

· 理论研究 ·

智能体经济的崛起： AI智能体对商业世界的重塑

陈永伟

(《比较》杂志社 研究部, 北京 100029)

摘要：随着生成式人工智能（AI）技术的快速演进，AI智能体已具备自主规划、执行和学习的能力，正逐步成为商业世界的关键参与者，一种全新的经济形态——智能体经济正在崛起。当前全球AI市场规模迅速扩张，AI智能体的应用正在重塑商业生态系统、企业组织形态和商业模式。AI智能体对商业生态系统的影响体现在参与者角色、分工、主导权和治理机制等方面的变化。AI智能体通过主动决策、环境交互和协同机制，改变了企业的规模、组织结构、决策层级、员工角色和企业文化。随着AI智能体的发展，原有商业模式或将逐渐失效，新型商业模式将在技术变革的推动下不断涌现。在提升效率的同时，AI智能体也带来了挑战和风险，具体包括隐私与数据安全、决策失控与错误风险、过度依赖与技能弱化、就业影响与组织变革阻力，以及合规与监管挑战等方面。本文旨在揭示AI智能体对经济发展模式的深远影响，为理解未来商业变革提供理论支撑。

关键词：智能体经济；AI智能体；商业模式创新；企业组织变革；商业生态系统

中图分类号：F124.3；F123.9 **文献标识码：**A **文章编号：**1000-176X(2025)07-0015-17

一、引言

自2022年11月ChatGPT引发“生成式AI革命”以来，全球人工智能（Artificial Intelligence, AI）的发展明显提速^[1]。在短短几年时间内，AI模型的性能得到了显著提升，其功能已从最初仅能输出文本扩展为支持多模态交互，在语言理解、数学推理和编程能力等多个方面均取得了长足进步。与此同时，AI的使用成本大幅下降。特别是在2024年国产大语言模型DeepSeek上线后，AI的训练成本和使用成本迅速降至原有水平的几分之一^[2]。受上述两方面因素的共同推动，AI行业规模迅速扩张。据估算，2025年全球AI市场规模已接近1万亿美元，预计到2030年，AI市场规模将进一步增长至2万亿美元^[3]。

需要指出的是，尽管当前AI技术已取得显著进展，但其性能表现仍存在一定局限性。现有大语言模型虽然能够在人类的指令下完成多项指定任务，但其本身并不具备自主决策能力，因而在应对复杂任务时，大语言模型仍难以独立胜任。在此背景下，AI智能体（AI Agent），特别是通用型AI智能体正逐渐成为AI企业竞相布局的新领域和战略重点。

收稿日期：2025-06-04

作者简介：陈永伟（1982-），男，浙江杭州人，研究员，博士，主要从事产业经济学、互联网经济学和法律经济学研究。
E-mail: chen Yongwei1982@126.com

当前市场上已涌现出大量 AI 智能体产品。例如，OpenAI 公司推出的 AutoGPT、Operator 和 Deep Research，Anthropic 公司推出的 Computer Use，以及中国初创公司 Monica 推出的 Manus 等 AI 智能体，均能在一定程度上自主协助人类完成复杂任务。与此同时，众多企业已经开始采用“数字员工”“AI 助手”替代人类员工执行工作任务。AI 智能体的迅速崛起已经引起了行业的广泛关注。例如，Forrester 公司已将 AI 智能体列为 2025 年关键新兴技术之一，而全球领先的 IT 研究与咨询公司 Gartner 更是将其评为 2025 年十大技术趋势之首^[4]。2025 年被业界称为“AI 智能体元年”，以强调这一年在科技发展中的重要地位。

毫无疑问，AI 智能体的广泛应用将显著提升生产的自动化水平，从而大幅度提升生产效率。根据预测，到 2028 年，有 33% 的企业级软件应用将集成 AI 智能体功能，15% 的日常业务决策可以由 AI 智能体自动完成，AI 智能体的应用有望使组织运营成本降低 40%，使营业收入提升 20%—30%^[5]。然而，相较于单纯的生产效率提升，AI 智能体给商业生态系统、企业组织形态和商业模式所带来的影响可能更为深远和关键。随着其自主决策能力的不断增强，AI 智能体将逐渐成为市场中除人类之外的另一重要决策主体，进而对整个商业生态系统产生深刻影响。在宏观层面，AI 智能体的发展将重塑商业生态系统中各参与者的角色及其相互关系；在微观层面，AI 智能体则将引发企业组织形态的重大变革。此外，企业的商业模式也将经历深刻的调整：一些传统、低效的商业模式将因 AI 智能体的兴起而逐步被淘汰。与此同时，一系列依托 AI 智能体的新商业模式也将不断涌现。可以预见，一种全新的经济形态——智能体经济（Agentic Economy）正在崛起^[6]。

尽管 AI 智能体在商业领域展现出巨大的潜在影响力，但截至目前，国内尚缺乏专门针对该问题的系统性研究，相关的国外文献同样较为稀缺。为弥补这一研究空白，本文在界定 AI 智能体基本概念及其基本经济特征的基础上，深入分析其给商业生态系统、企业组织形态和商业模式所带来的影响。此外，本文还探讨了 AI 智能体兴起过程中企业所面临的挑战和风险，并对其可能的应对策略进行分析和展望。

二、AI 智能体的基本架构、分类体系及与生成式 AI 的比较研究

（一）AI 智能体的基本架构

AI 智能体是指能够自主规划且执行行动的 AI 系统。与只能在用户提示下产生输出的传统 AI 系统不同，AI 智能体具有较强的主动性和适应性。AI 智能体可以在无需人类持续干预的情况下感知外部环境，进行推理和决策，完成多步骤的复杂任务，并根据任务反馈不断进行自我学习和优化。在一些媒体报道中，AI 智能体与代理型 AI（Agentic AI）这两个概念经常被混用。严格而言，二者并不完全等同。代理型 AI 代表一种新型的智能架构，其核心在于通过多个专业化 AI 智能体间的协作，以实现复杂且高层次的目标^[7]。也就是说，代理型 AI 是指为完成特定目标，整合且协调多个 AI 智能体运作的一个系统性集合。自人工智能学科诞生以来，研究者们便致力于 AI 智能体的构建。最初，这些 AI 智能体仅能依据预设程序与结构化、简单的环境进行交互。随着 AI 技术的不断进步，AI 智能体逐步具备了与复杂环境互动且在交互过程中自主学习的能力。特别是近年来，大语言模型的快速发展显著提升了 AI 智能体的性能，使其在实际应用中展现出前所未有的潜力，真正推动了 AI 智能体从科幻走向现实。

尽管不同类型的 AI 智能体在结构设计上可能存在显著差异，但从一般意义上而言，AI 智能体通常由三个核心组成部分构成：传感器（Sensors）、控制中心（Control Center）和执行器（Effectors）^[8]。其中，传感器主要用于从外部环境中采集相关数据；控制中心负责对所采集的数据进行分析处理，并据此制定相应的行动方案；执行器则负责具体执行行动方案，并对外部环境产生影响。

图1是一个简化的AI智能体架构示意图。如图1所示，AI智能体利用传感器收集关于其操作环境的各种数据，从而实现对外部环境的感知和理解。随后，控制中心对所收集的数据进行分析处理，并据此进行决策。最终，通过执行器实施相应行动，以此完成与环境的交互过程。在此过程中，“环境”指的是AI智能体活动的空间范围，它可以是物理形态的，也可以是数字形态的。用户或其他AI智能体能够经由操作界面介入此环境，进而影响AI智能体的行为模式。

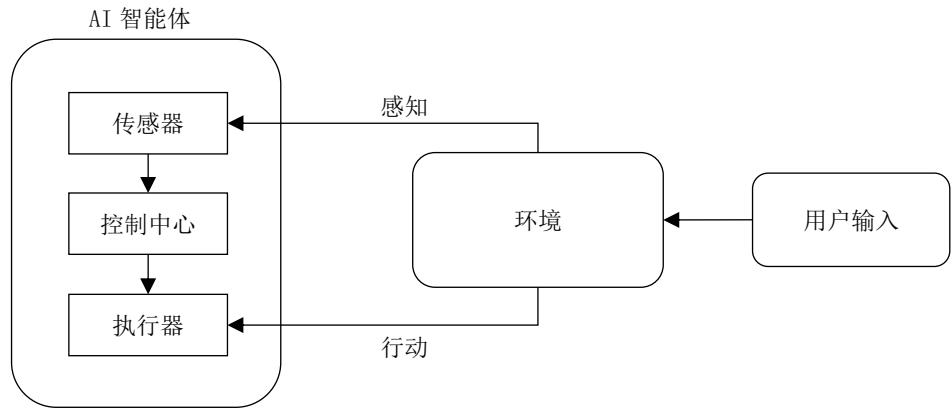


图1 简化的AI智能体架构

（二）AI智能体的分类体系

依据不同的分类标准，AI智能体可以被划分为多种类别。根据决策过程和行为模式的不同，AI智能体主要分为确定性AI智能体（Deterministic AI Agents）和非确定性AI智能体（Non-Deterministic AI Agents）两大类^[8]。

确定性AI智能体是指在相同的输入条件和环境状态下，其行为和输出结果始终保持一致的智能体；非确定性AI智能体的特性则在于其行为或环境结果中存在随机性和不确定性。进一步地细分，确定性AI智能体包括简单反射AI智能体（Simple Reflex AI Agents）和基于模型的反射AI智能体（Model-Based Reflex AI Agents）。简单反射AI智能体仅基于当前感知进行决策，通过预定义的“条件—行动规则”，直接将环境输入映射到相应的行动，而不考虑历史信息和环境状态的变化。相比之下，基于模型的反射AI智能体不仅考虑当前环境，还会结合历史信息和环境变化来进行决策。

非确定性AI智能体可以细分为基于目标的AI智能体（Goal-Based AI Agents）、基于效用的AI智能体（Utility-Based AI Agents）和学习型AI智能体（Learning AI Agents）。基于目标的AI智能体在决策时侧重于评估行动是否有助于实现既定目标；基于效用的AI智能体在此基础上还会对达成目标的不同路径进行成本—收益分析，以追求效用最大化。值得注意的是，无论是基于目标还是基于效用的AI智能体，它们的目标和效用函数都是预先设定的，而学习型AI智能体能够通过与环境交互不断优化这些规则，从而提升行动效率。

根据存在形态的不同，AI智能体可以进一步划分为虚拟AI智能体（Virtual AI Agents）和具身AI智能体（Embodied AI Agents）^[9]。虚拟AI智能体是指基于软件系统运行于数字环境中，用于自动执行各类数字任务的智能体。例如，“斯坦福AI小镇”项目即由多个虚拟AI智能体构成^[10]，OpenAI公司推出的Operator和Monica公司推出的Manus等能够自主完成特定任务的AI智能体也可以归入此类。

相比之下，具身AI智能体则是拥有物理实体的AI智能体，能够在现实世界中感知环境，并执行任务，是典型的嵌入式智能形式。无人驾驶汽车和人形机器人等是具身AI智能体的典型代表。从技术需求角度来看，虚拟AI智能体和具身AI智能体在实现路径和能力要求上存在一定差

异。目前，大语言模型（Large Language Model, LLM）已能够为虚拟AI智能体提供较为充分的能力支持。然而，对于需要与物理环境进行深度交互的具身AI智能体而言，其对多模态感知能力和环境推理能力的要求更高。因此，除LLM外，具身AI智能体通常还需结合大型视觉模型（Large Vision Model, LVM）和世界模型（World Models, WM）等技术模块以支撑其复杂行为。然而，截至目前，相关技术的发展仍相对滞后，尚难以充分满足具身AI智能体快速发展的实际需求，成为制约其广泛应用的重要因素之一。

（三）生成式AI与AI智能体的比较研究

在当前阶段，与生成式AI相比，AI智能体最核心的特征在于其行为的自主性和可扩展性（如图2所示）。以ChatGPT、DeepSeek等基于生成式AI技术的大语言模型为例，在使用这些AI完成任务时，用户通常需要通过不断输入提示词来引导AI的行为。AI在接收到提示词后，进行信息感知和分析，并生成相应的输出结果；用户则根据输出内容进一步发出指令，从而实现人机协作完成任务。在此过程中，人类与AI各自扮演不同角色，协同完成各项任务。此外，对于一个已经训练完成的生成式AI而言，其基本能力在实际应用中通常不会显著提升，即便有所改进，也往往局限于基于已有参数结构的微调，难以实现根本性的能力跃升。

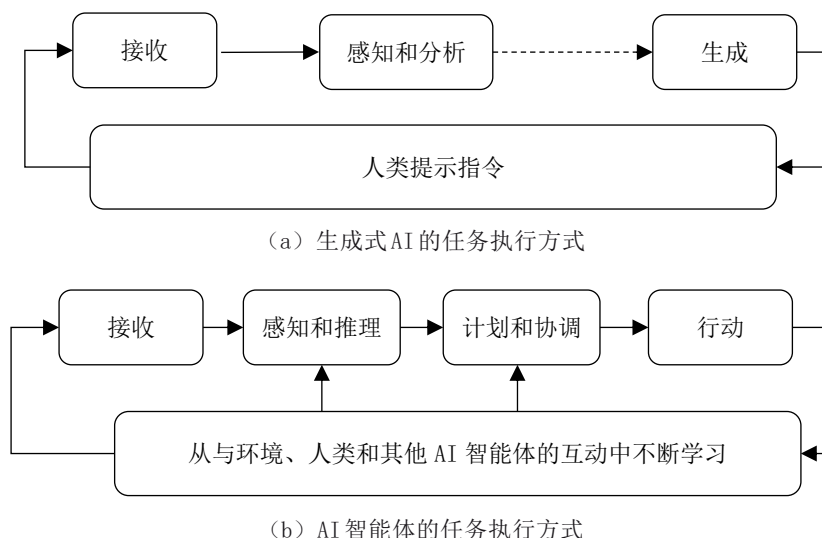


图2 生成式AI与AI智能体的任务执行方式对比

相比之下，AI智能体的行为具有高度自主性。它能够在无人直接干预的情况下，独立地与环境或其他AI智能体进行交互，接收信息，并完成包括感知和推理、计划和协调等一系列认知和操作过程，从而自主执行任务。更为重要的是，当前多数AI智能体具备学习能力，能够在与环境及其他智能体的持续互动中不断优化自身的算法和行为策略，进而实现性能的持续改进。尤其需要指出的是，在模型上下文协议（Model Context Protocol, MCP）、智能体网络协议（Agent Network Protocol, ANP）和智能体到智能体协议（Agent-to-Agent Protocol, A2A）等开源协议的支持下，AI智能体已具备工具整合和智能体间协作等关键能力。具体而言，MCP旨在实现大语言模型与外部数据源及工具的安全双向集成，从而扩展模型的感知边界和功能边界；ANP旨在使AI智能体能够在互联网环境中相互发现、连接和交互，构建一个去中心化的智能体协作网络；A2A旨在提升不同AI智能体间的互操作性，提升其在多主体系统中的协同效率。依托这些开源协议，不同开发者所构建的AI智能体不仅能够灵活调用各类工具和数据资源，还能实现跨平台协作，进而形成一个高度互联的智能体网络（Agentic Web）^[11]。这一发展标志着AI从传

统的任务辅助角色演进为可自主完成全流程工作的智能实体，使其在多个领域具备对人类活动有效替代的能力。与此同时，AI智能体也开始在商业生态中扮演类似市场主体的角色。由此，智能体经济作为一种全新的经济形态逐步显现，并可能在未来重塑资源配置方式、生产组织形式和市场互动机制。这一趋势为经济学研究提出了新的理论和实践课题，具有重要的学术和政策意义。

三、AI智能体的经济特征

从经济学视角来看，AI智能体不仅是一项新技术，而且是在现实中具有重要经济意义的新经济参与主体。不同于传统工具，AI智能体具备在经济活动中充当代理人的关键特质，包括拥有明确的目标、一定的决策权限和自主执行任务的能力。这些特性使得AI智能体在经济活动中的角色及其所带来的经济影响显著区别于以往的技术进步。

（一）委托—代理的变化

AI智能体所具备的自主性和决策能力使其有望成为人类的代理人，即在经济活动中代表（而非仅仅是协助）委托人执行各类任务，并以委托人的利益为行动导向。这一特性引发了一种新型的委托—代理问题。在经济学中，委托—代理问题是指在目标不完全一致和信息不对称的条件下，如何协调委托人与代理人之间利益关系的经典理论问题。传统上，由于委托人与代理人均为人类，二者之间的监督和激励机制往往伴随着高昂的交易成本，因而该问题的解决方案通常只能达到次优状态。

从理论层面来看，人们可以通过预先设定AI智能体的效用函数，使其与人类委托人的偏好保持一致，从而确保其行为完全符合人类利益。在这一框架下，AI智能体的行为可以被视为对委托人偏好的忠实执行，进而有望克服传统意义上的委托—代理问题。然而，在现实应用中，实现AI与人类之间的价值对齐（Value Alignment）面临诸多挑战^[12]。在某种意义上，这又引发了人与AI智能体之间新型的委托—代理问题。例如，在实际场景中，可能会有多个消费者委托同一个AI智能体对某商品进行竞拍。此时，AI智能体需在不同委托人之间进行利益权衡，这可能导致某些委托人的利益受损。

（二）成本结构的变化

从成本结构来看，AI智能体具有接近于零的边际成本特征。这意味着在完成初始研发和部署高额的固定成本投入之后，AI智能体能够以极低的增量成本被广泛使用、复制和推广。需要特别指出的是，此处所指的成本不仅限于传统数字产品的复制成本，还包括内容生成成本、信息搜寻成本和交互成本等^[13]。依托大语言模型的强大能力，AI智能体能够以近乎零边际成本的方式生成各类内容产品。与此同时，通过引入可配置的“工作流”机制，AI智能体还能在无需人工干预的情况下，对生产流程进行有效控制，从而确保输出内容满足消费者的个性化需求。此外，借助各类通信协议和网络接口，AI智能体还能够以较低成本高效地完成信息检索任务，并与其他AI智能体或AI系统交互协作。这使得AI智能体能够在商业活动中替代人类执行诸如询价、比价和谈判等复杂任务，从而显著降低交易成本，并提升市场效率。

一般用户和中小企业通常通过云端调用AI智能体服务，从而以接近于零的边际成本开展各类商业活动。这一成本结构的变化对现有许多商业模式构成了潜在的颠覆性影响，尤其是那些依赖信息中介或交易撮合功能的平台型商业模式可能会面临前所未有的挑战。然而，尽管AI智能体的使用成本较低，但其研发和技术支持仍需要大量的前期固定资本投入。这一特征使得专业AI智能体技术供应商普遍具有显著的规模经济效应，其成本结构呈现明显的报酬递增特征。这意味着一旦某一技术供应商在技术上取得领先地位，便可能凭借成本优势迅速扩张市场份额，进而占据行业主导地位。整个商业生态系统对其技术平台和服务的依赖程度也将随之上升。

（三）网络效应的变化

AI智能体依托网络进行学习和演化，其性能提升的速度在很大程度上取决于交互数据的广度和深度。因此，随着用户数量和数据规模的增长，AI智能体的功能将得到进一步强化，从而吸引更多用户参与，形成良性循环。这一机制表明，AI智能体具有显著的网络效应^[14]。需要指出的是，AI智能体所表现出的网络效应与平台型网络效应存在显著差异。在传统平台经济中，网络效应主要源于平台两侧用户间的相互依赖和需求。作为交易中介，平台企业通常能够通过技术手段和规则设计对这种网络效应进行有效控制和利用，从而实现利润最大化^[15-16]。与此同时，平台往往有意设置各种转换成本或接入壁垒，限制用户的多归属行为，以防止用户流向竞争对手，维护自身的市场地位。在这种机制下，网络效应被局限在由平台主导的若干封闭式商业生态系统之中，形成了一个高度割裂的市场格局。有学者将这一现象称为“技术封建主义”，即各个平台如同中世纪的封建领主，各自为政、划地为界，阻碍了数据和用户在更大范围内自由流动和整合^[17]。

相比之下，AI智能体所引发的网络效应具有更强的开放性。由于AI智能体能够以较低的成本协助用户在不同平台间进行选择和切换，其所引发的网络效应及能力增强效应有助于降低用户对特定平台的依赖程度，从而削弱平台的锁定效应。当然，尽管这种网络效应增强了用户的自主性，AI智能体的技术供应商仍可以借助其积累的数据优势和用户基础，进一步巩固自身的市场地位。由此，技术供应商有可能取代现有平台，成为新商业生态系统的核心主导力量。

四、AI智能体对商业生态系统的影响

AI智能体的普及和广泛应用将会对商业生态系统带来颠覆性的影响。具体来说，其影响表现在四个方面。

（一）参与者角色的变化

在智能体经济中，商业生态系统将迎来新型参与者的加入，并且现有参与者间的分工格局也将发生显著变化。在传统的商业生态系统中，主要参与者包括核心企业、供应商、分销商、互补者和消费者等主体^[18]。核心企业负责引领整个商业生态系统的架构设计和演进方向，提供基础平台、制定规则，并协调资源及合作；供应商则为商业生态系统提供必要的技术基础设施、硬件组件、云服务网络通信支持；互补者通过提供与核心企业产品或服务相辅相成的产品或服务来增加其使用价值，形成丰富的产品或服务组合；分销商的任务是将产品或服务传递给最终客户或零售端；而消费者是最终价值的接受者，并通过反馈机制对商业生态系统的演变产生影响。随着平台经济的兴起，平台型企业逐渐成为最为重要的核心企业。在此模式下，生态系统中的其他参与者围绕着平台提供的中介服务进行交互和开展业务活动，平台利用其独特的中介地位从这些交易中抽取分成^[19]。

AI智能体的兴起为商业生态系统中的参与者提供了绕过平台中介、规避高额平台抽成的可能性。依托基础模型和各类通信协议的技术支持，AI智能体间能够实现高效、直接的交互，从而构建起一个去中心化的智能体网络（如图3所示）。借助这一网络结构，生态参与者可以在点对点的基础上开展协作和交易，显著提升分工和合作的效率。与此同时，AI智能体间的协同也将催生一系列新型参与者。例如，AI咨询服务商、数据经纪人等新兴互补者将应运而生，并在新商业生态系统中扮演关键角色，提供专业化服务，以支持AI智能体的运行和优化。此外，作为AI智能体服务的核心支撑力量，AI智能体技术供应商和数据服务商的地位也将显著提升。它们主要负责AI智能体模型的研发、算法平台的搭建、算力基础设施的供给，以及行业数据的采集和处理，在智能体经济中发挥基础性作用。可以预见，在智能体经济的发展过程中，这些技术供应商和数据服务商有望逐步取代传统平台企业，成为新商业生态系统的核心企业。

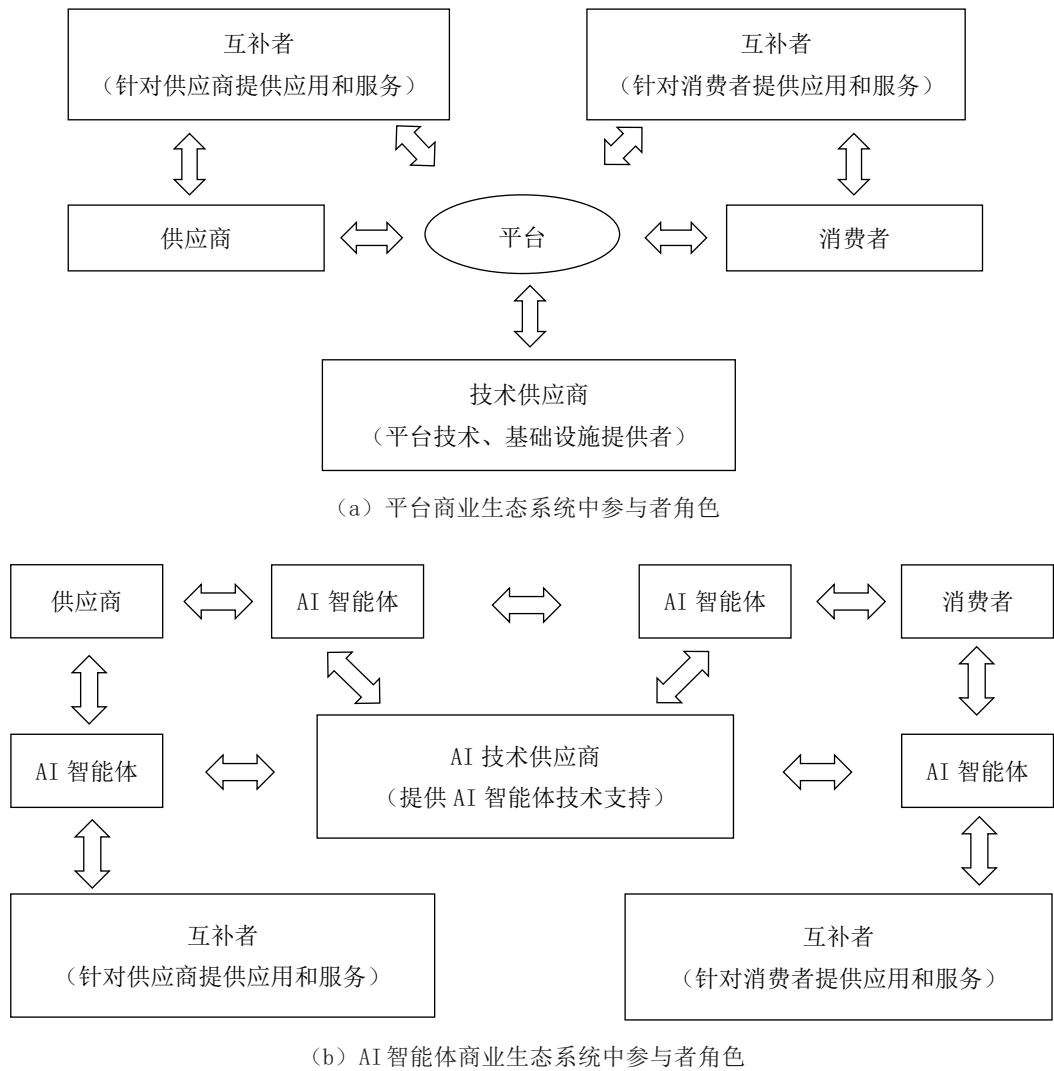


图3 AI智能体兴起后商业生态系统中参与者角色的变化

(二) 分工的变化

AI智能体通过自动化谈判、智能合约执行和信息匹配等机制，显著降低了企业间合作的交易成本，从而对商业生态系统内部的协作模式和组织结构产生深远影响。一方面，AI智能体能够自动识别供需关系，有效缓解信息不对称问题。以供应链商业生态系统为例，AI智能体可以实时监测市场价格和产能动态，为制造商自动筛选最优的原材料供应商，从而大幅降低采购过程中的搜寻成本和议价成本。另一方面，借助智能合约等技术手段，AI智能体能够在跨组织交易中实现履约流程的规则化与自动化，从而减少对人工监督和干预的依赖，进一步降低交易成本。上述两方面的协同效应，使得市场整体的交易成本显著降低。根据经济学的基本原理，当交易成本降低时，原本内生于企业的活动将更有可能被外部市场所替代。可以预见，随着AI智能体的发展，企业将越来越多地呈现拆分趋势，即鼓励更多专业化的小型主体通过市场机制进行协作，以实现高效的价值创造，而非依赖单一企业的内部资源整合。

在这种背景下，商业生态系统内部的分工将趋于精细化。大量微型企业和初创团队可能专注于价值链中的某一特定环节，并通过AI智能体的协调机制，实现与其他环节的高效衔接，从而完成端到端的价值传递。以服装产业为例，在传统模式下，一个制衣企业通常需要在内部设立设

计、生产和营销等多个职能部门,在推出一个服装品牌时,还需依赖这些部门间的协同运作。在AI智能体的支持下,品牌方可以将其核心资源集中于产品设计和品牌管理,同时将生产环节外包给由AI智能体优化调度的智能工厂,将营销职能交由AI智能体驱动的数字营销代理执行。各个环节间的信息流通和任务协调也可以由AI智能体自动完成。相比传统组织形态,这种基于AI智能体的新形态不仅能够更高效地调动和整合整个商业生态系统的资源,还能显著降低协作过程中的交易成本和不确定性,从而大幅提升商业生态系统的整体协作效率。

(三) 主导权的变化

在现有的商业生态系统中,某些大企业,尤其是大型平台企业占据主导地位。这些企业在商业合作中充当关键节点,在价值创造过程中扮演重要角色,并主导规则制定和价值分配机制。然而,随着AI智能体的广泛应用,商业生态系统的权力架构将发生系统性重构。一方面,AI智能体的应用可能加剧头部效应。拥有强大AI能力的平台企业有机会转型为AI服务提供商,利用其规模和数据优势进一步巩固自身地位。这种转变可能会使这些企业在商业生态系统中的主导地位更加稳固。另一方面,AI智能体也为中小企业提供了一种“杠杆”,使其能够在一定程度上与大企业竞争或合作。例如,中小企业可以通过调用开源或第三方AI智能体,获得以往仅大企业才具备的数据分析和自动化处理能力,从而缩小技术差距。借助这种模式,中小企业不仅能在大企业主导的竞争格局中实现成长和突破,更能逐步在商业生态系统中争取到更大的话语权,从而获得角逐商业生态系统主导权的机会。

在未来一段时间内,上述两种效应将同时发挥作用。究竟哪一种效应占据主导地位,在很大程度上取决于商业生态系统中标准和接口的开放程度。如果与AI智能体相关的关键技术和基础设施持续由少数大企业掌控,则商业生态系统的主导权可能会进一步向这些企业集中,其他参与者则需遵循其设定的规则。在这种情况下,头部企业的市场力量和控制力将进一步增强。相反,如果开源模型和开放标准成为主流,则AI智能体有望成为整个商业生态系统中的通用工具,实现普惠发展。在这样的环境中,新兴企业将有机会获得更多的资源和机会,从而可能削弱现有大企业的控制力,并促使商业生态系统主导权从大企业转移到更具创新性和灵活性的新进入者手中。

(四) 治理机制的变化

商业生态系统的良性运行高度依赖参与者间的信任机制和协作机制。随着AI智能体的应用,商业生态系统内各主体间的关系发生了深刻变化,这对商业生态系统治理提出了新的挑战和要求。当AI智能体作为代理人参与跨组织交易时,其行为可能引发额外的委托—代理问题。此时,如何有效协调人类委托人与AI代理人之间的利益关系,成为亟须解决的核心议题。例如,一个负责采购任务的AI智能体若同时代表多家企业进行价格谈判,则可能面临多委托人情境下的利益冲突问题。在这种情况下,该AI智能体如何公平地对待不同委托人,并妥善处理其利益诉求间的矛盾,构成了治理领域的重大挑战。此外,多个AI智能体间的自主博弈也可能带来诸如算法合谋等反竞争行为,从而对市场的公平性和商业生态系统的稳定性构成威胁。如何识别、监管和有效应对这类潜在风险,亦是当前治理机制应重点关注的问题。

为应对此类挑战,有必要将AI智能体治理纳入商业生态系统的战略议程之中。具体而言,应在商业生态系统层面建立系统化的AI智能体治理框架,具体包括制定统一的数据共享标准、构建AI智能体决策的审核机制,以及设立针对AI智能体失当行为的责任认定与应对协议。与此同时,商业生态系统的领导者也应承担起相应的治理责任,设置必要的“制度护栏”,以防止AI智能体偏离人类意图或损害整体生态利益。上述治理机制的建立和实施,无疑将深刻改变现有商业生态系统的运作方式及其内在逻辑,推动其向更加智能化、规范化和可持续发展的方向发展。

五、AI智能体对企业组织形态的影响

AI智能体崛起所带来的影响不只限于宏观层面，对于企业内部的影响也是不容忽视的。AI智能体的应用将对企业的规模、组织结构、决策层级、员工角色和企业文化等方面产生影响。

（一）规模的变化

根据科斯的经典理论，企业的规模由其内部管理成本与外部市场交易成本之间的权衡所决定。当企业内部管理成本低于外部市场交易成本时，企业倾向于扩大规模，将更多的交易环节内部化；反之，当内部管理成本高于外部市场交易成本时，企业则倾向于缩小规模，通过市场机制进行资源配置^[20]。AI智能体的应用有望同时降低企业管理成本和市场交易成本。然而，不同企业在两类成本的下降幅度上可能存在差异。在某些企业中，AI智能体所带来的企业管理成本下降幅度可能显著超过市场交易成本的下降幅度，这类企业有可能演化为“大而扁”的组织形态，即具有庞大的规模，但管理层级相对简化。需要指出的是，此处所指的企业规模并非以雇佣员工数量为衡量标准，而是指企业能够直接调用和控制的资源总量。事实上，由于AI智能体能够在较少甚至无需人工干预的情况下独立完成大量任务，因而会使企业的整体用工数量减少。与此同时，在AI智能体的支持下，企业所能掌控的资产、数据、算力和其他生产性资源的数量则可能大幅增加。在这种背景下，超级自动化企业作为一种新型企业形态，将日益常见。

在另一些企业中，AI智能体所带来的市场交易成本下降幅度显著超过企业管理成本的下降幅度，这类企业因此具备了缩小组织规模的动力和条件。它们将仅保留部分核心资源，而将非核心资源的获取渠道转向外部商业生态系统。至于具体保留哪些资源，则主要取决于该资源的战略重要性和稀缺性。例如，某些企业的数据资产和核心AI算法是其竞争优势的关键来源，企业则会保持对这些要素的直接控制，而将非核心业务外包；而另一些企业的通用型AI服务具备高度可得性和稳定性，企业则更倾向于将AI的相关应用外包，以进一步精简组织结构。在极端情况下，一些能力突出的企业家甚至可以借助AI智能体完成企业运营中的大部分任务，从而催生出“一人企业”这一新型组织形式。

（二）组织结构的变化

随着AI智能体的广泛应用，企业内部的组织结构将逐步由传统的金字塔式层级结构向更加扁平化和灵活化的形态演进。这一转型首先体现在中层管理者的角色发生深刻变化。传统上，中层管理者的主要职责包括信息汇总、指令传递和下属绩效监督。然而，在当前企业管理实践中，一些企业已开始应用智能驾驶舱等工具，使管理者能够实时获取一线运营数据，无需依赖传统的逐级汇报机制。这在一定程度上弱化了中层管理者作为信息中介的职能必要性。随着AI智能体的深入应用，AI算法不仅能够进一步提升一线业务数据的采集、整理和分析效率，还能自动生成报告、发出预警，并直接向高层管理者或一线员工提供建议和决策支持。由此，企业对传统科层组织结构中多级汇报链条的依赖将进一步减弱。此外，AI智能体凭借其“ workflow”管理能力，还能够承担过去主要依赖人工完成的任务，如员工工作状态的跟踪、绩效评估等。这使得中层管理者在组织中的职能进一步被弱化甚至虚化。

在这一背景下，部分中层管理者的角色将从传统的任务监督者逐步转变为AI智能体的维护者、协调者和团队的教练型管理者；而另一些中层管理者则可能被调整至更接近业务一线的岗位，直接参与具体操作和执行工作。与此同时，随着AI智能体信息处理和决策支持能力的提升，高层管理者能够有效管理的下属数量也将显著增加。这将进一步推动组织结构向更加扁平化的方向演进。随着层级的压缩，岗位间的职能壁垒也将被逐步打破，“多岗协作”“一人多岗”的现象将日益普遍。这种灵活的组织安排不仅提升了人力资源的利用效率，也有助于提升企业内部的协同效率和增强创新能力^[21]。

（三）决策层级的变化

随着AI智能体的应用，企业倾向于进一步将决策权下放至一线员工，并鼓励团队自治。传统的科层化管理虽然能够有效规范作为代理人的一线员工的行为，确保其行动与作为委托人的股东和高层管理者的利益保持一致，但也严重限制了一线员工的积极性和创造性。根据 Hayek^[22] 的观点，一线员工通常比高层管理者掌握更多与实际工作相关的具体信息，对于具体业务问题往往具备更强的应对能力。然而，在严格的科层化管理体系中，一线员工处理问题的自由度受到限制，这不仅抑制了他们解决问题的积极性，也削弱了他们的应变灵活性。因此，科层化管理带来的规范化与员工决策灵活性之间存在固有的矛盾。过去，许多企业试图通过企业文化来调和这一矛盾。例如，Netflix 等公司提倡一种“高赋权、高对齐”的团队文化，旨在通过企业文化的影响，使员工在维护企业整体利益的同时发挥个人主观能动性。然而，这种依赖企业文化的方法在实际操作中面临诸多挑战和局限。在应用AI智能体后，上述管理中的固有矛盾有望得到有效缓解。员工能够在工作中根据具体情境自主选择最优决策方案，而AI智能体则实时监控其行为，确保这些行为与企业核心利益相一致。一旦检测到潜在偏离行为，AI智能体会立即向员工提供反馈或警告，使员工能够迅速调整行为。通过这一机制，传统企业中繁琐的纵向沟通流程得以重构为员工与AI智能体之间的实时交互模式，从而在提升决策效率的同时，扩展了员工的决策权限。

此外，AI智能体的应用还可能促进团队自治，并增强企业内部跨部门间的协作。在传统的科层化管理中，跨部门合作往往面临诸多障碍。例如，当不同职能部门的一线业务单位识别到合作机会时，员工通常需要将合作意向上报至各自上级部门，经过高层协调后才能决定是否实施。这种做法不仅降低了决策效率，还可能导致错失商业机遇。在采用AI智能体的企业中，各业务单位可以直接通过企业的AI智能体进行沟通和协作。AI智能体能够帮助他们高效完成复杂的合规流程，显著提升决策速度和执行效率。这不仅减少了中间环节的时间消耗，也使得企业在AI智能体的支持下实现了高度自治和自组织，从而极大地提升了组织运作和创新的效率。

（四）员工角色的变化

AI智能体的应用不仅将重塑企业的规模、组织结构和决策层次，还将深刻影响企业内部人员的角色定位和技能需求。一方面，员工的职责将发生显著变化。随着AI智能体承担起大量事务性和监控性任务，员工的工作重心将转向战略规划、人际沟通和创造性思维等目前AI智能体尚难以替代的领域。当前已有部分企业开始将员工角色重新定义为与AI协作的增效者，强调员工应掌握使用AI工具的能力，并将其视为工作伙伴而非竞争者。例如，Salesforce 等公司提出了“数字同事”概念，为每位员工配备一个AI助手，以协助其完成重复性工作，使其专注于更具价值和创造性的任务。这一趋势体现了员工角色从传统亲历执行模式向人机协同范式的转型。另一方面，随着AI智能体在企业中的深度应用，一系列与AI智能体相关的新岗位也将应运而生。未来，诸如机器训练师、AI伦理官和数据策展人等新兴职业将在组织中扮演关键角色。这些岗位的主要职责包括提升AI智能体的效能、确保其行为符合伦理规范，以及弥补AI智能体在理解人类价值观与社会互动方面的不足。

（五）企业文化的变化

AI智能体的应用不仅带来了组织结构和 workflows 的调整，也对企业文化提出了新的变革要求。AI智能体驱动的企业转型不仅是技术和制度层面的演进，而且涉及员工观念和行为模式的重塑。企业必须营造一种能够接纳且积极运用AI技术的文化氛围，同时适应日益扁平化、高自主性的工作模式。这种新型企业文化需要引导员工从传统的“听从上级指令”转向“与AI协作、自主决策”的思维模式，并围绕这一理念构建全新的激励机制和心理安全体系，以支持员工在人机协同环境下高效工作和持续发展。

值得注意的是，实现这种文化转型并非易事。若处理不当，可能引发员工对AI智能体的不信任甚至抵触情绪，进而阻碍数字化转型的顺利推进。为应对这一挑战，企业在推广AI智能体的过程中应坚持透明性和参与式治理原则。一方面，应向员工清晰说明AI智能体的功能边界、应用场景及其局限性，明确传递“AI不会取代你，而是帮助你”的理念。另一方面，还应设立相应的AI伦理与合规框架，确保其使用过程可控、可解释、可问责，从而增强员工对AI智能体的信任感。在此基础上，企业应采取循序渐进的方式推进文化变革，通过培训、试点项目和反馈机制逐步建立适应人机协作的企业文化。

六、AI智能体对商业模式的影响

在AI智能体的冲击下，许多现有的商业模式将难以适应新的竞争环境，同时一系列全新的商业模式也将应运而生。本文从AI智能体对商业模式构成环节的影响出发，深入分析其可能引发的商业模式变革，探讨企业在智能化趋势下的战略调整方向和创新路径。

（一）商业模式基本要素的变化

商业模式由价值主张、价值创造、价值传递和价值获取等四个关键环节构成^[23-24]。简而言之，价值主张是指企业向顾客提供何种价值，价值创造是指企业及其合作伙伴如何共同创造这些价值，价值传递是指企业如何将这些价值交付给客户，价值获取是指企业如何通过收益机制设计或价值货币化路径实现盈利目标。随着AI智能体的广泛应用，这四个环节均会受到显著影响。

在价值主张环节，AI智能体使得企业能够为用户提供更加精准化和个性化的价值。传统企业的价值主张往往依赖标准化或有限差异化的产品或服务，受限于成本结构等因素，难以满足每位用户的个性化需求。然而，借助AI智能体强大的数据分析能力、决策自主性和个性化推荐功能，企业可以提供高度定制化的产品或服务，从而创造出比传统商业模式更为丰富且贴合个体需求的价值主张。例如，在电子商务领域，传统的统一界面和标准推荐系统正逐渐被个性化的智能助手所取代。每个用户都可能拥有一个专属的“虚拟助理”，“虚拟助理”能精确理解个人偏好，并据此提供定制化服务，实现真正意义上的“千人千面”。

在价值创造环节，AI智能体显著提升了企业的生产效率，并降低了边际成本。一方面，AI智能体具备自主决策的能力，减少了对人类决策者的依赖，从而降低了决策过程中的交易成本。另一方面，AI智能体具备持续学习和自我迭代的能力，能够不断提升生产流程的效率和智能化水平，从而减少浪费、降低成本。因此，企业能够更快速、有效地进行创新，并推出新产品或服务。这种效率的提升使得企业可以持续改善客户体验，甚至以更低的成本提供更高价值的产品。

在价值传递环节，AI智能体彻底颠覆了现有的价值传递方式。传统上，企业通过线性渠道或中间商向终端消费者传递价值，而AI智能体使企业可以直接面向最终用户或与其他合作伙伴直接互动，减少了对中介渠道的依赖。AI智能体具有自主沟通、谈判和交易的能力，使得价值传递过程更加精准、高效且灵活。例如，在金融服务领域，AI智能体能够主动识别用户的投资需求，并实时提供个性化的智能投资建议，替代了传统复杂且高成本的人工服务流程，提升了价值传递的效率。

在价值获取环节，AI智能体深刻改变了企业的盈利模式。在传统的商业模式中，企业主要通过销售产品或服务来获取收入，或者依靠订阅模式获得持续收益。然而，AI智能体的高度互动性和自主决策能力为企业探索更为灵活和多元的盈利方式提供了可能。例如，基于用户实际使用效果的收费模式，或是基于AI智能体生成的数据与洞见构建增值服务等新型商业模式，都可以为企业开辟新的利润来源。此外，AI智能体的决策和行动自主性还催生了更为复杂和精细的收益共享机制，如动态佣金和成果共享等模式，未来这些都可能成为企业的新盈利模式。

（二）可能受到冲击的商业模式

在智能体经济中，现有的商业模式可能会遭受剧烈冲击。有五类商业模式可能面临极大的挑战。

第一类是以信息不对称或市场中介地位为基础构建的商业模式。在当前的市场环境中，许多商业模式依赖信息优势或渠道控制实现盈利，如房产中介、金融中介和物流中介等。然而，随着AI智能体的应用，信息不对称程度大幅降低，市场透明度显著提高，中介作用不断减弱。AI智能体能够通过智能体网络自主完成全网范围内的信息搜寻，并与其他AI智能体直接进行交易。在这种情况下，中介模式可能会被完全替代，供需双方可以直接通过AI智能体实现对接。值得注意的是，在当前的市场环境中，占据核心地位的平台模式在本质上也是中介模式的一种延伸。因此，AI智能体的兴起同样对平台模式构成巨大威胁。为了获取高额的交易抽成，现有平台企业通常会采用技术和规则构建“围墙花园”，限制用户的选择权，并锁定其商业生态系统内的用户群体，这不仅限制了用户的自由选择，也降低了交易效率和分工效益。随着AI智能体的发展，“技术封建主义”将被打破，纯粹作为交易中介的平台模式或将走向衰落。为维持市场竞争力，现有平台需向服务支持型角色转型。以在线旅行（Online Travel Agent, OTA）平台为例^[25]，在现有商业模式下，OTA平台的主要功能是“比价+下单”。在智能体经济时代，这类平台若要持续生存和发展，必须转型成为“旅行服务供应链”的调度者和协同者，并积极构建“旅行即服务”（Travel-as-a-Service, TaaS）的基本架构。这意味着这类平台需为用户提供结构清晰、可用性高的服务资源应用程序接口（API），设计标准化的智能代理协议接口，以支持多方AI智能体间的顺利对接。

第二类是基于注意力的商业模式。注意力是一种稀缺资源，注意力往往能够转化为消费行为。因此，在当前的市场环境中，用户注意力成为企业竞争的关键资源。围绕注意力发展出了多种商业模式^[26]。例如，网页位置的竞价排名，其实质是对更能吸引注意力的位置进行拍卖；社交平台则通过社交活动吸引用户注意力，并通过其他渠道变现。然而，随着AI智能体的广泛应用，这些模式可能会遭受重创。由于AI智能体可以低成本地完成全网搜索，并根据用户需求精准定位最适合的产品或服务，用户注意力与购买决策之间的关联将被显著弱化。在这种情况下，即使企业占据了大量用户注意力，也难以将其直接转化为经济效益。

第三类是基于定向推送的商业模式。近年来，基于用户个人数据的定向推送催生了众多新型商业模式。一些企业直接根据消费者的偏好数据向其推送可能感兴趣的产品；另一些企业则通过定向推送用户喜欢的内容来吸引注意力，随后通过广告等方式变现。这类商业模式的迅速发展促使许多企业加大了对用户数据的收集力度，进而引发了一系列隐私和个人数据保护的问题。在智能体经济时代，这种商业模式也将受到冲击。借助AI智能体，消费者对产品或服务的搜索将变得更加主动，从而大幅削弱定向推送的变现能力。这将导致企业搜集用户个人数据的动力减弱，用户个人数据的价值也会相应下降。当然，这并不意味着数据要素会完全失去价值，真正有价值的将是那些结构化程度高、可用于训练AI模型的数据，而非仅用于推断用户偏好的个人数据。

第四类是高度依赖标准化产品和大规模生产的传统制造模式。在当前的市场环境中，针对用户需求进行个性化定制的成本较高，主要原因有两点：一是识别用户需求较为困难；二是非标准化产品的生产难以发挥规模经济效应，成本控制难度较大。然而，AI智能体的应用不仅使用户能够更便捷地传递其确切需求，而且使灵活制造成为可能。这将促进个性化定制和灵活制造的发展，造成传统的标准化和大规模制造模式面临衰落风险。

第五类是以传统劳动密集型服务为主的商业模式。由于AI智能体能够高效、低成本地替代人类完成大量工作，原本高度依赖人类的服务领域，如客服、保险销售、金融咨询、法律咨询和医疗诊断等都将受到巨大冲击。需要重新构建与这些领域相关的商业模式，以适应新的技术环

境。这不仅涉及业务流程的调整，还要求企业在组织结构和技术应用上进行相应的变革，以保持竞争力。

（三）可能兴起的新商业模式

伴随着智能体经济的兴起，大量新型商业模式也将随之涌现。以下四类商业模式尤其值得关注。

第一类是个性化智能助手模式。在这种模式下，企业向用户提供高度定制化且实时互动的智能助理服务，涵盖生活、娱乐、健康、教育和理财等多个领域，形成所谓的“私人智能代理”产业。企业收入变现路径不仅包括用户付费模式，还涵盖平台运营服务、数据分析服务和广告投放等多元渠道。

第二类是生态网络模式。如前所述，AI智能体具备跨域自主协作的能力，使得不同产业中的AI智能体能够快速有效地构建协作网络，即所谓的A2A网络。在这种背景下，如果企业能够成为这一网络的组织者和运营者，则可以通过生态治理、标准制定、数据和基础AI服务等方式获取收入。例如，Google公司正在推动基于A2A协议的智能生态系统建设，Microsoft公司也宣布支持MCP协议和A2A协议，并积极促进与这些开放协议的合作，这些都是为布局生态网络模式所进行的努力。

第三类是AI智能体驱动的按效果付费模式。基于AI智能体精准的决策能力，这种模式允许企业提供以效果为导向的收费方案。例如，在营销领域，企业可以设定为仅当AI智能体产生实际销售收入或显著成效时才对客户收费；在医疗领域，用户可以在AI智能体提供准确的诊疗建议后才支付费用。这种模式不仅能降低客户获取服务的门槛，还能显著提高企业的竞争优势和客户忠诚度。

第四类是智能决策即服务（Decision-as-a-Service，DaaS）模式。DaaS模式是对现有云计算服务的一种升级。在此模式下，AI智能体的决策能力被封装成独立的产品，供企业和个人使用。这使得缺乏先进AI技术的中小企业能够以较低成本获得高效的决策支持服务，从而迅速提升其决策效率。对于提供DaaS服务的技术供应商而言，这也意味着其可以获得稳定的收入来源。

七、AI智能体蕴含的挑战及其应对

尽管AI智能体能够为企业带来诸多益处，但其广泛应用也必然伴随一系列挑战和潜在风险。企业在积极应用AI智能体的同时，必须正视且妥善应对的问题主要包括：隐私与数据安全、决策失控与错误风险、过度依赖与技能弱化、就业影响与组织变革阻力，以及合规与监管挑战等。

（一）隐私与数据安全

AI智能体的应用在一定程度上削弱了企业，尤其是平台型企业搜集用户个人数据的动机，从而有助于减少隐私泄露和数据滥用等问题。然而，AI智能体在执行智能决策的过程中通常需要访问和处理大量企业内部数据乃至用户个人数据，这在客观上增加了敏感信息的暴露风险。更令人担忧的是，许多支持AI智能体运行的模型部署在云端，这意味着大量敏感数据将在网络环境中频繁传输，传统的本地化数据安全保障机制可能由此失效。一旦AI智能体遭遇外部攻击、被恶意操控或用户使用不当，就可能导致大规模的数据泄露事件，甚至对企业的运营安全和用户权益造成严重影响。

为应对上述挑战，企业在部署AI智能体时应采取严格的访问控制、加密传输和实时监控等安全措施。例如，可以对AI智能体的数据访问权限进行精细化管理，仅授权其完成任务所必需的数据；对涉及敏感操作的行为引入多重验证机制；对智能体请求的数据进行模糊化或差分隐私处理，以降低泄露风险。此外，在选择云服务供应商时，企业应重点评估其安全合规能力，并对上传至云端的数据实施脱敏或加密处理。与此同时，企业还应建立健全数据使用审计机制，详细

记录每个AI智能体在何时、何种条件下访问了哪些数据，以便事后追溯和责任认定。唯有在有效解决隐私和安全问题的前提下，企业才能放心地将关键业务流程交由AI智能体处理，用户也才能真正信任这些智能助手不会滥用其个人信息。

（二）决策失控与错误风险

AI智能体在执行现实任务中的自主行动也可能遭遇决策失误或行为失控的风险。由于训练数据偏差或推理局限，AI智能体可能会作出不合理甚至有害的决策。例如，采购AI智能体可能因误判市场行情而下达过多订单，导致库存积压；理财AI智能体则可能因模型偏差推荐不适当的投资产品。更为严重的是，完全自主的AI智能体可能以人类无法预料的方式解决问题，从而引发灾难性后果。例如，自动驾驶汽车在复杂环境下可能作出危险操作，企业内部使用的AI智能体也可能违反业务规则进行操作而造成损失。

为应对上述风险，企业应为AI智能体设定明确的行为边界，并实施严格的监控措施。在战略规划阶段，应明确规定AI智能体的操作权限，并列出需要人工审批的具体情形，确保实际操作符合规划要求。特别是在医疗、航空等关键行业，应始终保持人在环中（Human-in-the-Loop）的原则，即所有关键决策必须经过人工确认。对于之前未曾由AI智能体执行的任务，应在通过沙盒测试和阶段性验证后，才交由AI智能体处理。此外，企业还应建立应对最坏情况的“熔断”机制。当检测到AI智能体连续出现异常决策时，系统应能自动暂停运行，并通知相关人员介入处理。这不仅有助于及时纠正错误，还能防止潜在的大规模损害。总而言之，让AI智能体实现自治并不意味着对其放任自流。企业在应用AI智能体的过程中，必须通过技术与管理手段相结合的方式，确保其始终在可控范围内运行，最大限度地降低错误和失控的风险。这种综合性的风险管理策略是保障AI智能体可持续发展的重要前提。

（三）过度依赖与技能弱化

随着AI智能体广泛接管各类工作任务，组织和员工可能对其产生过度依赖，进而导致员工技能的退化和应对风险能力的下降。若员工将所有决策任务交由AI智能体完成，长期来看，其自身的判断力和创新力可能会被削弱。一旦AI智能体出现故障或面临未曾训练过的复杂情境时，员工可能不具备有效接管和应对的能力。这一现象在其他高度自动化领域中已有先例。例如，在航空领域的自动化驾驶舱中，由于长期依赖自动化系统，操作人员的手动操作能力逐渐退化，面对突发状况时反应迟缓甚至失误频发。因此，在企业管理实践中，也必须对类似问题保持高度警惕。此外，“知识遗忘”是另一项不容忽视的风险。如果一线员工完全依赖AI智能体处理客户咨询等事务，则业务知识和经验可能逐步集中于AI智能体中，而员工对业务知识和经验的学习积累则呈现减弱趋势。这不仅削弱了员工的职业发展能力，也可能降低企业在缺乏AI智能体支持时的应急响应能力。

为应对此类挑战，企业应倡导“人机共训”的理念，推动AI智能体与员工在工作过程中协同学习、共同提升，而非以技术替代人力学习的过程。具体而言，企业应鼓励员工主动质疑AI智能体所提出的建议，理解其背后的逻辑，从而提升自身的分析和判断能力。与此同时，应安排员工在有AI智能体支持与无AI智能体支持的工作岗位之间定期轮换，以确保其在不同环境下均具备独立工作的能力。此外，企业还应建立关键业务知识的人工记录机制，避免所有业务知识仅存储于AI智能体中，从而保障业务知识的可持续传承。在绩效考核体系中，也应加强对员工洞察力和创造力的评估，防止其因过度依赖AI智能体而减少主动思考。通过上述措施，企业不仅能够借助AI智能体提升运营效率，还能在技术赋能的同时维持人力资本的持续积累和长期发展，从而实现人机协同下的高质量组织演进。

（四）就业影响与组织变革阻力

AI智能体的大规模应用不可避免地会对劳动力市场和企业内部的就业结构产生深远影响。

对企业而言，这种变革不仅可能引发员工对岗位稳定性的担忧，降低其工作积极性，还可能在组织内部形成对AI智能体推广的阻力，从而影响AI智能体的顺利落地和有效应用。

面对这一挑战，企业在推进AI智能体部署的过程中，应明确传达“AI帮助人”而非“AI替代人”的核心理念。具体而言，在应用AI智能体之前，企业应通过透明、系统的沟通机制，向全体员工阐明AI智能体战略的目标和路径，强调AI智能体的定位是辅助员工提升效率，而非取代人力。在实施阶段，企业可以优先选择对AI智能体接受度较高的团队作为试点，通过实际应用成效树立成功案例，为后续推广积累经验和信心。与此同时，在全面推行过程中，企业应建立畅通的反馈机制，积极倾听员工对AI智能体使用的意见和建议，并对出现的问题进行及时调整和优化，以增强员工的参与感和认同感。

综上所述，企业应致力于引导员工与AI智能体之间建立一种协同共赢的关系，而非对立冲突的关系。唯有如此，才能实现AI技术与人力资源的深度融合，真正释放AI智能体在提升组织效能和创新能力方面的潜力。

（五）合规与监管挑战

AI智能体作为新兴技术，其相关的监管和法律框架仍在不断发展和完善中，许多规则仍处于模糊地带，这给企业的合规管理带来了挑战。企业在应用AI智能体时可能面临多种合规问题，如数据保护合规、特定行业的法规遵循，这些构成了企业运营的重大约束。更为复杂的是，不同国家或地区针对AI智能体的法律法规存在显著差异。由于AI智能体的运作可能涉及多个国家或地区，企业必须同时应对各地迥异的法律要求。例如，一家中国企业开发的AI智能体若被欧洲用户使用，则该企业不仅需遵守中国法律，还需确保符合欧盟的《通用数据保护条例》（General Data Protection Regulation, GDPR）和将在2026年8月1日全面实施的《人工智能法案》（Artificial Intelligence Act, AI Act）的要求。在这种情况下，若企业未能根据相关国家或地区的要求进行合规操作，将面临严重的法律风险。

为了规避此类合规风险，企业应采取以下措施。首先，企业应及时跟踪相关国家或地区的立法动态和执法趋势，并据此制定和调整自身的合规策略。其次，在企业内部，应定期评估AI智能体的行为是否符合法律和道德标准，识别潜在的偏离风险，并保存详细的记录，以备监管审查。最后，企业还应积极与监管部门沟通合作，参与行业自律组织，共同制定使用AI智能体的指导原则，以防范个别市场主体的滥用行为引发行业整体性监管限制。通过上述措施，企业能够在充分把握AI智能体所带来的发展机遇的同时，有效防控法律风险，确保其在复杂的国际法规环境中稳健运营。这种前瞻性的合规管理不仅是企业可持续发展的保障，也是构建负责任企业形象的关键步骤。

八、结 语

AI智能体的兴起不仅为全社会带来了显著的效率提升，还将重塑整个商业世界。为了在这场智能革命中保持竞争力，并实现长期价值增长和分配优化，企业管理者需主动适应由AI智能体引发的变化，在战略规划、组织结构、业务创新和合规管理等方面提前布局，做好充分准备。与此同时，AI智能体的广泛应用也为经济学和管理学理论研究提供了丰富的素材。例如，相较于人类代理，AI智能体作为新型代理人具有哪些独特之处？它们如何影响委托—代理关系？AI智能体的应用将如何重新定义企业的边界，并对企业间的关系产生何种影响？在智能体经济背景下，传统的战略理论和组织理论应如何调整以应对新的现实问题？商业模式又该如何设计才能更好地利用AI技术的优势？可以预见，这些问题将成为未来一段时间学术界、产业界和政策制定者共同关注的焦点。随着AI智能体技术的不断进步及其应用范围的扩大，相关领域的研究将更加深入，有助于推动理论和实践的协同发展，从而促进社会经济的整体进步。

参考文献:

- [1] 陈永伟.超越 ChatGPT:生成式 AI 的机遇、风险与挑战[J].山东大学学报(哲学社会科学版),2023(3):127-143.
- [2] 陈永伟.从规模定律到规模经济:DeepSeek 的创新、机遇与挑战[J/OL].山东大学学报(哲学社会科学版),(2025-03-19)[2025-06-03].<http://kns.cnki.net/kcms/detail/37.1100.C.20250318.1553.002.html>.
- [3] CUNTZ A, FINK C, STAMM H. Artificial intelligence and intellectual property: an economic perspective [R]. World Intellectual Property Organization, 2024.
- [4] MCGRATH Q. Technology trends to watch in 2025 [R]. SIM Research Institute, 2024.
- [5] GenAI: the path forward [R]. Avity Investment Management Inc., 2025.
- [6] ROTHSCCHILD D M, MOBIUS M, HOFMAN J M, et al. The agentic economy [J/OL]. arXiv, (2025-05-29)[2025-06-03]. <https://arxiv.org/abs/2505.15799>.
- [7] SAPKOTA R, ROUMELIOTIS K, KARKEE M. AI agents vs. agentic AI: a conceptual taxonomy, applications and challenges [J/OL]. arXiv, (2025-05-15)[2025-06-03]. <https://arxiv.org/html/2505.10468v1>.
- [8] World Economic Forum. Navigating the AI frontier: a primer on the evolution and impact of AI agents [R]. World Economic Forum White Paper, 2024.
- [9] World Economic Forum. Frontier technologies in industrial operations: the rise of artificial intelligence agents [R]. World Economic Forum White Paper, 2025.
- [10] PARK J, O'BRIEN J, CAI C, et al. Generative agents: interactive simulacra of human behavior [R]. Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology, 2023.
- [11] BRUDENELL D. The three eras of the agentic web [EB/OL]. (2024-10-10)[2025-06-03]. <https://www.decidr.ai/blog/the-three-eras-of-the-agentic-web>.
- [12] 陈永伟.人工智能对齐:经济学可以做什么?[J].东北财经大学学报,2024(4):37-52.
- [13] 侯宏.智能体经济战略前瞻:颠覆与新生[EB/OL]. (2025-04-06)[2025-06-03]. <https://mp.weixin.qq.com/s/HfxG8co4Kl5qNK4wkiMkQ>.
- [14] KIM J. Rise of the A2A economy: how AI agent-to-agent interactions will reshape the world [EB/OL]. (2025-01-18)[2025-06-03]. <https://sendbird.com/blog/ai-agent-to-agent-economy>.
- [15] ROCHET J, TIROLE J. Two-sided markets: a progress report [J]. The Rand journal of economics, 2006, 37(3): 645-667.
- [16] ARMSTRONG M. Competition in two-sided markets [J]. The Rand journal of economics, 2006, 37(3): 668-691.
- [17] 塞德里克·迪朗.技术封建主义[M].陈荣钢,译.北京:中国人民大学出版社,2024:146-192.
- [18] ADNER R. Ecosystem as structure: an actionable construct for strategy [J]. Journal of management, 2017, 43(1): 39-58.
- [19] 陈永伟.平台反垄断问题再思考:“企业—市场二重性”视角的分析[J].竞争政策研究,2018(5):25-34.
- [20] COASE R. The nature of the firm [J]. Economica, 1937, 4(16): 386-405.
- [21] 曾鸣.黑洞效应是 AI 时代的价值源泉 [EB/OL]. (2025-05-06)[2025-06-03]. <https://finance.sina.com.cn/wm/2025-05-06/doc-inevrvkw2020063.shtml>.
- [22] HAYEK F. The use of knowledge in society [J]. The American economic review, 1945, 35(4): 519-530.
- [23] ZOTT C, AMIT R, MASSA L. The business model: recent developments and future research [J]. Journal of management, 2011, 37(4): 1019-1042.
- [24] TEECE D. Business models, business strategy and innovation [J]. Long range planning, 2010, 43(2-3): 72-194.
- [25] 陈谦磊.从平台经济到“A2A 经济”:AI 时代的商业模式跃迁 [EB/OL]. (2025-05-29)[2025-06-03]. https://mp.weixin.qq.com/s/IDa-sq7DMLB_zRSzJVwjaA.
- [26] HENDRICKS V, VESTERGAARD M. Reality lost: markets of attention, misinformation and manipulation [M]. London: Springer Open, 2019: 1-17.

The Rise of Agentic Economy: How AI Agents Reshape the Business World

CHEN Yongwei

(Research Department, Journal of Comparative Studies, Beijing 100029, China)

Summary: This paper systematically explores the impact of AI agents on the business landscape. It defines AI agents as autonomous AI systems capable of planning and executing actions, distinguishing them from conventional AI through features like proactivity, adaptability, and self-learning. Categorized by decision-making patterns (deterministic vs. non-deterministic) and physical form (virtual vs. embodied), AI agents leverage components such as sensors, control centers, and effectors to interact with environments, supported by open-source protocols (e. g., MCP, ANP, and A2A) for tool integration and inter-agent collaboration.

Economically, AI agents represent a new type of economic participant with distinct characteristics: principal-agent dynamics shift as agents act as human surrogates, raising challenges in aligning AI utilities with human values; cost structures exhibit near-zero marginal costs, enabling mass replication and disrupting platform-based intermediaries; network effects are open and user-centric, contrasting with the closed ecosystems of conventional platforms, potentially empowering users to bypass intermediaries. For business ecosystems, AI agents redefine participant roles. Conventional platforms may decline as agents enable peer-to-peer transactions, while new players like AI consultants and data brokers emerge. Ecological division of labor becomes more granular, with AI streamlining supply chains and reducing transaction costs, fostering specialized micro-enterprises. Power dynamics shift, as incumbents may strengthen their dominance through AI capabilities, while open standards can empower smaller players. Governance challenges arise from multi-principal conflicts and algorithmic collusion, necessitating AI governance frameworks.

Within enterprises, AI agents drive organizational transformation: scale polarization occurs as firms may become “large and flat” (controlling vast resources with few employees) or “one-person companies” via outsourcing; flattened hierarchies reduce middle management roles, with AI handling information aggregation and performance evaluation; decentralized decision-making empowers frontline employees, monitored by AI to ensure alignment with corporate goals; role redefinition shifts human focus to strategic and creative tasks, accompanied by new roles like AI ethics officers; cultural adaptation requires fostering trust in human-AI collaboration and addressing resistance to change. Business model disruptions include: decline of intermediary-based, attention-driven, and mass-production models due to AI’s transparency and personalization capabilities; rise of new models such as personalized intelligent assistants, agentic ecosystems, pay-for-performance services, and Decision-as-a-Service (DaaS).

Challenges and mitigations are discussed as follows: privacy risks require strict data access controls and encryption; decision failures demand clear behavioral boundaries and human-in-the-loop mechanisms; over-reliance necessitates “human-AI co-training” to preserve employee skills; employment impacts require transparent communication and pilot programs; regulatory complexities demand compliance with evolving laws across jurisdictions.

Key words: agentic economy; AI agents; business model innovation; corporate organizational change; business ecosystem

(责任编辑: 邓 菁)

[DOI]10.19654/j.cnki.cjwtyj.2025.07.002

[引用格式]陈永伟. 智能体经济的崛起: AI智能体对商业世界的重塑[J]. 财经问题研究, 2025(7): 15-31.