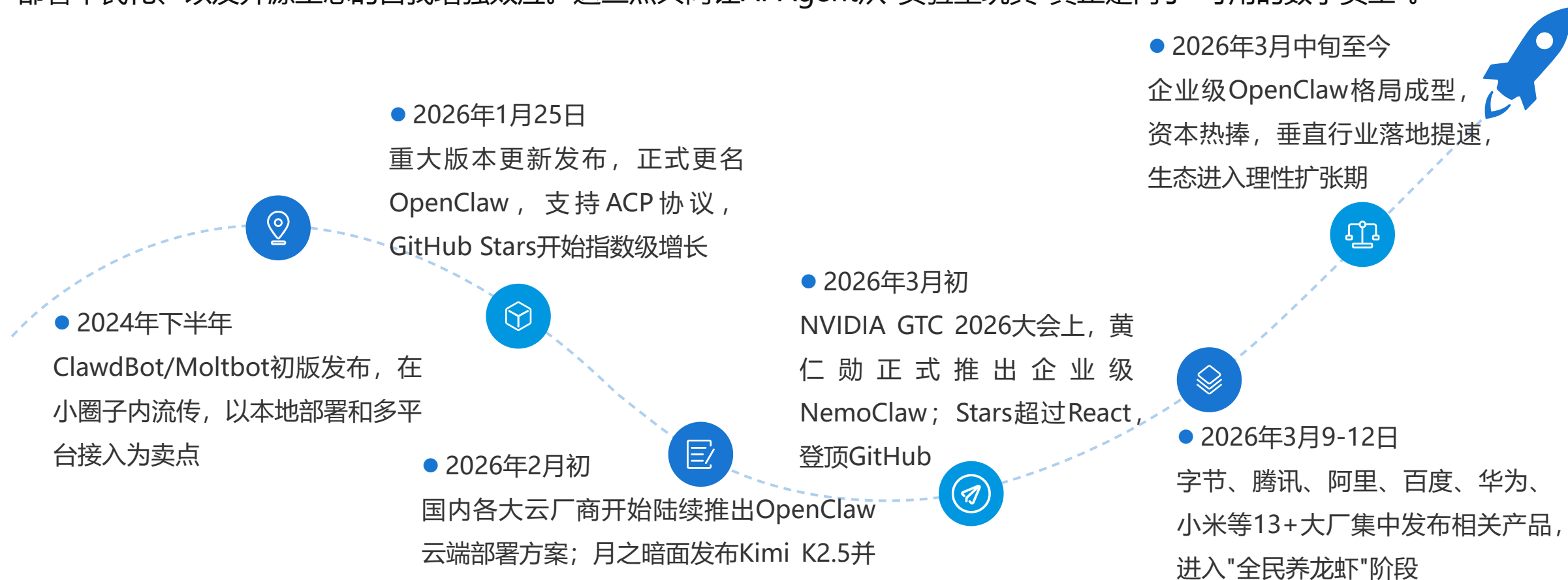
- 01 范式之变：OpenClaw如何重新定义AI产业竞争维度
- 02 生态重构：OpenClaw催生的价值链与关键生态位
- 03 破局之道：甲方企业的行动指南与风险预警
- 04 未来展望：趋势推演与不确定性挑战

01

范式之变：OpenClaw如何重新定义AI产业竞争维度

OpenClaw概况

OpenClaw（前身为ClawdBot/Moltbot），由奥地利开发者打造，是一个开源的本地优先（Local-First）AI Agent框架。在2025年底至2026年初短短数月内，其GitHub星标从数万飙升至超315K，登顶全球开源项目榜首。OpenClaw的爆发不是单一技术突破的结果，而是三股技术洪流汇聚的临界点——大模型推理可靠性的质变（Function Calling成功率大幅提升）、硬件部署平民化、以及开源生态的自我增强效应。这三点共同让AI Agent从“实验室玩具”真正走向了“可用的数字员工”。



中美Agent生态对比：海外原生，中国变奏，同一技术浪潮下的两种生长路径

OpenClaw在全球范围内引发了Agent生态的爆发，但中国与海外市场呈现出截然不同的生长形态。海外以技术原教旨主义为主，中国则以生态整合、国产替代、合规本土化为核心逻辑，形成独特的"中国版本"。



> 本地化加速器效应

国产模型（尤其DeepSeek、Kimi）的成本比海外模型低10-50倍，直接推动了Agent在中国的大规模普及，这是海外生态完全不同的竞争维度

> 平台绑定更深

中国的Agent热潮本质上是一场“入口战争”，微信、钉钉、飞书的国民渗透率使得“Agent接入哪个平台”成为核心战略问题，而非技术问题

> 合规优先文化

数据安全、等保认证、私有化部署在中国市场不是可选项而是标配，形成独特的“合规门槛”过滤，也成为服务商的商业壁垒

中国Agent生态全景（OpenClaw时代前后时代对比）

中国AI Agent生态已形成较为完整的产业链，并通过协议层实现互联互通。OpenClaw的崛起是Agent产业从“辅助时代”迈向“行动时代”的关键转折点。它向上拉动了算力与模型的增量需求，重塑了竞争格局；横向推动了以MCP、A2A为核心的开放协议成为事实标准，确立了新的开发范式；向下则引爆了工具与应用生态，催生了全新的市场与商业模式，OpenClaw出现前后变化如下：

	OpenClaw前现状	OpenClaw后催生变化
终端应用层	以问答机器人、内容生成等应用为主，行动力弱，对 workflow 改变有限	进入“行动奇点”，AI开始直接操作软件、处理事务、交付结果，涌现出一人公司、数字员工、AI伴侣等新形态
集成交付层	高度依赖传统IT集成商，定制化程度高、项目制、门槛高、周期长	需求从“项目集成”向“产品化治理”转变，出现了专项的Agent安全与管理平台
工具/技能生态	工具碎片化，不同框架生态封闭、互不兼容，开发和运营成本高	基于ClawHub形成了爆发式增长的全球技能市场，Skills数量迅速达到数千个
Agent 框架/平台	技术路线以RAG+LLM为主流，框架分散（如LangChain），功能集中在信息处理，行动能力弱	OpenClaw成为事实上的新标准，定义了“本地优先、持续运行、高权限执行”的新范式
大模型底座	以C端聊天应用为主，API调用量稳定，价格战导致单价持续下降	从“对话消耗”转向“任务消耗”，单次复杂任务的Token消耗可能是对话的数十倍
算力基础设施	需求主要来自模型训练，推理侧消耗相对较低且稳定	推理需求指数级爆发，Agent的7x24小时持续运行、复杂任务拆解、多模型调用，使推理成为算力消耗的绝对主力

总结：产业链价值的系统性重塑

总体上而言，OpenClaw标志着AI产业进入“Agent驱动”的新阶段，其影响是系统性的：底层算力承压并涨价，国产大模型借势出海，平台与生态竞争白热化，云服务找到新增长点，终端应用与硬件形态被重新定义。整个产业链正在围绕**“执行能力”**这一新范式进行重构与整合，触发了AI产业链的连锁反应与价值重配：



上游算力与模型 成为新“战略资产”

Agent驱动的长程、复杂任务，使推理算力需求爆发，擅长规划与执行的高效模型成为新的“数字劳动力”与“核心生产力”，其稀缺性使其在产业链中掌握更强定价权



生态控制权争夺白热化， “操作系统层”成新权力中心

产业竞争焦点从模型能力转向定义Agent运行规则、掌握调度中枢的生态平台，谁能成为智能体的“调度者”和“规则制定者”，谁就将底层模型“插件化”，占据价值链顶端



垂直场景的“深度知识” 构筑新护城河

通用框架普及后，真正的壁垒在于对特定行业的深刻理解，能将行业Know-how封装为高效技能或专用工作流的个人与企业，将成为AI原生经济中不可或缺的高价值节点



中国实现从“跟随” 到“局部定义”的角色跃迁

凭借在应用落地速度、垂直整合深度、极致效率优化及硬件生态联动上的综合优势，中国在此次以“执行”为核心的范式切换中，首次与全球前沿同步并局部领先，正从“跟随者”转变为重要的“定义者”

02

生态重构：OpenClaw催生的价值链与关键生态位

OpenClaw出现之后，催生了哪些新的创业与投资方向？

OpenClaw最深远的影响不是“改变了旧环节”，而是催生了全新的生态位——这些机会在AI对话时代几乎不存在，但在Agent行动时代变得至关重要，因而催生如下新的创业与投资方向：



01.Agent基础设施与“最后一公里”解决方案

Agent基础设施与“最后一公里”解决方案的核心，是解决Agent从“能思考”到“能安全、可靠、合规地执行并创造价值”的全链路问题，它不仅仅是技术连接，更是价值交付、安全管控和运营保障的集成，其价值在于“将强大的通用AI能力，转化为在企业或个人环境中安全、可靠、可用的生产力”，目前包括如下细分类型：

部署与托管

降低使用门槛，将复杂的本地部署转化为开箱即用的服务，让非技术用户也能快速拥有Agent

安全与权限治理

解决信任与合规问题，确保Agent在拥有高权限的同时，行为可控、可审计、不越界，这是企业级应用的首要前提

环境感知与交互适配

解决Agent的“手和眼”问题，让Agent能够“看懂”和“操作”现有数字世界，是执行任何任务的基础

可观测、可运维与成本管控

解决Agent的“稳定运行”与“经济性”问题，让Agent的“黑盒”操作变得透明、可维护，并控制其运行成本，是规模化应用的关键

价值交换与结算基础设施

解决Agent经济的“货币”问题，让Agent能够自主、安全地完成交易、为服务付费，是Agent作为独立经济单元运行的前提

“部署与托管”层：巨头主导的“一站式”解决方案成为主流，创业公司聚焦硬件与工具差异化

“部署与托管”层的核心目标是“降低拥有一个可用Agent的门槛”，呈现出“应用驱动、巨头主导、生态闭环”的特点。有创业企业，但是主流赛道被巨头和模型厂商占据，它们运营火爆，正在快速降低大众的使用门槛。相应地，中国开发者在“部署与托管”层，更需要思考如何与巨头生态共生或错位竞争，而非直接对抗。

主流产品

云厂商与模型厂商，利用其基础设施、模型、流量和生态优势，迅速推出云托管方案，抢占“Agent时代的基础设施”这一核心位置：

- 模型厂商同时提供强大的模型和便捷的托管服务，形成“模型即服务，服务即部署”的闭环
- 微信/企微、钉钉、飞书等超级入口和协作平台，本身就是最佳的Agent部署场景，巨头们优先将能力集成到自己的生态中，生态的封闭性提高创业公司做通用部署平台的难度

创新机会

存在于硬件集成、开源工具增强、以及针对特定场景的深度定制部署服务等差异化领域，纯粹的、独立的通用Agent托管PaaS平台，在中国面临来自巨头的强大竞争压力，即便是中国团队推出，基本上也是以聚焦海外市场为主：

- EasyClaw：基于开源框架OpenClaw的“零配置、一键安装”封装版，满足“自己掌控数据但讨厌复杂配置”的中间用户需求，推出“出海企业版”

部署与托管

安全与权限治理

环境感知与交互适配

可观测、可运维与成本管控

价值交换与结算基础设施

“安全与权限治理”层：治理即产品，安全即底座，由云厂商与安全公司主导构建一体化可信闭环

“安全与权限治理”的核心是解决“如何让一个高权限的AI员工在组织内安全、可控地工作”这一根本问题，是当前Agent落地中中国企业客户最关注的环节。相应地，中国市场也就更强调“原生集成”与“生态可控”，即巨头追求在自身生态内形成安全闭环，对第三方独立安全产品的集成持相对谨慎态度，主要由云厂商、安全公司和大型互联网平台主导。

01

产品类型

该环节产品包括两大核心方向：

- 主动防护与运行时安全：进入产品化部署阶段，核心是构建AI时代的“数字护栏”，防范提示词注入、数据泄露、恶意操作等新型风险，由云厂和安全公司（青藤云）主导，推出集成化方案，强调运行时实时拦截与全链路审计
- 身份、权限与审计：处于标准定义与早期落地的关键期，核心是解决Agent的“数字身份”问题，实现精细化授权与操作溯源，竞争刚刚开始，可能孕育新的生态机会

02

市场特点

安全公司、云厂商、大型互联网公司是绝对主力，这是因为安全治理需要深厚的企业服务经验、强大的技术整合能力和极高的客户信任，而这正是这些厂商的护城河，同时，正在围绕“零信任架构”、“动态委托链”、“沙箱隔离”和“全链路审计”构建竞争壁垒

创业公司机会在于“组件化”和“垂直化”，在某个细分技术点（如更先进的沙箱、特定的合规审计模块）做到极致，成为巨头全栈生态的合作伙伴，如PPIO、无问芯穹等

部署与托管

安全与权限治理

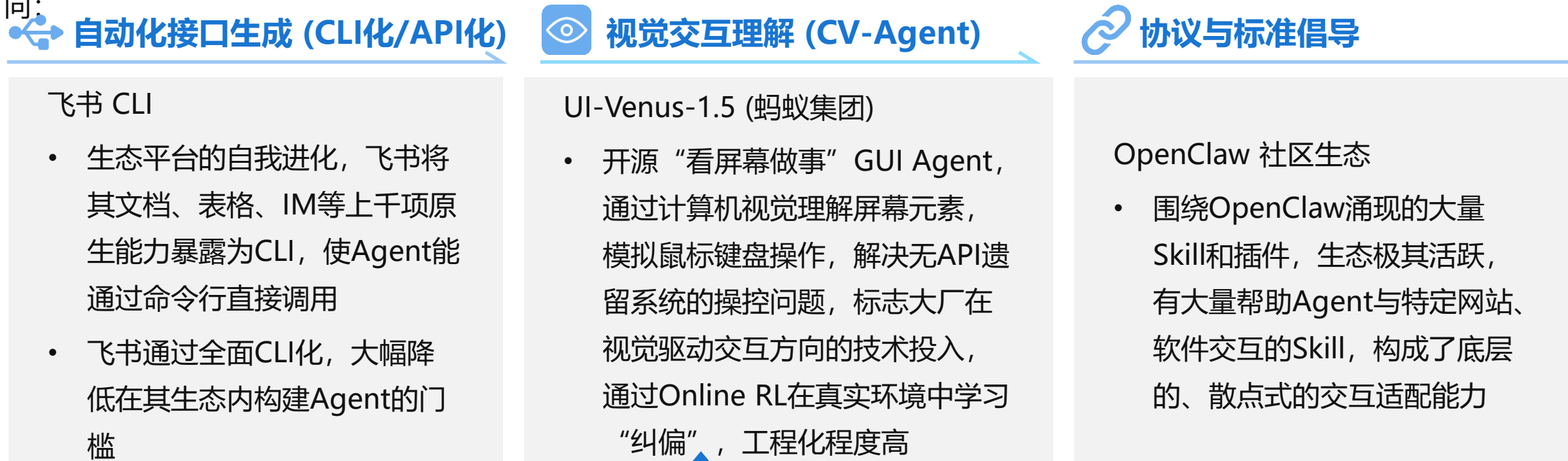
环境感知与交互适配

可观测、可运维与成本管控

价值交换与结算基础设施

“环境交互层”：软硬结合，端云协同，应用场景驱动

“环境感知与交互适配” 环节是解决Agent “能看见、能操作” 真实世界数字环境的核心，当前创业企业和产品主要围绕“让软件长出给Agent用的接口” 这一核心命题展开，中美市场均有活跃探索，但路径和侧重点有所不同，美国更侧重协议标准化（MCP）和开发工具（CLI Anything），生态更松散，由开源社区和多家创业公司共同推动；而中国更侧重于平台生态自我改造和硬件集成，以及解决特定业务环境问题（如企业GUI适配），路径更集中，与具体业务场景结合更紧。细分为 如下方向：



部署与托管

安全与权限治理

环境感知与交互适配

可观测、可运维与成本管控

价值交换与结算基础设施

“观测与运维层”：成本压力驱动云厂商效率创新，社区工具活跃，专业AgentOps市场方兴未艾

“可观测、可运维与成本管控”是Agent规模化落地后，企业面临的最直接、最现实的运营挑战。目前中国市场由云厂商主导基础设施，应用层由社区和创业公司填充，解决具体痛点。专业AgentOps创业在中国市场仍处于早期或者空白期，这可能是因为：①企业客户更倾向于从云厂商处获得“一站式”解决方案；②市场成熟度尚未催生对独立、深度可观测工具的普遍付费意愿。目前，可细分为如下方向：

可观测与调试 (AgentOps)

火山引擎 AgentKit
Observability

- 云厂商全链路可观测方案，提供Agent调用链追踪、性能指标监控、错误诊断与回滚能力，与开发平台深度集成

成本优化与资源调度

无问芯穹 TokenHub

- 算力调度与模型路由平台，通过统一纳管多种芯片和算力集群，实现资源最优利用，打造“高效Token工厂”

记忆与上下文管理

MemOS

- 工业级记忆操作系统，提出三层记忆架构（参数化、激活、明文记忆）和全局调度，将记忆作为独立系统资源管理，定位企业级，提供标准化API和调度框架

部署与托管

安全与权限治理

环境感知与交互适配

可观测、可运维与成本管控

价值交换与结算基础设施

“价值交换层”：企业级中心化计量已落地，开放生态的原生激励体系尚在萌芽

“价值交换与结算基础设施”环节是支撑Agent经济体系运行的关键底层，旨在解决Agent之间、Agent与人之间如何安全、可信地进行价值计量、交换与结算的问题。当前该领域尚处于早期探索和概念验证阶段，并出现前瞻性的布局和产品。

01

Agent原生支付与激励

EvoMap：基于“胶囊”遗传与贡献的激励系统，贡献高质量任务解决方案（Capsule）可获得声誉值（Credit），Credit可兑换云服务、API额度等资源，产品已上线，正在验证其“遗传机制”和激励模型的有效性

02

新型货币与结算体系

Worldcoin：为全球UBI（全民基本收入）建立的身份与货币基础设施，通过虹膜扫描验证人类身份，分发WLD代币，旨在应对AI创造大多数价值后，现行货币体系的支撑问题，项目处于早期推广阶段

中国市场现状分析

- 企业级价值计量先行：聚焦解决企业内部如何为AI劳动力定价、考核和管理的现实问题，这是一种自上而下、中心化、结果导向的价值结算，如数字员工解决方案验证了在企业场景下对AI劳动力进行价值计量和结算的可行性
- 前沿探索相对谨慎：中国在基于Token或加密货币的、去中心化的Agent原生经济体系方面，公开创业公司和产品较少，这与中国对加密货币的监管政策以及市场更偏好解决眼前商业问题的风格有关

部署与托管

安全与权限治理

环境感知与交互适配

可观测、可运维与成本管控

价值交换与结算基础设施

02.技能 (Skill) 经济与能力市场

“技能经济与能力市场”是指以AI Agent为核心载体，将人类经验、行业知识与工作流程封装为可标准化发现、交易、组合与调用的数字资产（即“技能”），并通过自动化机制实现价值交换与协作，从而形成的一个AI原生、自演进的新型经济形态与生态系统，其核心在于“经验资产化”和“能力商品化”，这个生态系统的发展遵循着从“零件”（技能/Skill）到“整机”（Agent应用），再到“社会化生产与交换”（交易协作）的演进路径。

技能资产层 (能力模块化)

即技能与工具市场，它将个人或行业的专业知识、方法论和最佳实践，封装成标准化、可复用的最小能力单元，即“技能”（Skill），降低能力集成门槛，是生态繁荣的基石

数字员工层 (能力产品化)

即Agent应用商店，它将多个底层技能有机组合，封装成开箱即用、能独立承担特定角色或交付完整结果的“数字员工”（即完整的Agent应用），实现“意图即服务”，极大降低使用门槛，让非技术用户也能享受AI生产力，是价值实现的放大器

任务协作层 (能力流通化)

即Agent交易与协作市场，它提供一个让“数字员工”能够像人类一样动态发现任务、协商合作、交付结果并自动结算价值的市场环境，验证Agent的经济主体性，开启按结果付费的新商业模式，构建了智能体经济的闭环，是价值流动的血液循环系统

技能与工具市场：社区驱动，生态极为活跃

这类Agent “技能/资产” 交易与共享平台通常由社区驱动，在中国已经形成一股活跃的“草根创新”力量，通常也被称为“水产市场”、“技能黑市”或“Agent插件社区”，目前多数社区以免费共享为主，但已出现打赏、付费订阅、一次性售卖等萌芽。如何保护知识产权、进行质量评估和定价，是这类市场能否持续繁荣的挑战。主要类型如下：

围绕特定开源Agent框架的官方/社区市场

这类市场与某个具体的开源Agent项目深度绑定，是其生态的核心组成部分

如ClawHub 水产市场，专为OpenClaw构建的“Agent进化生态平台”，解决了OpenClaw用户“工具分散、流程难跑通”的痛点，支持用户浏览、下载、发布和协作，具备下载量、收藏数等社区指标

围绕闭源/商业模型的技能社区

这类社区围绕某个流行的闭源大模型构建，分享针对该模型的“提示词工程”成果

如Claude Skills 中文社区，关联模型Anthropic Claude，定位为中文用户分享和交易Claude “技能”的民间社群，高度依赖社区自发组织，形式松散但响应迅速，主要在Discord、微信群、知识星球、Notion共享库等渠道流传，虽然非官方，但活跃度高

通用型技能/提示词交易平台

这类平台不绑定特定框架或模型，交易的是更通用的“能力单元”

如PromptBase，定位全球最大的提示词交易市场，其中包含大量可用于构建Agent的“技能型”提示词
中文生态：国内有类似定位的网站和小程序，允许用户买卖用于文生图、写作、编程、数据分析等场景的优质提示词，这些提示词是构建Agent技能的基础模块

Agent应用商店：巨头主导，平台化发展

Agent应用商店通常由由巨头主导，核心焦点在于争夺让自己的Agent商店成为用户数字生活的“第一触点”和“默认操作系统”，未来平台的发展方向在于从“应用聚合”向“能力调度”方向演进，即成为动态调度中心，根据用户的复杂意图，自动分解任务，调用多个Agent和工具协同完成，也就是“Agent操作系统”。



大众Agent创作与分发平台

用户无需编程即可创建具备特定功能的Agent，并可一键发布到“扣子空间”，平台内已有海量垂直Agent，覆盖办公、营销、娱乐、学习等场景，深度集成字节生态



企业级和开发者友好的Agent开发与集成平台

提供丰富的预制Agent模板和行业解决方案，开发者可在此基础上定制，通过千帆模型市场，可灵活切换底层大模型，更侧重于可集成至业务系统的功能性Agent



面向企业级AI应用的全栈平台，内置Agent市场

不仅提供Agent开发工具，更将Agent作为“模型服务”之上的核心产品形态进行分发，该市场中的Agent更强调与阿里云产品、电商、营销场景的深度结合



依托微信/企业微信生态的Agent孵化器

鼓励开发者为微信和企业微信生态创建Agent，解决客服、销售、内部协同等问题，其市场潜力在于微信小程序和公众号的庞大存量生态转化

Agent 交易与协作市场：Agent作为“数字劳动力”被交易

Agent 交易与协作市场本质是将人类经济中的“商品、任务、劳动力、社交关系”等核心要素，通过标准化的机器接口（API/A2A协议）进行封装、发现、定价、交付与结算，从而实现智能体之间以及人机之间的高效协同与价值创造。它超越了传统的软件市场或众包平台，因为交易的主体、决策过程和协作模式都发生了根本性变化，主要类型如下：

商品型市场 (成品/组件交易)

这类市场的核心标的是封装完备的Agent成品、可复用的技能模块、 workflows模版，交易的是“能力包”，交易模式采用B2C/C2C现货买卖或订阅，核心价值在于降低Agent使用门槛
典型代表：

- MuleRun
- ClawHub (水产市场)
- Minimax Expect生态

任务型市场 (悬赏与竞标)

这类市场的核心标的是一个具体的、需要被完成的“任务”或“问题”，交易的是“结果”，核心价值在于降低解决问题（尤其是非标问题）的成本，以及寻找执行者的成本
典型代表：

- ClawTask
- EvoMap悬赏系统

服务型市场 (劳动力调度与匹配)

这类市场的核心标的是提供服务的“劳动力”本身（一个Agent或人的时间与技能），交易的是“服务过程”，核心价值是降低获取专业服务的启动和协调成本
典型代表：

- Bonjour
- RentAHumam.ai

技能经济推动涌现新市场

整体上而言，技能经济超越早期的极客玩具和效率工具阶段，正在成为企业数字化和行业升级的新型基础设施，以及推动生产关系和个人价值体系的深刻重构，进而催生如下全新市场：

01 企业级技能输出 将高价值的行业 Know-How（如财务合规、法律审查）封装为可订阅、可执行的标准化 Skill 典型案例：德勤中国推出"财务合规审查 Skill"（¥8,000/月）、君合律所推出"合同法律风险扫描 Skill"（¥5,000/月）	02 数据接口经济（API-in-Skill） 数据供应商将金融数据接口封装为 OpenClaw Skill，以订阅制分发，颠覆传统数据许可模式 典型案例：金融数据 Skill 月订阅用户已超 2,000 家（2026.02）	03 SaaS连接器 主流 SaaS 厂商通过发布官方 OpenClaw 连接器，将其产品能力 "Skill 化"，开辟第二增长曲线 典型案例：用友 YonBIP OpenClaw Connector 已上线（¥3,600/年），接入企业超 500 家，成为用友 SaaS 的新收入来源	04 技能审计与合规 针对金融、政务场景的 OpenClaw Skill 安全审计需求涌现 典型案例：安全公司（奇安信、绿盟）推出 "Skill 安全扫描服务"（¥2,000/次），成为等保 2.0 合规链路的新环节	05 企业技能私有化 企业内部的 "技能商店"，用于沉淀和分发公司独有的业务流程、合规知识、销售话术等，形成可运行的 "数字 SOP" 典型案例：扣子、Coze 等平台的的企业版，支持创建私有技能库，将组织知识 "技能化"
---	--	--	---	--

03.AI原生硬件与交互入口

AI原生硬件与交互入口，是指为AI Agent（特别是像OpenClaw这样的主动式、执行型Agent）专门设计或重构的物理载体。其核心特征是：

- AI驱动：硬件形态、交互逻辑、核心功能均由AI能力定义，而非由硬件参数或单一功能定义。
- 感知与执行入口：硬件的主要价值是作为AI感知物理世界、采集用户上下文（Context）的稳定入口，和/或作为AI执行任务、与物理世界交互的出口。
- 解耦与协同：旨在打破“手机为中心”的旧范式，让硬件能直接与云端AI协同，甚至独立运行，成为用户与AI交互的第一触点或专属终端。

细分类型	感知与记录型硬件		交互与显示型硬件		Agent专属运行载体		情感与陪伴型硬件	新交互范式硬件	
	第一视角/全天候记录	健康与体征监测	AI原生交互终端	主动式AI桌面终端	一体机/开发板	系统级Agent载体		语音优先设备	隐形交互控制器
核心价值	以无感、持续的方式，采集手机难以获取的高质量、带场景上下文的生活数据，为AI提供丰富的“记忆”和“理解”素材	采集生理数据作为“体征状态”上下文，让AI更懂用户健康，提供个性化服务	提供比手机更专注、更沉浸、更自然的AI交互界面，成为“AI办事”的专属入口	将AI从“被动聊天”升级为“主动观察并执行”的桌面实习生，安全接管电脑操作	为Agent提供稳定、安全、开箱即用的专用运行环境，解决在主力机上部署的复杂性和安全问题	将AI深度植入设备操作系统底层，让设备本身成为AI的“身体”	通过实体形态提供情感价值与互动，但需结合具体功能场景（如教育、养老）才能成立	将语音作为核心甚至唯一交互方式，解放双手双眼，降低使用门槛	解决在公共场合语音交互的尴尬，提供隐蔽、便捷的操控方式

AI原生硬件与交互入口发展中美市场对比

中国已经有大量相应的创业项目和企业，并且发展非常活跃，在某些细分领域甚至领先全球，且阿里、字节、腾讯、小米等大厂全面入场，将AI硬件视为下一代入口进行争夺。

中美市场发展现状对比

维度	美国市场	中国市场
发展特点	愿景驱动，巨头定义。更侧重于由巨头（如OpenAI、Meta、苹果）从顶层定义下一代交互范式和硬件形态，赌的是“替代手机”的下一代计算平台	应用驱动，生态蔓延。更侧重于依托成熟的供应链和快速落地的能力，围绕现有AI生态（如OpenClaw、豆包、千问）做“外围硬件”创新和场景深耕，追求快速验证和商业化
发展阶段	处于前瞻性研发与高端市场验证阶段，巨头产品（如Meta眼镜）已证明大规模出货的可能性，但下一代“杀手级”形态仍在探索中	处于百花齐放的生态爆发与早期竞争阶段，大量创业项目涌现，在录音、第一视角、主动式终端等细分赛道已有成功案例和头部玩家，但市场整体仍处于早期，用户满意度有待提升
优势	强大的品牌、软件生态、原创技术定义能力	供应链能力、快速迭代的工程能力、对细分场景的敏锐洞察和庞大的内需市场
挑战	硬件制造依赖全球供应链（尤其中国），成本控制和生产灵活性可能受限	1. 同质化竞争激烈：一个赛道验证后迅速内卷（如AI眼镜、录音硬件） 2. 长期愿景与耐心：部分项目可能过于追逐热点，在定义“下一代平台”的长期愿景和耐心上不如美国巨头 3. 系统级生态掌控力：在定义像iOS、Android这样的底层系统级AI生态上，话语权仍相对较弱

中国市场目前相对欠缺的，可能是在定义全球性的、通用型AI原生操作系统（AI OS）及其终极硬件形态上的绝对主导权。

目前中国企业正在通过如下两种方式参与竞争并破局：

- 路径一：将AI深度融入现有设备系统（手机、电脑），争夺现有设备的“AI OS”控制权，如小米、华为
- 路径二：通过自研模型、芯片、云和硬件矩阵，试图构建一个软硬一体、服务闭环的独立AI生态，如阿里

04.基于Agent的新商业模式与 “一人公司” （OPC）

基于Agent的新商业模式与 “一人公司（OPC） ” 是指利用AI Agent（特别是像OpenClaw这样的自主执行型Agent）作为核心生产力或协作伙伴，从根本上重构个人或小微团队的创业形态、价值创造方式和盈利模式。中国市场的OPC创业在地方政府强力政策推动和庞大的应用场景催化下，呈现出快速、多元的落地态势，主要聚焦于以下几个方向：

方向	OPC发展方向			OPC赋能生态	
核心价值	极大扩展个体的能力边界，让一个人能挑战过去需要公司才能做的事			服务于这些新个体创业者的产业机会，形成层次丰富的生态	
主要方向	AI原生内容与IP创作	AI驱动电商与本地生活	传统产业数字化升级	Agent落地服务商（FDE模式）	OPC生态赋能者
细分场景	- 短视频/短剧矩阵 - 虚拟偶像与数字人 - 知识付费与教育	- 跨境电商 - 本地生活服务 - 直播电商	专业服务：在财务、法律、人力资源等流程中，用Agent自动化重复性任务	- 部署与培训 - 定制开发	- 社区与孵化 - 工具与供应链平台
核心特点	门槛低、变现快，依托中国成熟的短视频和电商生态，快速实现流量变现和知识付费	结合供应链与流量运营，充分发挥中国在供应链和本地生活服务领域的优势，实现 “小团队、大产出”	政策鼓励，与实体经济结合，地方政府通过补贴引导OPC解决制造业等传统产业的细微痛点	解决 “最后一公里”，这是目前最清晰、能快速产生现金流的OPC模式，契合中国市场对落地服务的强需求	服务于OPC创业者，在OPC热潮中，为创业者提供基础设施和资源，本身也是一种成功的OPC或小团队商业模式

05.垂直行业的Agent化重构

垂直行业的Agent化重构是指以OpenClaw这类具备自主执行能力的Agent OS为技术底座，对特定行业（如医疗、金融、法律、制造）的核心业务流程、知识体系、协作模式乃至商业模式进行系统性、深层次的智能化再造垂直行业的Agent化重构，其价值在于解决行业长期存在的“流程长、系统多、合规严、风险高、知识隐性化”等根本性痛点。目前，主要方向如下：

行业专属Agent OS/平台	为行业提供一套可组装、可治理、可交付的智能体基础设施，降低每个企业自建AI系统的成本，并实现行业能力的标准化与沉淀，如智诊科技WiseClaw
核心业务流程的Agent化	将行业内部高度重复、规则明确但流程复杂的任务（如报告生成、数据录入、合规审核）交给Agent，大幅提升效率并降低人为错误
行业知识与证据系统Agent化	将无法写入SOP的行业专家经验（情境依赖的判断、沟通分寸）通过Agent的“人设”（soul）、记忆（memory）和工具（tool）配置进行封装，成为可复用的数字资产
垂直场景的“AI+硬件”融合	通过专用硬件（如工业摄像头、传感器、机器人）为Agent提供物理世界的感知和控制能力，实现从数字世界到物理世界的闭环

中国市场垂直行业Agent化重构方面，核心优势在于强大的产业基础、政策推动力以及极致的产品化与集成能力，具体发展特点如下：

- 应用场景广覆盖与快速落地，不局限于高附加值领域，而是在制造业、政务、医疗、零售、电商、内容创作等实体经济与消费领域全面铺开
- 偏好“平台+行业模板”的一体化解决方案，由大厂或头部创业公司提供企业级平台，或深度集成于现有超级APP，降低企业使用和集成门槛
- 解决方案深度结合现有产业生态，与国内制造业供应链、电商生态、本地生活服务紧密结合，不追求纯数字颠覆，而是赋能和优化现有业务流程

03

破局之道：甲方企业的行动指南与风险预警

企业AI应用模式发生根本性变革：API对接→轻量外挂

OpenClaw代表了企业AI落地范式的深刻转变——从“重集成的API对接”到“轻量外挂的Agent直接执行”。企业不需要等待IT改造，只需部署OpenClaw并接入现有IM系统，就可以让数字员工开始工作。但企业级使用需要解决安全隔离、权限管理、审计合规等关键问题，切勿盲目拥抱。

“轻量外挂”模式带来的机遇

- 敏捷响应与快速验证：企业可以针对临时性或探索性的需求，快速部署专用Agent进行验证
- 激活存量系统与数据价值：部分老旧系统没有开放API或改造困难，OpenClaw可以通过“界面自动化”能力直接操作这些系统，让沉睡在老旧系统中的数据和流程重新产生价值，实现了“零改造智能化”
- 赋能业务一线：员工可以直接通过IM向Agent下达指令，获得实时协助，将AI能力民主化、平民化，这契合了“AI原生组织”中，智能体成为每个人随叫随到搭档的趋势

企业级应用必须跨越的关键鸿沟

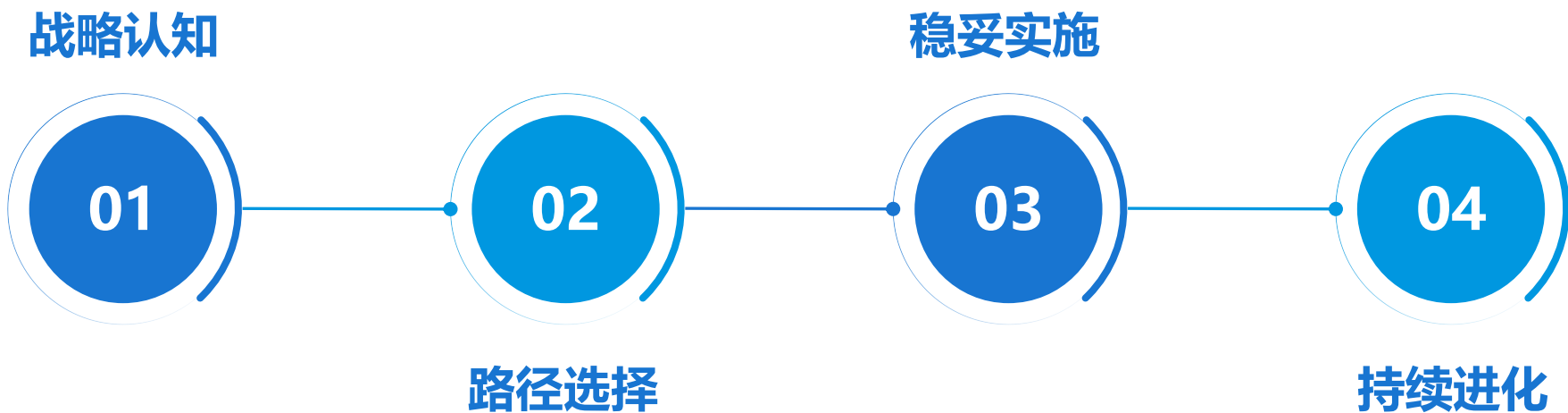
- 安全隔离与边界模糊：Agent以高权限直接运行于主机，缺乏沙箱隔离，导致攻击面扩大，主机易被远程接管
- 权限失控与最小权限：为求便利赋予Agent过高权限（如root），易引发误操作或越权访问敏感数据与系统
- 审计缺失与操作不可追溯：Agent自主执行过程若无完整日志记录，事故发生时无法追溯原因、界定责任，难合规
- 供应链安全与技能投毒：从开源社区安装的第三方Skills可能内含恶意代码，诱导Agent泄露数据或执行恶意操作
- 成本与资源的不可控：Agent自主规划可能导致不可预知的巨额API调用成本（Token消耗）或过量占用系统资源

破局之道：甲方企业的行动指南

对于计划入局的甲方企业，建议遵循“战略认知-路径选择-稳妥实施-持续进化”的框架，系统性地规划入局与应用。

需在战略层面更新对AI的认知，将Agent视为“新型数字劳动力”

Agent的“高权限”特性伴生着高风险，实施必须坚持安全可控



战略认知：重新定位AI价值，明确入局目标

甲方企业首先需在战略层面更新对AI的认知，将Agent视为“新型数字劳动力”和“业务流程重构者”，而非简单的聊天机器人或效率工具。

认知范式转变

理解OpenClaw代表的“从对话到执行”的范式革命。AI的价值不再仅限于生成内容，而在于能自主完成跨系统、多步骤的复杂任务，成为真正的“数字员工”

明确核心价值目标

结合企业自身痛点，明确引入Agent的核心目标，通常可分为三级：

- 一级：降本增效，替代重复、规则明确的劳动密集型工作
- 二级：体验升级与价值创造，提升客户服务体验、赋能员工，或创造新的智能产品/服务
- 三级：商业模式与组织重构，利用Agent能力重塑核心业务流程，甚至孵化新的业务模式

评估自身禀赋

盘点企业是否具备Agent落地关键资源：

- 数据资产：是否有高质量、结构化的业务数据？非结构化文档（合同、报告、邮件）是否完备？
- 流程标准化（SOP）：目标业务是否有清晰、可描述的工作流程？
- 技术生态：现有IT系统（CRM、ERP、OA等）的API开放程度如何？是否易于集成？

路径选择：三种入局模式与场景切入点

轻量应用模式

使用现有SaaS化Agent产品或利用大厂平台，该模式成本低、验证快。

- **适用企业类型：**

所有企业，尤其是初次尝试、资源有限的中小企业。

- **关键动作：**

1. 选用云端SaaS产品：直接使用腾讯云Lighthouse、火山引擎ArkClaw、阿里云CoPaw等提供的开箱即用Agent服务。
2. 接入成熟生态：在飞书、企微、钉钉等办公平台内，试用其官方或第三方开发的预制Agent（如飞书AI助手、北汽的巡检Agent）。
3. 采购专项技能：从ClawHub等技能市场购买与业务相关的现成Skill（如“周报生成”、“竞品监控”），装入自有Agent。

垂直重构模式

平台生态模式

路径选择：三种入局模式与场景切入点

轻量应用模式

在核心业务环节打造专属的“数字员工”，该模式价值高，深度融合。

● 适用企业类型：

在特定领域有深厚积累、流程复杂、数据丰富的行业领军企业。

● 关键动作：

1. 聚焦“一米宽，百米深”的场景：选择高价值、高频率、高数据可得性的核心环节切入，如金融业的智能投研、制造业的智能质检、零售业的智能供应链调度。
2. 构建“深度知识+独家数据”壁垒：将企业内部的专家经验、历史案例、专有数据库进行系统化梳理和数字化封装，作为Agent训练的独家“燃料”。
3. 选择可靠的技术伙伴：与具备行业经验的AI公司或云厂商（如火山引擎与券商共创）合作，共同开发，降低技术风险。

垂直重构模式

平台生态模式

路径选择：三种入局模式与场景切入点

轻量应用模式

将Agent能力平台化，对内赋能各部门，对外构建行业生态，核心目标在于谋生态、定标准。

- **适用企业类型：**

大型集团企业、平台型公司，或志在成为行业智能枢纽的企业。

- **关键动作：**

1. 建设企业级Agent中台：参考阿里云“Agent友好云”或腾讯云Agent Runtime的理念，构建统一、安全、可管理的Agent调度与治理平台，供各业务部门按需调用。
2. 推动内部“技能经济”：鼓励员工将优秀工作方法封装成Skills，在内网市场分享和交易，激活内部创新。
3. 探索行业生态：若条件允许，可考虑将自身成熟的业务流程Agent化，向上下游合作伙伴输出，成为行业解决方案的一部分。

垂直重构模式

平台生态模式

稳妥实施：四大核心原则与风控要点

Agent的“高权限”特性伴生着高风险，实施必须坚持安全可控。



安全与治理先行原则

- 最小权限原则：严格限制Agent访问权限
- 全流程审计：所有Agent操作必须有完整日志记录，做到可追溯、可审计、可复盘
- 人工审核关口：涉及关键节点，必须设置强制人工确认或审批环节



成本可控原则

- 警惕“Token黑洞”：需建立成本监控体系，设置单日/单任务调用预算上限，防止意外成本
- 优化模型策略：采用“大小模型混编”，简单任务用小模型/规则引擎，复杂任务再用大模型，平衡成本与效果



人机协同设计原则

- 明确角色分工：贯彻“AI划桨，人掌舵”，Agent负责执行与初步判断，人类负责目标设定、复杂决策和把关
- 设计交接机制：当Agent遇到困难或不确定时，应有顺畅的机制将任务移交人类，并附带清晰的上下文



组织与文化适配原则

- 设立新角色：考虑设立“AI流程专员”或“数字员工管理员”，负责Agent的培训、维护和效果优化
- 全员培训：提升员工AI素养
- 鼓励拥抱变化：管理层面需明确传达Agent是“增强员工”，将释放的人力引导至更具创造性的工作上

持续进化：从工具到伙伴的长期视角

Agent技术迭代飞速，企业需建立持续学习和演进的能力。

01

建立效果评估与反馈闭环

不仅看效率提升百分比，更要关注任务完成质量、商业价值转化（如成交率、客户满意度），建立机制，将人类员工的纠正和优化反馈回流，用于持续训练Agent

02

关注生态，保持开放

密切关注ClawHub等技能市场的新能力，积极引入外部优质Skills，同时，评估开源生态与闭源平台的发展，保持技术路线的灵活性

03

规划多智能体 (Multi-Agent) 演进

当单个Agent应用成熟后，可规划多个Agent协同工作，例如，设计“销售Agent”、“履约Agent”、“客服Agent”组成虚拟团队，完成从商机到售后的全流程

04

为“AI原生组织”做准备

从长远看，Agent将推动组织形态向流态化、网络化发展，企业可开始思考如何将组织结构、考核方式向“目标驱动、人机混合团队”方向调整

04

未来展望：趋势推演与不确定性挑战

技术演进趋势：从“能说”到“能做”，并向“能协作”与“能进化”深化



执行能力 成为核心指标

AI评价标准从模型参数和对话质量，转向任务完成率、复杂任务处理能力、执行可靠性与安全性，技术投资重点转向长程规划、工具调用鲁棒性、上下文工程等“行动赋能”技术



从单Agent到 多Agent系统 (Swarm)

个人助手形态的“单龙虾”将演进为专业化、可协作的“数字团队”，由不同专长Agent组成的协同 workflows，实现复杂任务的分解与并行处理



记忆与持续学习 成为关键壁垒

持久化、可管理、可共享的长期记忆系统（如MemOS、OpenViking提供的方案）将成为提升Agent效能、降低Token消耗的核心基础设施



模型调用模式 向“主辅模型协同”演进

为平衡成本与性能，系统架构会采用主模型负责核心推理，廉价辅助模型处理图像分析、网页提取、记忆检索等边角任务的模式

产品与形态趋势：工作台普及与交互入口重构



“AI原生桌面智能体工作台” 成为主流生产力工具

以Workbuddy、QoderWork为代表的产品，将作为“数字同事”深度集成到本地工作环境，通过自然语言驱动完成从信息处理到内容创作的端到端任务



交互入口从“独立App”回 归“超级入口”

用户将习惯从一个入口（如飞书、微信等即时通讯软件或统一的桌面工作台）操作几乎所有事情，软件的竞争力从争夺用户时长，转向争夺“被Agent优先调度和调用”的权利



部署形态“云端托管”与 “本地可控”并存

为降低使用门槛，开箱即用、云端托管的Agent服务将快速发展；同时，对数据主权和安全有高要求的企业及个人，仍会选择本地/私有化部署，形成混合架构

产业生态趋势：新价值链与关键生态位形成

OpenClaw正在催生一个层次分明的新生态，投资和创业机会围绕以下关键生态位展开：

调度层（操作系统/框架）

核心价值在于任务编排与执行控制权，如 OpenClaw、Hermes Agent等基础框架，以及其上更易用的变体

连接器层

核心价值在于打通数字与物理世界，如工具集成平台（MCP协议）、硬件入口（AI眼镜、机器人）等

价值交换层（市场）

核心价值在于技能与能力的流通，如Agent应用商店、技能商店等

垂直重构者

核心价值在于行业知识与流程封装，如医疗（WiseClaw）、金融（券商智能体）、教育（九章龙虾）等领域的深度解决方案

安全与治理平台

这是企业规模化应用的基石，如提供安全隔离、权限管控、成本审计、操作追溯的企业级Agent管理平台（如火山引擎AgentKit、阿里云“Agent友好”的云）

不确定性挑战：繁荣背后的四重隐忧

OpenClaw时代中国Agent产业的未来，画卷宏大但笔触未定。确定的趋势是Agent将更深地融入生产流程，推动基础设施智能化，并重构软件生态，而最大的不确定性来自于如何跨越“算力成本、安全信任、生态主导权、商业可持续”这四座大山。

01

技术悬崖：长上下文与自进化的成本悖论

挑战：Agent完成复杂任务依赖长上下文和持续学习，但这导致Token消耗呈百倍增长，形成“算力黑洞”。

不确定性：中国模型厂商能否在长上下文效率、推理成本控制上实现突破，打破与顶尖闭源模型的技术代差，将决定中国Agent生态是依附于人还是自主可控。

03

生态分裂：开源协议与本土标准的博弈

挑战：OpenClaw等开源项目掌握着底层协议演进的主导权。中国厂商在快速跟进和适配的同时，也面临技术路线被“卡脖子”的风险。

不确定性：中国产业是会深度融入全球开源生态，还是出于安全、合规和数据主权考虑，催生出独立的“中国版Agent协议栈”？这关系到中国生态的全球影响力与互操作性。

02

安全与信任：规模化落地的“阿克琉斯之踵”

挑战：Agent的高权限特性使其成为安全重灾区。恶意技能注入、权限滥用、操作幻觉、数据泄露等风险从技术问题升级为企业运营风险。

不确定性：整个行业尚未建立成熟的企业级安全范式，是出现统一的安全标准与合规框架，还是各家形成封闭的“安全孤岛”，将影响生态的开放性与发展速度。

04

经济模型与可持续发展：Token经济的平衡木

挑战：Agent驱动的Token消耗爆发式增长，但可持续的商业模式仍在探索，用户能否接受为结果付费？企业ROI是否清晰？如何避免陷入“赔本赚吆喝”的流量陷阱？

不确定性：未来是出现健康的、分层（To B/To C）的Agent价值计价体系，还是陷入巨头补贴、中小玩家难盈利的恶性竞争？这决定了整个产业是走向繁荣还是泡沫。

易观分析

易观旗下专注数智化市场发展与趋势研究

• 行业洞察 • 策略咨询 • 用户洞察 • 解决方案

易观分析



数字经济全景洞察

易观千帆



金融行业数字用户
同业对标

易观方舟



全场景私域用户运营

易观社群



加入易观社群
与行业伙伴一同交流