

# AI Agent: 基于大模型的自主智能体, 在探索 AGI 的道路上前进

## 核心观点

- **AI Agent (人工智能代理)** 是一种能够感知环境、进行决策和执行动作的智能实体。不同于传统的人工智能, AI Agent 具备通过独立思考、调用工具去逐步完成给定目标的能力。AI Agent 和大模型的区别在于, 大模型与人类之间的交互是基于 prompt 实现的, 用户 prompt 是否清晰明确会影响大模型回答的效果。而 AI Agent 的工作仅需给定一个目标, 它就能够针对目标独立思考并做出行动。和传统的 RPA 相比, RPA 只能在给定的情况条件下, 根据程序内预设好的流程来进行工作的处理, 而 AI Agent 则可以通过和环境进行交互, 感知信息并做出对应的思考和行动。
- **大语言模型的浪潮推动了 AI Agent 相关研究快速发展, AI Agent 是当前通往 AGI 的主要探索路线。**大模型庞大的训练数据集中包含了大量人类行为数据, 为模拟类人的交互打下了坚实基础; 另一方面, 随着模型规模不断增大, 大模型涌现出了上下文学习能力、推理能力、思维链等类似人类思考方式的多种能力。将大模型作为 AI Agent 的核心大脑, 就可以实现以往难以实现的将复杂问题拆解成可实现的子任务、类人的自然语言交互等能力。由于大模型仍存在大量的问题如幻觉、上下文容量限制等, 通过让大模型借助一个或多个 Agent 的能力, 构建成为具备自主思考决策和执行能力的智能体, 成为了当前通往 AGI 的主要研究方向。
- **一个基于大模型的 AI Agent 系统可以拆分为大模型、规划、记忆与工具使用四个组件部分。**AI Agent 可能会成为新时代的开端, 其基础架构可以简单划分为 Agent = LLM + 规划技能 + 记忆 + 工具使用, 其中 LLM 扮演了 Agent 的“大脑”, 在这个系统中提供推理、规划等能力。
- **AI Agent 发展迅速, 出现多款“出圈”级研究成果。**2023 年 3 月起, AI Agent 领域迎来了第一次“出圈”, 西部世界小镇、BabyAGI、AutoGPT 等多款重大 Agent 研究项目均在短短两周内陆续上线, 引发了大家对 AI Agent 领域的关注。目前已经涌现了在游戏领域大放异彩的英伟达 Voyager 智能体、能够帮助个人完成简单任务的 Agent 助理 HyperWrite、以及主打个人情感陪伴的 AI 助理 Pi 等多款优秀的 Agent 成果, AI Agent 的研究进展迅速。
- **“Agent+”有望成为未来产品的主流, 有望在多个领域实现落地应用。**我们认为, AI Agent 的研究是人类不断探索接近 AGI 的过程, 随着 Agent 变得越来越“可用”和“好用”, “Agent+”的产品将会越来越多, 未来将有望成为 AI 应用层的基本架构, 包括 to C、to B 产品等。
- **2B 和垂直领域仍是 AI Agents 容易率先落地的方向, 用户对 Agent 的认知正在形成, 初创企业正在卡位。**由于 Agent 对环境反馈的依赖性较强, 具备显著特点的企业环境是更加适合 Agent 建立起对某一个垂直领域认知的场景。当前关于 AI Agent 的研究主要还是以学术界和开发者为主, 商业化产品极少, 但是用户对于 Agent 的关注度正在提升, 可能未来几年间就会涌现出大量以 Agent 作为核心的产品应用到各行各业。目前, 已经有一些初创公司开始以企业的智能体平台作为主要的产品研发方向, 例如澜码科技正在打造基于 LLM 的企业级 Agent 平台。

## 投资建议与投资标的

我们认为, 未来几年是 AI Agent 的快速发展窗口期, 具备底层大模型算法技术的公司以及相关的应用软件公司有望基于 AI Agent 实现应用的落地。

- **大模型领域:** 建议关注科大讯飞(002230, 买入)、三六零(601360, 未评级)、拓尔思(300229, 未评级)等公司
- **应用软件领域:** 建议关注金山办公(688111, 增持)、泛微网络(603039, 未评级)、致远互联(688369, 未评级)、彩讯股份(300634, 未评级)、汉得信息(300170, 未评级)、新致软件(688590, 未评级)等公司

## 风险提示

技术落地不及预期; 政策监管风险

行业评级 看好 (维持)

国家/地区 中国  
行业 计算机行业  
报告发布日期 2023 年 08 月 25 日



## 证券分析师

证券分析师 浦俊懿  
021-63325888\*6106  
pujunyi@orientsec.com.cn  
执业证书编号: S0860514050004

证券分析师 陈超  
021-63325888\*3144  
chenchao3@orientsec.com.cn  
执业证书编号: S0860521050002

证券分析师 谢忱  
xiechen@orientsec.com.cn  
执业证书编号: S0860522090004

## 联系人

联系人 杜云飞  
duyunfei@orientsec.com.cn

联系人 覃俊宁  
qinjunning@orientsec.com.cn

联系人 宋鑫宇  
songxinyu@orientsec.com.cn

## 目录

一、AI Agent: 探索 AGI 的真实形态.....	5
1.1 什么是 AI Agent? .....	5
1.2 Agent 的最终发展目标: 通用人工智能 AGI.....	6
二、AI Agent 拆解: 大模型、规划、记忆与工具.....	8
2.1 大模型+规划: Agent 的“大脑”, 通过思维链能力实现任务分解 .....	9
2.2 记忆: 用有限的上下文长度实现更多的记忆.....	10
2.3 工具: 懂得使用工具才会更像人类 .....	11
三、AI Agent 研究与应用进展 .....	13
3.1 AutoGPT: 推动 AI Agent 研究热潮 .....	13
3.2 游戏领域应用: 西部世界小镇与我的世界 .....	14
3.3 HyperWrite: 推出首个人工 AI 助理 Agent .....	17
3.4 ModelScopeGPT: 国内首个大模型调用工具.....	18
3.5 Inflection AI: 高情商个人 AI——Pi .....	19
3.6 AgentBench: LLM 的 Agent 能力评估标准 .....	20
四、“Agent+”有望成为未来 AI 领域产品主流 .....	21
4.1 AI Agent 有望多个领域实现落地应用 .....	21
4.2 2B+垂类 Agent 认知正在形成, 有望率先落地.....	23
投资建议与投资标的 .....	24
风险提示.....	24

## 图表目录

图 1: Hyperwrite 研发的 AI Agent 个人助理插件实现自动预订航班机票 .....	5
图 2: AI Agent 的工作流程 .....	5
图 3: AlphaGo 战胜柯洁 .....	6
图 4: OpenAI Five 战胜《Dota 2》世界冠军 .....	6
图 5: 大语言模型浪潮 .....	7
图 6: 大模型的能力涌现现象 .....	7
图 7: 研究 AI Agent 的最终目标是通向 AGI .....	7
图 8: 由 LLM 驱动的自主智能体系统的架构 .....	8
图 9: 通过调整 prompt 可以提升大模型推理效果 .....	9
图 10: AI Agent 的反思框架 .....	9
图 11: 人类记忆的分类 .....	10
图 12: 非结构化数据的向量化表征 .....	11
图 13: 不同文本在向量空间中的相似度计算 .....	11
图 14: GPT 模型函数调用功能示例 .....	11
图 15: HuggingGPT 的工作步骤流程 .....	12
图 16: AI Agents 领域动态 .....	13
图 17: AutoGPT 在 GitHub 的星数增长 .....	13
图 18: AutoGPT 可以实现自主分析浏览器页面 .....	13
图 19: 基于 AutoGPT 完成网站建设 .....	14
图 20: 网页版 AgentGPT .....	14
图 21: GPT-4 和 GPT-3.5 的 API 价格 .....	14
图 22: AutoGPT 陷入死循环 .....	14
图 23: 斯坦福学者打造的西部世界小镇 .....	15
图 24: 西部世界小镇中 Agents 的架构 .....	15
图 25: 记忆流包含大量的观察、检索过程 .....	15
图 26: 英伟达打造 Voyager 智能体游玩《我的世界》 .....	16
图 27: Voyager 玩游戏的水平相比之前的方法大幅提升 .....	16
图 28: Voyager 由三大新型组件组成 .....	16
图 29: Voyager 的科技树解锁速度最快 .....	17
图 30: Voyager 的探索范围远大于其他 Agent 框架 .....	17
图 31: HyperWrite 推出个人 AI 助理 Personal Assistant .....	17
图 32: HyperWrite Personal Assistant 交互界面 .....	18
图 33: HyperWrite Personal Assistant 的思考与执行操作过程 .....	18
图 34: ModelScopeGPT 简介 .....	18

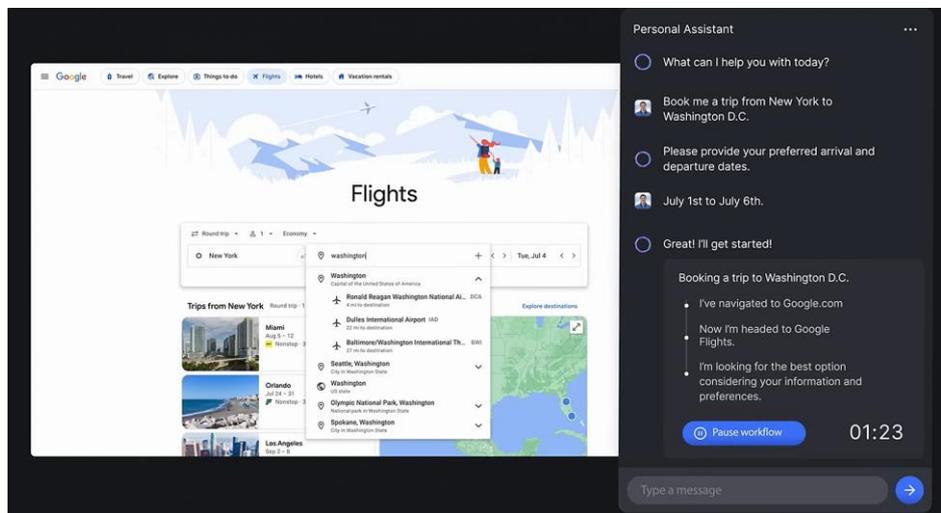
图 35: ModelScopeGPT 演示.....	18
图 36: 阿里云旨在建设中国大模型生态.....	19
图 37: 个人 AI 助理 Pi.....	19
图 38: Inflection-1 可媲美 GPT-3.5 和 LLaMA(65B).....	19
图 39: Pi 的幽默回复.....	20
图 40: Pi 能够提供情感方面的建议.....	20
图 41: AgentBench 评价 LLM 作为 Agent 的能力.....	20
图 42: 常用的 LLM 的 Agent 能力排名.....	20
图 43: Agent 的可能用例.....	21
图 44: GitHub 关于自主代理的项目已经超过 100 个.....	21
图 45: 澜码科技打造企业级 Agent 平台.....	23
表 1: 将 AI 和人类协作的程度类比自动驾驶的不同阶段.....	8
表 2: 人类记忆与 AI Agent 记忆的映射.....	10
表 3: AI Agent 可能的应用领域.....	22

## 一、AI Agent：探索 AGI 的真实形态

### 1.1 什么是 AI Agent?

**AI Agent（人工智能代理）**是一种能够感知环境、进行决策和执行动作的智能实体。不同于传统的人工智能，AI Agent 具备通过独立思考、调用工具去逐步完成给定目标的能力。比如，告诉 AI Agent 帮忙下一份外卖，它就可以直接调用 APP 选择外卖，再调用支付程序下单支付，无需人类去指定每一步的操作。Agent 的概念由 Minsky 在其 1986 年出版的《思维的社会》一书中提出，Minsky 认为社会中的某些个体经过协商之后可求得问题的解，这些个体就是 Agent。他还认为 Agent 应具有社会交互性和智能性。Agent 的概念由此被引入人工智能和计算机领域，并迅速成为研究热点。但苦于数据和算力限制，想要实现真正智能的 AI Agents 缺乏必要的现实条件。

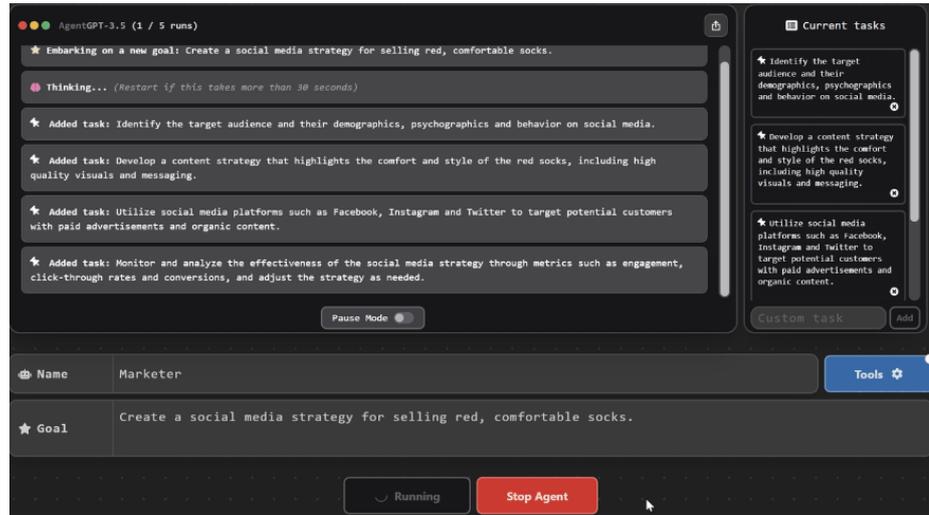
图 1：Hyperwrite 研发的 AI Agent 个人助理插件实现自动预订航班机票



数据来源：Hyperwrite，东方证券研究所

**大语言模型和 AI Agent 的区别**在于 AI Agent 可以独立思考并做出行动，和 RPA 的区别在于它能够处理未知环境信息。ChatGPT 诞生后，AI 从真正意义上具备了和人类进行多轮对话的能力，并且能针对相应问题给出具体回答与建议。随后各个领域的“Copilot”推出，如 Microsoft 365 Copilot、GitHub Copilot、Adobe Firefly 等，让 AI 成为了办公、代码、设计等场景的“智能副驾驶”。AI Agent 和大模型的区别在于，大模型与人类之间的交互是基于 prompt 实现的，用户 prompt 是否清晰明确会影响大模型回答的效果，例如 ChatGPT 和这些 Copilot 都需要明确任务才能得到有用的回答。而 AI Agent 的工作仅需给定一个目标，它能够针对目标独立思考并做出行动，它会根据给定任务详细拆解出每一步的计划步骤，依靠来自外部的反馈和自主思考，自己给自己创建 prompt，来实现目标。如果说 Copilot 是“副驾驶”，那么 Agent 则可以算得上一个初级的“主驾驶”。和传统的 RPA 相比，RPA 只能在给定的情况条件下，根据程序内预设好的流程来进行工作的处理，在出现大量未知信息、难以预测的环境中时，RPA 是无法进行工作的，AI Agent 则可以通过和环境进行交互，感知信息并做出对应的思考和行动。

图 2：AI Agent 的工作流程



数据来源: Zapier, 东方证券研究所

## 1.2 Agent 的最终发展目标: 通用人工智能 AGI

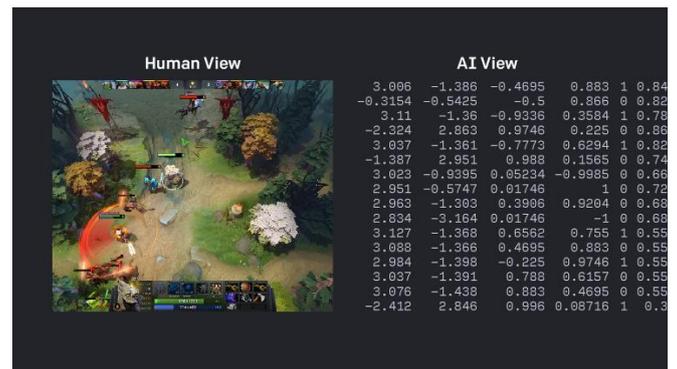
AI Agent 并不是一个新兴的概念, 早在多年前就已在人工智能领域有了研究。例如 2014 年由 DeepMind 推出的引发全球热议的围棋机器人 AlphaGo, 也可以看做是 AI Agent 的一种。与之类似的还有 2017 年 OpenAI 推出的用于玩《Dota2》的 OpenAI Five, 2019 年 DeepMind 公布用于玩《星际争霸 2》的 AlphaStar 等, 这些 AI 都能根据对实时接收到的信息的分析来安排和规划下一步的操作, 均满足 AI Agent 的基本定义。当时的业界潮流是通过强化学习的方法来对 AI Agent 进行训练, 主要应用场景是在游戏这类具有对抗性、有明显输赢双方的场景中。但如果想要在真实世界中实现通用性, 基于当时的技术水平还难以实现。

图 3: AlphaGo 战胜柯洁



数据来源: HardwareZone, 东方证券研究所

图 4: OpenAI Five 战胜《Dota 2》世界冠军



数据来源: OpenAI, 东方证券研究所

大语言模型的浪潮推动了 AI Agent 相关研究快速发展。AI Agent 需要做到能够像人类一样进行交互, 大语言模型强大的能力为 AI Agent 的突破带来了契机。大模型庞大的训练数据集中包含了大量人类行为数据, 为模拟类人的交互打下了坚实基础; 另一方面, 随着模型规模不断增大, 大模型涌现出了上下文学习能力、推理能力、思维链等类似人类思考方式的多种能力。将大模型作为

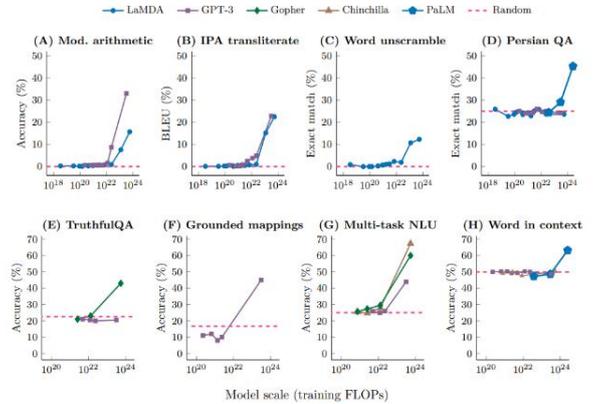
AI Agent 的核心大脑, 就可以实现以往难以实现的将复杂问题拆解成可实现的子任务、类人的自然语言交互等能力。大模型的快速发展大幅推动了 AI Agent 的发展。

图 5: 大语言模型浪潮



数据来源: 东方证券研究所绘制

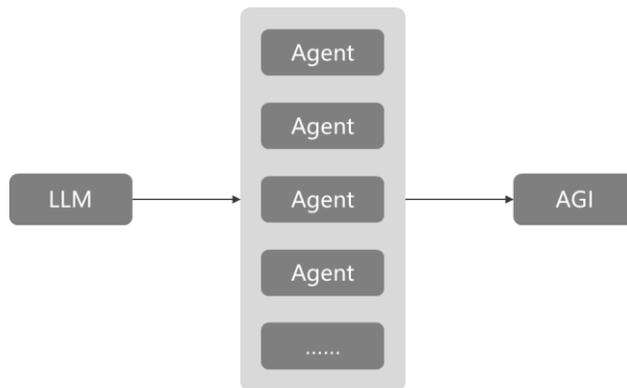
图 6: 大模型的能力涌现现象



数据来源: Wei, et al. 《Emergent Abilities of Large Language Models》, 东方证券研究所

**通往 AGI 的道路仍需探索, AI Agent 是当前的主要路线。**在大模型浪潮席卷全球之时, 很多人认为大模型距离真正的通用人工智能 AGI 已经非常接近, 很多厂商都投入了基础大模型的研究。但经过了一段时间后, 大家对大模型真实的能力边界有了清晰的认知, 发现大模型仍存在大量的问题如幻觉、上下文容量限制等, 导致其无法直接通向 AGI, 于是 AI Agent 成为了新的研究方向。通过让大模型借助一个或多个 Agent 的能力, 构建成为具备自主思考决策和执行能力的智能体, 来继续实现通往 AGI 的道路。OpenAI 联合创始人 Andrej Karpathy 在一次开发者活动中讲到, OpenAI 内部对 AI Agents 非常感兴趣, AI Agent 将是未来 AI 的前沿方向。扎克伯格也在 Meta 的一季度财报电话会上提到, Meta 将会把 AI Agents 介绍给数十亿用户。

图 7: 研究 AI Agent 的最终目标是通向 AGI



数据来源: 东方证券研究所绘制

**AI Agent 可以类比为自动驾驶的 L4 阶段, 距离真正实现仍有差距。**根据甲子光年报告, AI 与人类的协作程度可以和自动驾驶等级进行类比。像 ChatGPT 这类对话机器人可以类比 L2 级别自动驾驶, 人类可以向 AI 寻求意见, 但 AI 不直接参与工作; Copilot 这类副驾驶工具可以类比为 L3 级别的自动驾驶, 人类和 AI 共同协作完成工作, AI 根据 prompt 生成初稿, 人类仅需进行修改调整; 而 Agent 则进一步升级为 L4, 人类给定一个目标, Agent 可以自己完成任务规划、工具调用等。

有关分析师的申明, 见本报告最后部分。其他重要信息披露见分析师申明之后部分, 或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

但就如同 L4 级别的自动驾驶还未真正实现一样，AI Agents 容易想象和演示，却难以实现，AI Agents 的真正应用还在不确定的未来。

表 1：将 AI 和人类协作的程度类比自动驾驶的不同阶段

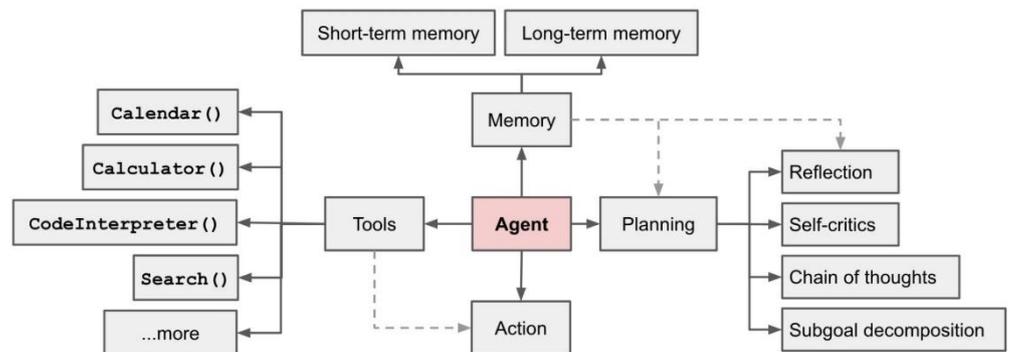
AI 等级 (类比自动驾驶)	名称	特点	示例
L1	Tool	人类完成所有工作，没有任何显性的 AI 辅助	目前绝大多数软件产品
L2	Chatbot	人类完成绝大部分工作。人类向 AI 询问意见，了解信息，AI 提供信息和建议但不直接处理工作	初代 ChatGPT 等 Chatbot
L3	Copilot	人类和 AI 进行协作，工作量相当。AI 根据人类 prompt 完成工作初稿，人类进行目标设定、修改调整，最后确认	GitHub Copilot、Midjourney、Jasper 等
L4	Agent	AI 完成绝大部分工作，人类负责设定目标、提供资源和监督结果。AI 完成任务拆分，工具选择，进度控制，实现目标后自主结束工作	AutoGPT 等
L5	Species	完全无需人类监督，AI 自主拆解目标、寻找资源、选择并使用工具、完成全部工作，人类只需给出目标	机器人？

数据来源：甲子光年，东方证券研究所

## 二、AI Agent 拆解：大模型、规划、记忆与工具

一个基于大模型的 AI Agent 系统可以拆分为大模型、规划、记忆与工具使用四个组件部分。6 月，OpenAI 的应用研究主管 Lilian Weng 撰写了一篇博客，认为 AI Agent 可能会成为新时代的开端。她提出了 Agent = LLM + 规划技能 + 记忆 + 工具使用的基础架构，其中 LLM 扮演了 Agent 的“大脑”，在这个系统中提供推理、规划等能力。

图 8：由 LLM 驱动的自主智能体系统的架构

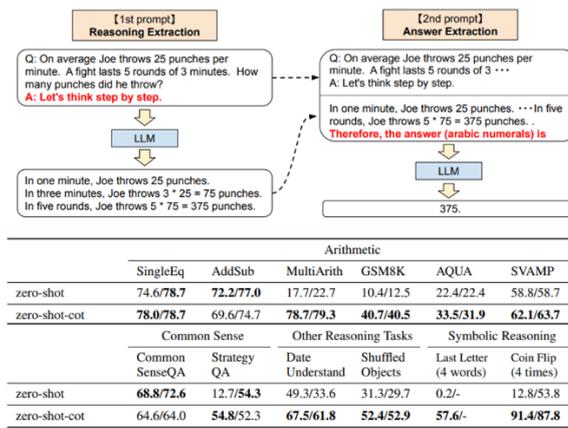


数据来源：Lilian Weng 《LLM Powered Autonomous Agents》，东方证券研究所

## 2.1 大模型+规划：Agent 的“大脑”，通过思维链能力实现任务分解

LLM 具备逻辑推理能力，Agent 可以将 LLM 的逻辑推理能力激发出来。当模型规模足够大的时候，LLM 本身是具备推理能力的。在简单推理问题上，LLM 已经达到了很好的能力；但在复杂推理问题上，LLM 有时还是会出现错误。事实上，很多时候用户无法通过 LLM 获得理想的回答，原因在于 prompt 不够合适，无法激发 LLM 本身的推理能力，通过追加辅助推理的 prompt，可以大幅提升 LLM 的推理效果。在《Large language models are zero-shot reasoners》这篇论文的测试中，在向 LLM 提问的时候追加“Let's think step by step”后，在数学推理测试集 GSM8K 上的推理准确率从 10.4%提升到了 40.7%。而 Agent 作为智能体代理，能够根据给定的目标自己创建合适的 prompt，可以更好地激发大模型的推理能力。

图 9：通过调整 prompt 可以提升大模型推理效果



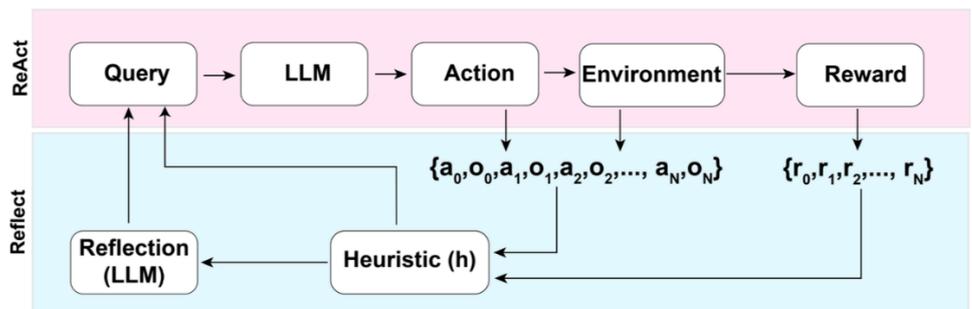
Zero-shot CoT: 例子

Zero-shot CoT: 效果明显提升

数据来源：Kojima, et al. 《Large language models are zero-shot reasoners》，东方证券研究所

对于需要更多步骤的复杂任务，Agent 能够调用 LLM 通过思维链能力实现任务分解与规划。在 AI Agent 的架构中，任务分解规划的过程是基于大模型的能力来实现的。大模型具备思维链（Chain of Thoughts, CoT）能力，通过提示模型“逐步思考”，利用更多的计算时间来将困难任务分解为更小，更简单的步骤，降低每个子任务的规模。

图 10：AI Agent 的反思框架



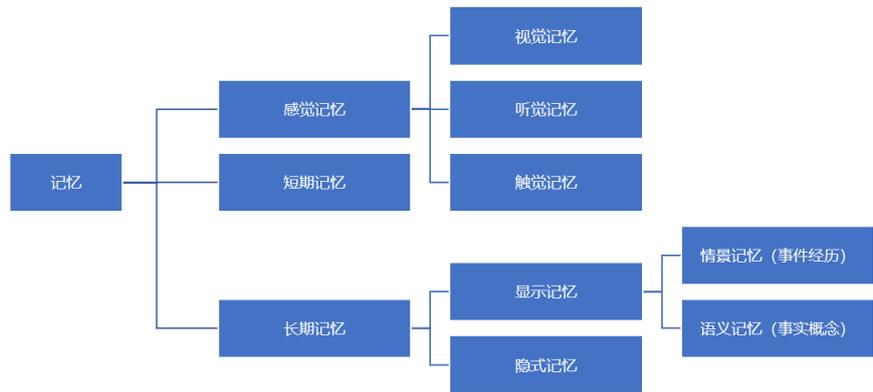
数据来源：Noah, et al. 《Reflection: Language Agents with Verbal Reinforcement Learning》，东方证券研究所

通过反思与自省框架，Agents 可以不断提升任务规划能力。AI Agent 可以对过去的行为进行自我批评和反思，从错误中学习，并为未来的步骤进行完善，从而提高最终结果的质量。自省框架使 Agents 能够修正以往的决策、纠正之前的失误，从而不断优化其性能。在实际任务执行中，尝试和错误是常态，反思和自省两个框架在这个过程中起到了核心作用。

## 2.2 记忆：用有限的上下文长度实现更多的记忆

对 AI 智能体系统的输入会成为系统的记忆，与人类的记忆模式可实现一一映射。记忆可以定义为用于获取、存储、保留以及随后检索信息的过程。人脑中有多种记忆类型，如感觉记忆、短期记忆和长期记忆。而对于 AI Agent 系统而言，用户在其交互过程中产生的内容都可以认为是 Agent 的记忆，和人类记忆的模式能够产生对应关系。感觉记忆就是作为学习嵌入表示的原始输入，包括文本、图像或其他模态；短期记忆就是上下文，受到有限的上下文窗口长度的限制；长期记忆则可以认为是 Agent 在工作时需要查询的外部向量数据库，可通过快速检索进行访问。目前 Agent 主要是利用外部的长期记忆，来完成很多的复杂任务，比如阅读 PDF、联网搜索实时新闻等。任务与结果会储存在记忆模块中，当信息被调用时，储存在记忆中的信息会回到与用户的对话中，由此创造出更加紧密的上下文环境。

图 11：人类记忆的分类



数据来源：Lilian Weng 《LLM Powered Autonomous Agents》，东方证券研究所绘制

表 2：人类记忆与 AI Agent 记忆的映射

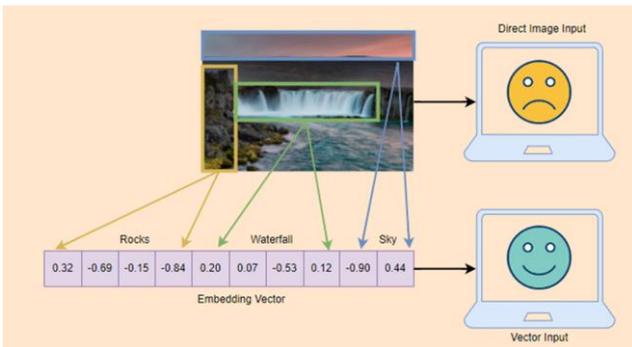
记忆类型	映射	例子
感觉记忆	学习原始输入的嵌入表示，包括文本、图像或其他形式，短暂保留感觉印象。	看一张图片，然后在图片消失后能够在脑海中回想起它的视觉印象。
短期记忆	上下文学习（比如直接写入 prompt 中的信息），处理复杂任务的临时存储空间，受有限的上下文长度限制。	在进行心算时记住几个数字，但短期记忆是有限的，只能暂时保持几个项目。
长期记忆	在查询时 Agent 可以关注的外部向量存储，具有快速检索和基本无限的存储容量。	学会骑自行车后，多年后再次骑起来时仍能掌握这项技能，这要归功于长期记忆的持久存储。

数据来源：东方证券研究所整理

向量数据库通过将数据转化为向量存储，解决大模型海量知识的存储、检索、匹配问题。向量是 AI 理解世界的通用数据形式，大模型需要大量的数据进行训练，以获取丰富的语义和上下文信息，导致了数据量的指数级增长。向量数据库利用人工智能中的 Embedding 方法，将图像、音视频等非结构化数据抽象、转换为多维向量，由此可以结构化地在向量数据库中进行管理，从而实现快速、高效的数据存储和检索过程，赋予了 Agent “长期记忆”。同时，将高维空间中的多模态数据映射到低维空间的向量，也能大幅降低存储和计算的成本，向量数据库的存储成本比存到神经网络的成本要低 2 到 4 个数量级。

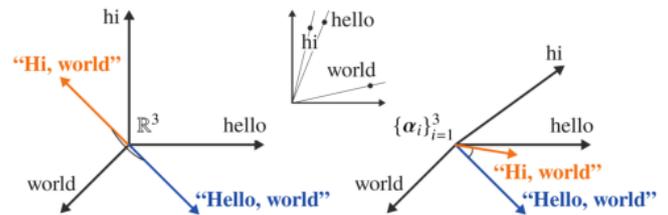
**Embedding 技术和向量相似度计算是向量数据库的核心。** Embedding 技术是一种将图像、音视频等非结构化数据转化为计算机能够识别的语言的方法，例如常见的地图就是对于现实地理的 Embedding，现实的地理地形的信息其实远远超过三维，但是地图通过颜色和等高线等来最大化表现现实的地理信息。在通过 Embedding 技术将非结构化数据例如文本数据转化为向量后，就可以通过数学方法来计算两个向量之间的相似度，即可实现对文本的比较。向量数据库强大的检索功能就是基于向量相似度计算而达成的，通过相似性检索特性，针对相似的问题找出近似匹配的结果，是一种模糊匹配的检索，没有标准的准确答案，进而更高效地支撑更广泛的应用场景。

图 12：非结构化数据的向量化表征



数据来源：ShowMeAI，东方证券研究所

图 13：不同文本在向量空间中的相似度计算

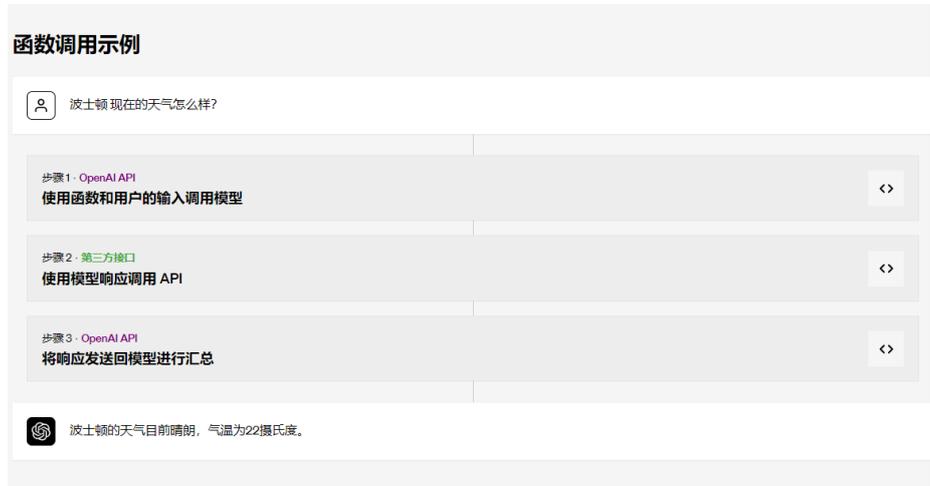


数据来源：墨天轮，东方证券研究所

## 2.3 工具：懂得使用工具才会更像人类

**AI Agent 与大模型的一大区别在于能够使用外部工具拓展模型能力。**懂得使用工具是人类最显著和最独特的地方，同样地，我们也可以为大模型配备外部工具来让模型完成原本无法完成的工作。ChatGPT 的一大缺点在于，其训练数据只截止到了 2021 年底，对于更新一些的知识内容它无法直接做出回答。虽然后续 OpenAI 为 ChatGPT 更新了插件功能，能够调用浏览器插件来访问最新的信息，但是需要用户来针对问题指定是否需要使用插件，无法做到完全自然的回答。AI Agent 则具备了自主调用工具的能力，在获取到每一步子任务的工作后，Agent 都会判断是否需要通过调用外部工具来完成该子任务，并在完成后获取该外部工具返回的信息提供给 LLM，进行下一步子任务的工作。OpenAI 也在 6 月为 GPT-4 和 GPT-3.5 更新了函数调用的功能，开发者现在可以向这两个大模型描述函数，并让模型智能地选择输出包含调用这些函数的参数的 JSON 对象。这是一种更可靠地将 GPT 的功能与外部工具和 API 相连的新方法，允许开发者更可靠地从模型中获得结构化的数据，为 AI 开发者提供了方便。

图 14：GPT 模型函数调用功能示例

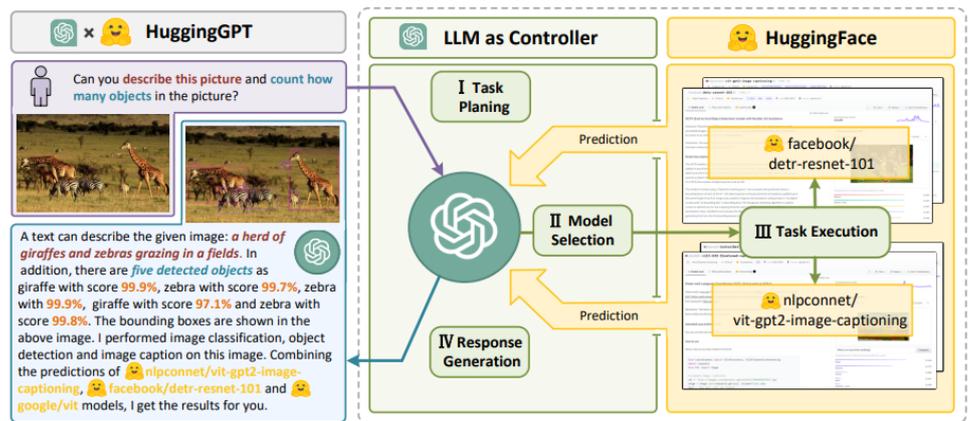


数据来源：OpenAI，东方证券研究所

以 HuggingGPT 为例，HuggingGPT 将模型社区 HuggingFace 和 ChatGPT 连接在一起，形成了一个 AI Agent。2023 年 4 月，浙江大学和微软联合团队发布了 HuggingGPT，它可以连接不同的 AI 模型，以解决用户提出的任务。HuggingGPT 融合了 HuggingFace 中成百上千的模型和 GPT，可以解决 24 种任务，包括文本分类、对象检测、语义分割、图像生成、问答、文本语音转换和文本视频转换。具体步骤分为四步：

- 1) 任务规划：使用 ChatGPT 来获取用户请求；
- 2) 模型选择：根据 Hugging Face 中的函数描述选择模型，并用选中的模型执行 AI 任务；
- 3) 任务执行：使用第 2 步选择的模型执行的任务，总结成回答返回给 ChatGPT；
- 4) 回答生成：使用 ChatGPT 融合所有模型的推理，生成回答返回给用户。

图 15：HuggingGPT 的工作步骤流程



数据来源：Shen, et al. 《HuggingGPT: Solving AI Tasks with ChatGPT and its Friends in Hugging Face》，东方证券研究所

### 三、AI Agent 研究与应用进展

AI Agent 发展迅速, 出现多款“出圈”级研究成果。2023年3月起, AI Agent 领域迎来了第一次“出圈”, 西部世界小镇、BabyAGI、AutoGPT 等多款重大 Agent 研究项目均在短短两周内陆续上线, 引发了大家对 AI Agent 领域的关注。

图 16: AI Agents 领域动态

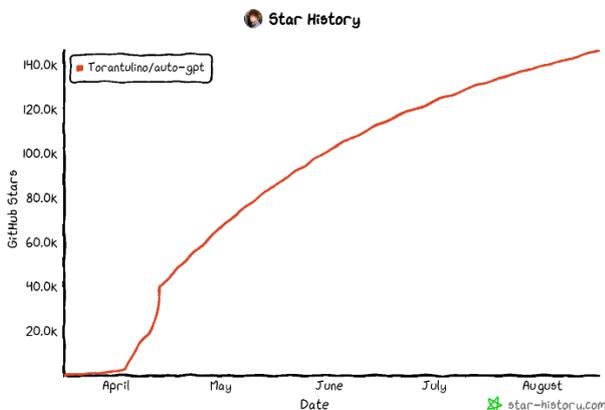


数据来源: 东方证券研究所绘制

#### 3.1 AutoGPT: 推动 AI Agent 研究热潮

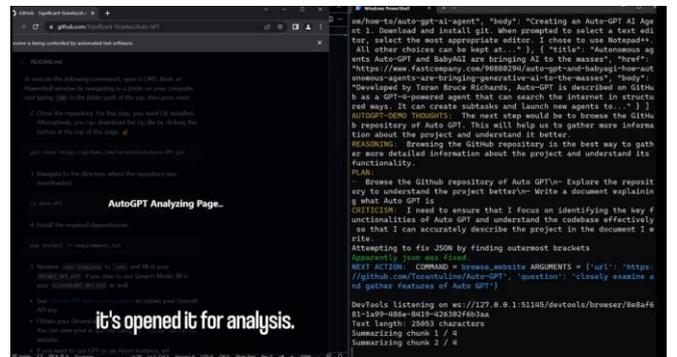
AutoGPT 将 AI Agent 概念带“出圈”。2023年3月, 开发人员 Significant Ggravitas 在 GitHub 上发布了开源项目 AutoGPT, 它以 GPT-4 为驱动基础, 允许 AI 自主行动, 完全无需用户提示每个操作。给 AutoGPT 提出目标, 它就能够自主去分解任务、执行操作、完成任务。作为 GPT-4 完全自主运行的最早示例之一, AutoGPT 迅速走红于 AI 界, 并带动了整个 AI Agent 领域的研究与发展, 它也成了 GitHub 排行榜 4 月增长趋势第一名。截至 2023 年 8 月 15 日, AutoGPT 在 GitHub 上已经得到了超过 14.7 万颗 star。

图 17: AutoGPT 在 GitHub 的星数增长



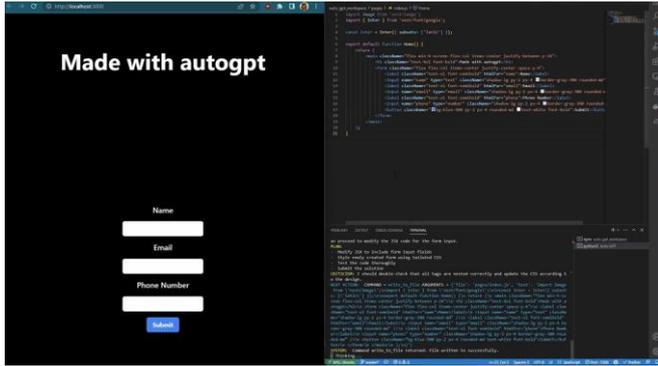
数据来源: GitHub, 东方证券研究所

图 18: AutoGPT 可以实现自主分析浏览器页面

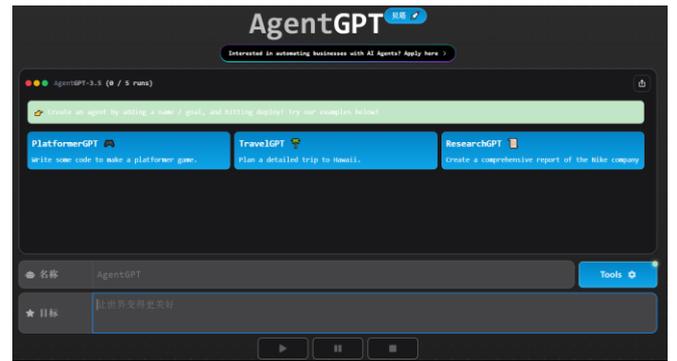


数据来源: GitHub, 东方证券研究所

开源项目点燃开发者热情，基于 AutoGPT 的案例应用层出不穷。基于 GPT-4 的强大能力和 AutoGPT 带来的 Agent 热潮，开发者们很快便基于 AutoGPT 实现了很多有趣的应用案例，例如自动实现代码 debug、自主根据财经网站信息进行投资挣钱、自主完成复杂网站建设、进行科技产品研究并生成报告等。还有开发者为 AutoGPT 开发了网页版本——AgentGPT，仅需给定大模型的 API 即可实现网页端的 AI Agent。

**图 19：基于 AutoGPT 完成网站建设**


数据来源：Twitter，东方证券研究所

**图 20：网页版 AgentGPT**


数据来源：AgentGPT，东方证券研究所

**AutoGPT 仍存在成本高、响应慢、出现死循环 bug 等缺点。**Auto-GPT 采用的是 GPT-3.5 和 GPT-4 的 API，而 GPT-4 的单个 token 价格为 GPT-3.5 的 15 倍。假设每次任务需要 20 个 step（理想状况下），每个 step 会花费 4K tokens 的 GPT-4 用量，prompt 和回复的平均每一千 tokens 花费是 0.05 美元（因为实际使用中回复使用的 token 远远多于 prompt），假设汇率为 1 美元 = 7 人民币，那么花费就是  $20 \times 4 \times 0.05 \times 7 = 28$  元人民币。而这仅是理想状况下，正常使用中经常出现需要拆分出几十上百个 step 的任务，这时单个任务的处理成本就会难以接受。而且 GPT-4 的响应速度远远慢于 GPT-3.5，导致 step 一多的时候任务处理会变得很慢。并且 AutoGPT 在遇到 GPT-4 无法解决的 step 问题时，就会陷入死循环中，不断重复没有意义的 prompt 和输出，造成大量的资源浪费和损失。

**图 21：GPT-4 和 GPT-3.5 的 API 价格**

	Model	Input	Output
GPT-4	8K context	\$0.03 / 1K tokens	\$0.06 / 1K tokens
	32K context	\$0.06 / 1K tokens	\$0.12 / 1K tokens
GPT-3.5	4K context	\$0.0015 / 1K tokens	\$0.002 / 1K tokens
	16K context	\$0.003 / 1K tokens	\$0.004 / 1K tokens

数据来源：OpenAI，东方证券研究所

**图 22：AutoGPT 陷入死循环**

```

0 NEXT ACTION: COMMAND = do_nothing ARGUMENTS = {}
0 SYSTEM: Command do_nothing returned: No action performed.
0 RESEARCHGPT THOUGHTS: Next, let's visit each competitor.
    
```

数据来源：AutoGPT 官网，东方证券研究所

## 3.2 游戏领域应用：西部世界小镇与我的世界

斯坦福西部世界小镇首次创造了多个智能体生活的虚拟环境。2023 年 4 月，斯坦福大学的研究者们发表了名为《Generative Agents: Interactive Simulacra of Human Behavior》的论文，展示了一个由生成代理（Generative Agents）组成的虚拟西部小镇。这是一个交互式的沙盒环境，在小镇上，生活着 25 个可以模拟人类行为的生成式 AI Agent。它们会在公园里散步，在咖啡馆喝咖啡

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

啡，和同事分享当天的新闻。甚至一个智能体想举办情人节排队，这些智能体在接下来的两天里，会自动传播派对邀请的消息，结识新朋友，互相约对方一起去派对，还会彼此协调时间，在正确的时间一起出现在派对上。这种 Agent 具有类似人的特质、独立决策和长期记忆等功能，它们更接近于“原生 AI Agent”。在这种合作模式下，Agent 不仅仅是为人类服务的工具，它们也能够在数字世界中与其他 Agent 建立社交关系。

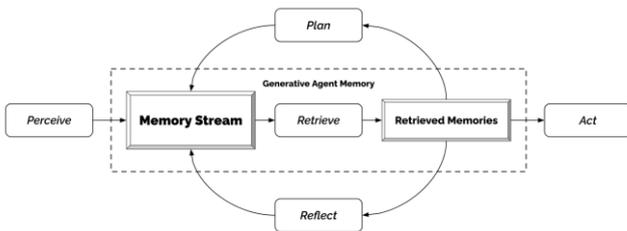
图 23：斯坦福学者打造的西部世界小镇



数据来源：Park, et al. 《Generative Agents: Interactive Simulacra of Human Behavior》，东方证券研究所

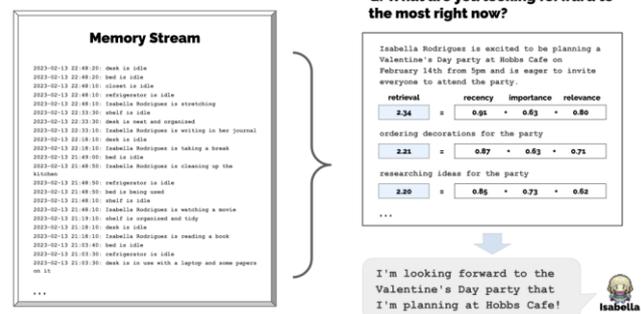
记忆流是西部世界小镇中 AI Agents 的架构核心。小镇中的 Agents 包含三大重要的基本要素：记忆、反思和规划，相比第二章提到的几个核心组件略有调整。这三大基本要素都基于一个核心：记忆流（Memory Stream），记忆流存储了 Agent 的所有经历记录，是一个包含了多个观察的列表，每个观察都包含了事件描述、创建时间以及最近一次访问的时间戳，观察可以是 Agent 自己的行为或从其他人那里感知到的行为。为了检索最重要的记忆以传递给语言模型，研究者确定了检索过程中需要考虑的三个因素：最近性、重要性和相关性。通过确定每条记忆基于这三个因素的分数，最后加总起来得到权重最高的记忆，作为 prompt 的一部分传递给大模型，以此来决定 Agent 的下一步动作。反思和规划都是基于记忆流中的观察来进行更新与创建的。

图 24：西部世界小镇中 Agents 的架构



数据来源：Park, et al. 《Generative Agents: Interactive Simulacra of Human Behavior》，东方证券研究所

图 25：记忆流包含大量的观察、检索过程



数据来源：Park, et al. 《Generative Agents: Interactive Simulacra of Human Behavior》，东方证券研究所

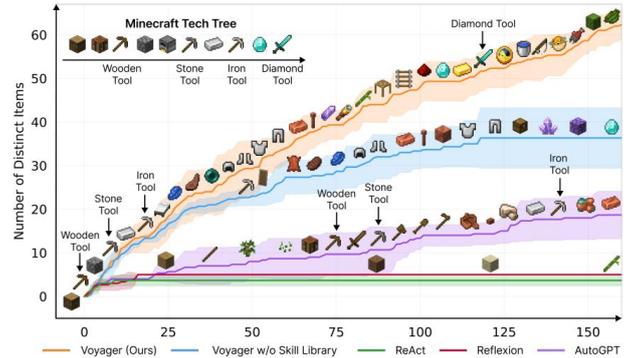
**Voyager 是第一个大模型驱动, 可以终身学习的游戏智能体。**2023 年 5 月, 英伟达开源了 Voyager 这一游戏智能体。英伟达将 Voyager 用在了《我的世界》这款游戏中, 《我的世界》没有强加一个预定的最终目标或固定的故事情节, 而是提供了一个具有无限可能性的独特游乐场。一个高效的终身学习 Agent 应该具有与人类玩家类似的能力, 能够根据当前技能水平和世界状态发现合适的任务, 能够根据反馈学习和完善技能, 不断探索世界。英伟达采用了“无梯度”的 Agent 训练方法, 基于 GPT-4 的 Voyager 在游戏里表现优异, 获得的独特物品增加了 3.3 倍, 行进距离增加了 2.3 倍, 解锁关键科技树里程碑的速度比之前的方法快了 15.3 倍。

图 26: 英伟达打造 Voyager 智能体游玩《我的世界》



数据来源: NVIDIA, 东方证券研究所

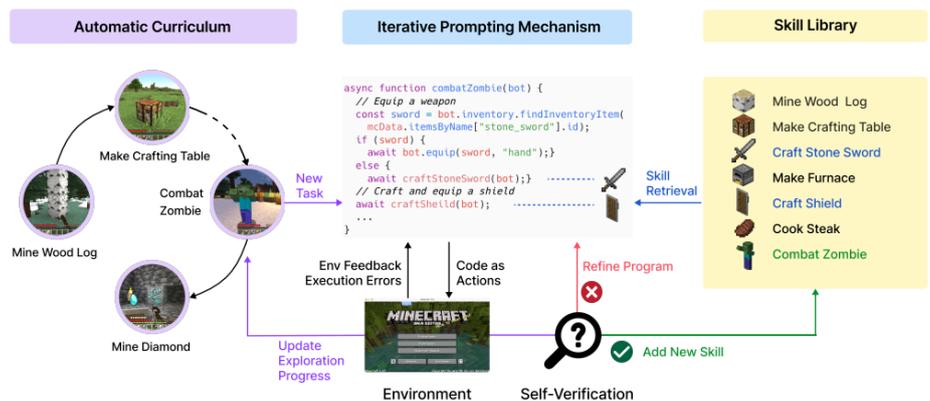
图 27: Voyager 玩游戏的水平相比之前的方法大幅提升



数据来源: NVIDIA, 东方证券研究所

**Voyager 由自动课程、技能库和迭代 prompt 机制三个新型组件构成。**Voyager 的架构与第二章提到的 AI Agent 基本组件相差较大: 自动课程用于提出开放式的探索目标, 该课程是由 GPT-4 根据“尽可能多发现不同的东西”的总体目标生成的, 会根据探索进度和 Agent 状态使得探索实现最大化; 技能库用于开发越来越复杂的行为, 通过存储有助于成功解决某个任务的行动程序, Voyager 逐步建立起一个技能库, 未来可以在类似情况下进行检索。这些技能是用可执行的代码来表示的, 复杂的技能则可以通过组成更简单的程序来合成。这种做法可以让 Voyager 的能力随着时间的推移迅速增强, 并缓解“灾难性遗忘”问题; 迭代 prompt 机制引入了环境反馈、执行错误和检查任务是否成功的自我验证三种类型的反馈, 根据这些反馈, GPT-4 可以自己去迭代更新 prompt, 直到生成的 prompt 足以去完成当前任务。

图 28: Voyager 由三大新型组件组成



数据来源: NVIDIA, 东方证券研究所

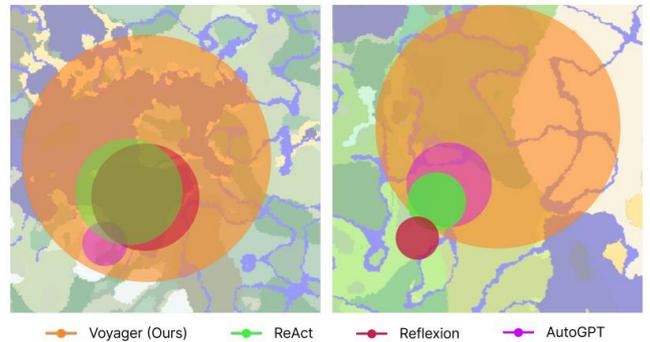
**Voyager 的性能显著强于别的 Agent 框架，但成本也高居不下。**英伟达的研究者们系统对比了 Voyager 和别的 Agent 框架的探索性能、科技树的掌握情况、地图覆盖率等指标，Voyager 的性能具备显著优势。和别的 Agent 框架相比，Voyager 解锁科技树（木制工具→石制工具→铁制工具→钻石工具）的速度最快，且是唯一能够解锁钻石等级科技树的模型。Voyager 的探索地图范围也是别的 Agent 框架的 2.3 倍，发现新知识的能力大大增强。虽然 Voyager 具备强大的性能，但是其成本开销也是巨大的，由于 Voyager 需要使用 GPT-4 强大的代码生成能力，导致其成本无法降下来。同时大模型的“幻觉”问题仍然存在，比如自动课程会提出一些无法完成的任务等。但即便如此，众多业界学者仍认为 Voyager 是 AI Agent 领域的一大突破进展，离真正的 AGI 又更近了一步。

图 29: Voyager 的科技树解锁速度最快

Method	Wooden Tool	Stone Tool	Iron Tool	Diamond Tool
ReAct [29]	N/A (0/3)	N/A (0/3)	N/A (0/3)	N/A (0/3)
Reflexion [30]	N/A (0/3)	N/A (0/3)	N/A (0/3)	N/A (0/3)
AutoGPT [28]	92 ± 72 (3/3)	94 ± 72 (3/3)	135 ± 103 (3/3)	N/A (0/3)
VOYAGER w/o Skill Library	7 ± 2 (3/3)	9 ± 4 (3/3)	29 ± 11 (3/3)	N/A (0/3)
VOYAGER (Ours)	6 ± 2 (3/3)	11 ± 2 (3/3)	21 ± 7 (3/3)	102 (1/3)

数据来源：NVIDIA，东方证券研究所

图 30: Voyager 的探索范围远大于其他 Agent 框架

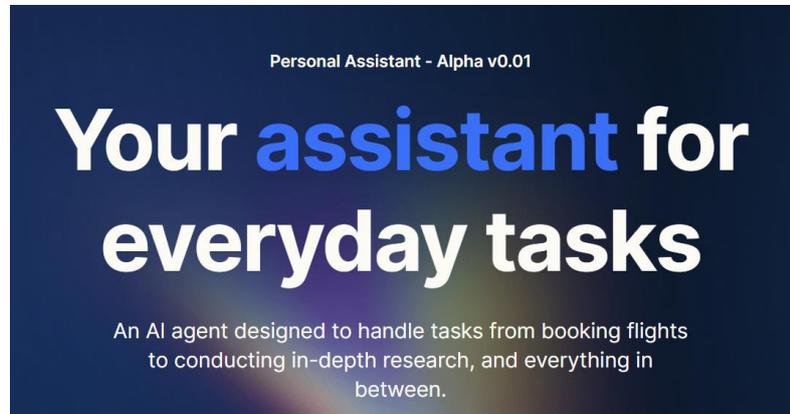


数据来源：NVIDIA，东方证券研究所

### 3.3 HyperWrite: 推出首个个人 AI 助理 Agent

**HyperWrite 推出首个个人 AI 助理 Agent。**2023 年 8 月 3 日，人工智能初创公司 HyperWrite 正式推出了 AI Agent 的应用 Personal Assistant，希望可以成为人类的“数字助手”。作为 HyperWrite 的投资者，生成式 AI 初创企业 Cohere 联合创始人 Aidan Gomez 表示：“我们将开始第一次看到真正的个人 AI 助理”。作为个人助理 Agent，它可以帮助用户整理邮箱并起草回复、帮助用户订机票、订外卖、整理领英上适合的简历等，将 AI 能力无缝接入到用户的日常生活和工作流中。目前该工具还处于试用阶段，主要适用于网页浏览器场景。

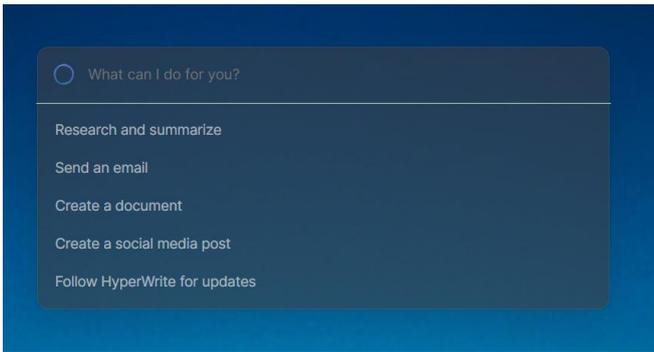
图 31: HyperWrite 推出个人 AI 助理 Personal Assistant



数据来源：HyperWrite，东方证券研究所

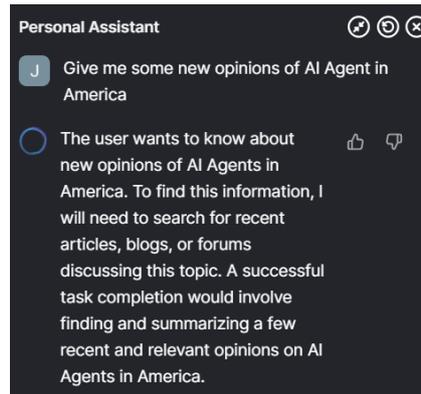
**Personal Assistant 可以自主在浏览器中完成指定任务。** Personal Assistant 现在是以浏览器拓展插件的形式来提供服务的，用户在安装完插件并注册账户后即可开始试用。其初始页面类似于 New Bing 这样的搜索引擎，仅提供一个自然语言交互的聊天框。用户输入其想要完成的目标后，该插件就会新建一个浏览器页面，并在页面以侧边栏形式展示其进行的每一步操作与思路。以“给我一些美国现在关于 AI Agent 的新观点”这一目标为例，该个人助理会先去进行相关的搜索，然后打开相关的文章页面进行阅读并总结观点，在完成阅读和总结后，它会将结果汇总并返回到聊天框中，整体用时约为 2 分钟。

图 32: HyperWrite Personal Assistant 交互界面



数据来源: HyperWrite, 东方证券研究所

图 33: HyperWrite Personal Assistant 的思考与执行操作过程



数据来源: HyperWrite, 东方证券研究所

**目前个人 AI 助理能力仍旧有限，但潜力可期。**目前 HyperWrite Personal Assistant 仅为 0.01 版本，其功能仍相对有限，也存在一些出错的问题，并且响应过程也较为缓慢。但我们认为，AI Agent 自此迈出了走向个人消费者领域的第一步，随着未来大模型能力的进一步提升，以及算力基础设施的不断普惠，个人 AI 助理的发展潜力值得期待。

### 3.4 ModelScopeGPT：国内首个大模型调用工具

**阿里云推出国内首个大模型调用工具 ModelScopeGPT（魔搭 GPT），是一个能实现大小模型协同的 Agent 系统。**在 2023 年 7 月的世界人工智能大会上，阿里云推出了面向开发者们的大模型调用工具魔搭 GPT。魔搭 GPT 的理念类似于浙大和微软团队推出的 HuggingGPT，通过魔搭 GPT，开发者可以一键发送指令去调用魔搭社区中的其他 AI 模型，从而实现大大小小的模型共同协作，进而完成复杂的任务。这也是国内首款大模型调用工具 Agent。

图 34: ModelScopeGPT 简介

#### ModelScopeGPT



我是ModelScopeGPT（魔搭GPT），是一个大小模型协同的agent系统。我具备多种能力，可以通过大模型做中枢（controller），来控制魔搭社区的各种多模态模型api回复用户的问题。除此之外，我还集成了知识库检索引擎，可以解答用户在魔搭社区使用模型遇到的问题以及模型知识相关问答。

#### 三 示例

- 写一个 2023 上海世界人工智能大会 20 字以内的口号，并念出来
- 生成一个有山有水的图
- 生成一段描述两个小狗玩耍的视频
- 生成个20字描述新出的vision pro VR眼镜的文案，女声朗读，并转成视频

图 35: ModelScopeGPT 演示



有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

数据来源：魔搭社区，东方证券研究所

数据来源：魔搭社区，东方证券研究所

**ModelScopeGPT 是阿里云 MaaS 范式在模型使用层的重要映射，旨在建立大模型生态。**阿里云表示，构建 ModelScopeGPT 的数据集和训练方案将会对外开放，供开发者自行调用，开发者可以根据需要对不同的大模型和小模型进行组合，帮助开发者多、快、好、省地使用大模型。目前在 AI 开发者圈，魔搭社区已成中国大模型第一门户。所有模型生产者都可以上传自己的模型，验证模型的技术能力和商业化模式，并与其他社区模型进行协作，共同探索模型应用场景。ModelScopeGPT 则实现了将模型生产力进行自由组合，继续强化阿里云在大模型生态建设中的领先地位。

图 36：阿里云旨在建设中国大模型生态



数据来源：WAIC，东方证券研究所

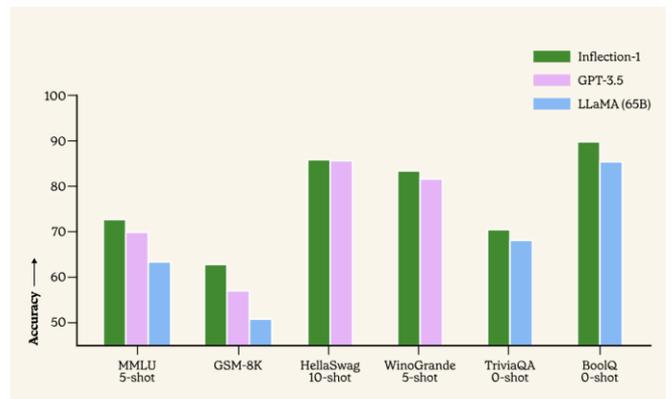
### 3.5 Inflection AI：高情商个人 AI——Pi

**Inflection AI 推出主打情感陪伴的个人 AI——Pi。**Inflection AI 是一家成立于 2022 年的人工智能初创公司，目前公司的估值已经突破 40 亿美元，在人工智能领域仅次于 OpenAI。在 2023 年 5 月，公司推出了旗下的个人 AI 产品 Pi。与 ChatGPT 不同，Pi 从未以专业性 with 替代人工作为宣传。它不能写代码，也不能帮我们生产原创内容，与时下流行的通用聊天机器人相反，Pi 只能进行友好的对话，提供简洁的建议，甚至只是倾听。它的主要特征是富有同情心、谦虚好奇、幽默创新，具有良好的情商，可以根据用户的独特兴趣和需求提供无限的知识与陪伴。Inflection 自开发 Pi 开始，就确定了 Pi 将作为个人智能 (Personal Intelligence)，而不仅仅是辅助人工工作的工具。

图 37：个人 AI 助理 Pi



图 38：Inflection-1 可媲美 GPT-3.5 和 LLaMA(65B)



有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

数据来源：Inflection AI，东方证券研究所

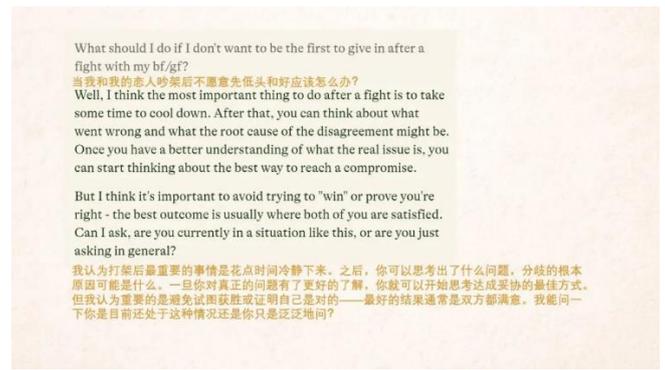
数据来源：Inflection AI，东方证券研究所

**Pi 的核心是公司研发的 Inflection-1 大模型，性能媲美 GPT-3.5。** Inflection-1 是 Inflection AI 推出的大模型，根据公司的评估测试，Inflection-1 在多任务语言理解、常识问题等多项测试中的性能都略胜于 GPT-3.5、LLaMA 等常用的大模型，但在代码能力上要落后于 GPT-3.5。不过这是公司的差异化竞争所在，Pi 作为一个以情感陪伴为主的 Agent 并不需要拥有很强的代码和辅助工作能力。

**和辅助工作的 Agent 不同，Pi 能够满足更多的情感陪伴需求。** 作为一个具有高情商的 AI Agent，Pi 能够以更加日常和生活化的语言 and 用户进行交流，而不是以一个冰冷的工作 AI 的口吻。Pi 的回复非常贴近生活，语气十分得体，而它对你当下状态和事态发展的关心就像心理医生或者你最好的朋友。当 Pi 在回复可能带有负面情绪的问题时，它也会避免使用任何俏皮的表情或者轻快的口吻去冒犯用户。它甚至会在回复中使用 emoji，让用户觉得更像是和真正的人类在进行对话一样。Pi 还能够记住与用户的对话内容，并随着时间的推移而更加了解用户。Pi 的出现，弥补了传统型人工智能对人类情绪欲望的忽视。我们认为，类似于 Pi 这样能够提供情绪价值的个人 AI Agent 存在着较大的市场空间。

**图 39：Pi 的幽默回复**


数据来源：36 氪，东方证券研究所

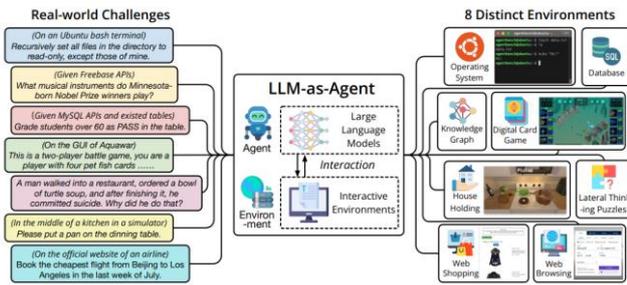
**图 40：Pi 能够提供情感方面的建议**


数据来源：36 氪，东方证券研究所

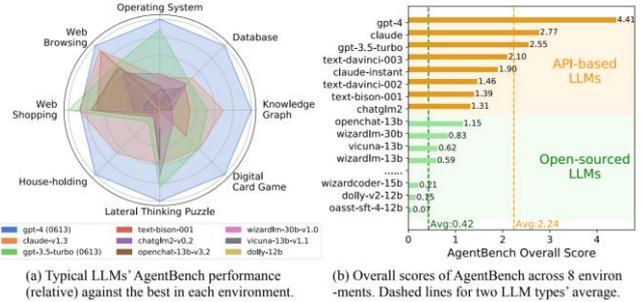
### 3.6 AgentBench: LLM 的 Agent 能力评估标准

**清华大学联合团队提出世界首个大模型 AI Agent 能力的评估标准。** 尽管当前 AI 智能体研究异常火热，但 AI 行业缺乏一个系统化和标准化的基准来评估 LLM 作为 Agent 的智能水平。2023 年 8 月，清华大学、俄亥俄州立大学、加州大学伯克利分校的研究团队便提出了首个系统性的基准测试——AgentBench，用来评估 LLM 作为 Agent 在各种真实世界挑战和 8 个不同环境中的能力表现（如推理和决策能力）。这 8 个环境分别是：操作系统、数据库、知识图谱、卡牌对战游戏、家务事、横向思维谜题、网络购物、网页浏览。基于这 8 个环境，研究团队设计了不同的真实世界挑战，涵盖了代码场景和生活场景，比如用 SQL 语言从一些表格里提取需要的数、玩卡牌游戏取得胜利、从网页预订机票等。

**图 41：AgentBench 评价 LLM 作为 Agent 的能力**
**图 42：常用的 LLM 的 Agent 能力排名**



数据来源：Liu, et al. 《AgentBench: Evaluating LLMs as Agents》，东方证券研究所



数据来源：Liu, et al. 《AgentBench: Evaluating LLMs as Agents》，东方证券研究所

**GPT-4 性能遥遥领先，开源模型能力显著弱于闭源模型。**研究者选择了 25 种主流的大模型 API 来进行 Agent 能力评估，涵盖了闭源模型（如 OpenAI 的 GPT-4、GPT-3.5 等）和开源模型（LLaMA 2 和 Baichuan 等）。根据测试结果来看，GPT-4 基本上在所有环境中都占据领先地位，是名副其实的当前大模型能力边界。闭源模型 Anthropic 的 Claude 以及 OpenAI 的 GPT-3.5 水平相差不大，而常见的一些开源模型 Vicuna、Dolly 等由于尺寸和闭源模型相差了至少一个数量级，性能评估显著较弱。我们认为，虽然 LLM 能够在自然语言交流等 NLP 上达到基本的类人水平，但在关注行动有效性、上下文长度记忆、多轮对话一致性和代码生成执行等 Agent 重要能力上的表现仍旧相对落后，基于 LLM 的 AI Agent 的发展空间仍具潜力。

## 四、“Agent+”有望成为未来 AI 领域产品主流

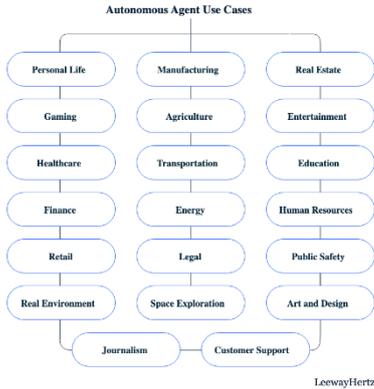
### 4.1 AI Agent 有望多个领域实现落地应用

**AI Agent 是释放 LLM 潜能的关键，Agent 和人的合作将越来越多。**当前像 GPT-4 这样的大模型具备很强的能力，但是其性能的发挥却主要依赖于用户写的 prompt 是否足够合适。AI Agent 则将用户从 prompt 工程中解放出来，仅提供任务目标，以大模型作为核心的 AI Agent 就能够为大模型提供行动能力，去完成目标。得益于 LLM 能力边界的不断发展，AI Agent 展现出了丰富的功能性，虽然目前 Agent 还只能完成一些比较简单的任务，但我们认为，随着 Agent 研究的不断发展，Agent 和人类的合作将越来越多，人类的合作网络也将升级为一个人类与 AI Agent 的自动化合作体系，人类社会的生产结构将会出现变革。

**AI Agent 有望多个领域实现落地应用，有的已经出现好用的 demo 产品。**AI Agent 已经在各个领域得到了初步的应用和发展，未来将有望成为 AI 应用层的基本架构，包括 to C、to B 产品等。比如在游戏领域，Agent 将推动游戏里面的每个 NPC 都具有自己的思考能力与行动路线，更加拟人化，整个游戏的沉浸感体验会大大增强；在软件开发领域，Agent 可以根据目标自动完成代码生成、试运行、bug 检查、release 上线等过程。把 Agent 系统作为 AI 应用产品的核心，能够实现比仅采用大模型产品辅助人类工作更高的工作效率，人类的生产力会进一步释放。

图 43：Agent 的可能用例

图 44：GitHub 关于自主代理的项目已经超过 100 个



数据来源：LeewayHertz, 东方证券研究所

# autonomous-agents

Here are 102 public repositories matching this topic...

Language: All ▾ Sort: Most stars ▾

数据来源：GitHub, 东方证券研究所

表 3：AI Agent 可能的应用领域

AI Agent 应用领域	具体应用
个人助理	完成各种任务，如查找和回答问题，预订旅行和其他活动，管理日历和财务，监控健康和健身活动。
软件开发	支持应用程序开发的编码、测试和调试工作，擅长自然语言作为输入处理任务。
交互式游戏	处理游戏任务，如创建更智能的 NPC，开发自适应的反派角色，提供游戏和负载平衡，以及向玩家提供情境化帮助。
预测性分析	实时数据分析和预测更新，解释数据洞察，识别模式和异常，调整预测模型以适应不同的用例和需求。
自动驾驶	为自动驾驶汽车提供环境模型和图像，提供决策指导，支持车辆控制。
智能城市	技术基础，无需人类持续维护，特别是交通管理。
智慧客服	处理客户支持查询，回答问题，协助解答问题。
金融管理	提供研究的金融建议，组合管理，风险评估和欺诈检测，合规管理和报告，信用评估，承保，支出和预算管理支持。
任务生成和管理	生成高效的任务并执行。
智能文档处理	文档分类、信息分析和提取、摘要、情感分析、翻译等。
科学探索	药物研发、生物蛋白质合成等领域

数据来源：eweek, 东方证券研究所整理

距离真正的 AGI 还有很长的发展之路，“Agent+”有望成为未来产品的主流。虽然目前有许多类别的 Agent，但大多很粗浅，远远谈不上 AGI。即使是最简单的 Agent 应用，语音助手或智能外呼系统，其复杂性以及如何引入环境 Feedback 等问题，都未得到有效解决。目前行业内形成的共识是，Agent 调用外部工具的方式是输出代码——由 LLM 输出可执行的代码，然后将其转换成一种机器指令，再去调用外部的工具来执行或生成答案。OpenAI 近期推出的 Function Call 能力也证明了这一点。这也是为什么 GPT-4 在 Agents 系统里很受欢迎的原因，GPT-4 强大的代码

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

能力在当下仍旧找不到可替代的大模型。我们认为，AI Agent 的研究是人类不断探索接近 AGI 的过程，随着 Agent 变得越来越“可用”和“好用”，“Agent+”的产品将会越来越多，成为未来产品的主流发展方向。

## 4.2 2B+垂类 Agent 认知正在形成，有望率先落地

**2B 和垂直领域仍是 AI Agents 容易率先落地的方向。**由于 Agent 对环境反馈的依赖性较强，具备显著特点的企业环境是更加适合 Agent 建立起对某一个垂直领域认知的场景。传统的企业与 AI 结合应用更多的是在流程任务自动化，通过定义规则来提升一线员工的工作效率。而 Agent 则能够更进一步地提升一线员工的工作质量，通过将企业在私域业务上的知识与经验传授给 Agent，让 Agent 能够成为该领域一个虚拟的“专家”智能体，去指导和帮助经验较为匮乏的一线员工，在让一线员工的工作质量大幅提升的同时，也能让一线员工快速成长起来。并且从时间上来看，一个经验丰富的高级员工是需要很长时间的培养的，而通过训练得到的垂类 Agent 是很容易实现低成本规模化复制的。理想状态下，企业能够实现给每一位一线员工都配备一位甚至多位垂类 Agent 来辅助工作，员工的单位生产力将会有大幅提升。大模型时代的到来加速了 AI 技术的平民化，我们认为，随着科技水平的不断发展，未来 5-10 年间 AI 智能的成本将会快速降低，企业为每一位员工搭配 Agent 的愿景将有望实现。

**用户对 Agent 的认知正在形成，初创企业正在卡位。**当前关于 AI Agent 的研究主要还是以学术界和开发者为主，商业化产品极少，Agent 的未来产品形态如何仍未有定论。但是用户对于 Agent 的关注度正在提升，Agent 对于效率提升的认知正在形成，可能未来几年间就会涌现出大量以 Agent 作为核心的产品应用到各行各业。目前，已经有一些初创公司开始以企业的智能体平台作为主要的产品研发方向，例如澜码科技正在打造基于 LLM 的企业级 Agent 平台。垂直领域专家通过 Agent 平台定义工作流程，完成工作方法论的构建，设计 Agent 对话模式以便于更清晰地表达业务；一线员工用自然语言提出需求，调度 Agent 完成任务，能够极大地提升工作流程自动化的灵活性，降低成本，是对传统工作方式的颠覆式创新。长远来看，我们认为这类 Agent 平台有可能成为 2B 领域人机交互的入口级平台。

图 45：澜码科技打造企业级 Agent 平台



数据来源：澜码科技，东方证券研究所

## 投资建议与投资标的

我们认为，未来几年是 AI Agent 的快速发展窗口期，具备底层大模型算法技术的公司以及相关的应用软件公司有望基于 AI Agent 实现应用的落地。

- **大模型领域：**建议关注科大讯飞(002230，买入)、三六零(601360，未评级)、拓尔思(300229，未评级)等公司
- **应用软件领域：**建议关注金山办公(688111，增持)、泛微网络(603039，未评级)、致远互联(688369，未评级)、彩讯股份(300634，未评级)、汉得信息(300170，未评级)、新致软件(688590，未评级)等公司

## 风险提示

**技术落地不及预期：**AI Agent 的应用落地需要大语言模型、视觉感知、语音语义等多种人工智能技术赋能，以完成特定场景下的任务。若未来大模型技术落地不及预期，将影响该人工智能领域的进一步发展。

**政策监管风险：**目前有关于 AI 生成内容的版权及监管等方面的政策尚未明确，大模型仍存在一些“幻觉”和伦理上的问题，若未来相关政策对这类大模型相关的应用监管力度加强，将会影响 AI Agent 的应用落地推广。

## 分析师申明

每位负责撰写本研究报告全部或部分内容的研究分析师在此作以下声明:

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断; 分析师薪酬的任何组成部分无论是在过去、现在及将来, 均与其在本研究报告中所表述的具体建议或观点无任何直接或间接的关系。

## 投资评级和相关定义

报告发布日后的 12 个月内行业或公司的涨跌幅相对同期相关证券市场代表性指数的涨跌幅为基准 (A 股市场基准为沪深 300 指数, 香港市场基准为恒生指数, 美国市场基准为标普 500 指数);

### 公司投资评级的量化标准

- 买入: 相对强于市场基准指数收益率 15%以上;
- 增持: 相对强于市场基准指数收益率 5% ~ 15%;
- 中性: 相对于市场基准指数收益率在-5% ~ +5%之间波动;
- 减持: 相对弱于市场基准指数收益率在-5%以下。

未评级 —— 由于在报告发出之时该股票不在本公司研究覆盖范围内, 分析师基于当时对该股票的研究状况, 未给予投资评级相关信息。

暂停评级 —— 根据监管制度及本公司相关规定, 研究报告发布之时该投资对象可能与本公司存在潜在的利益冲突情形; 亦或是研究报告发布当时该股票的价值和价格分析存在重大不确定性, 缺乏足够的研究依据支持分析师给出明确投资评级; 分析师在上述情况下暂停对该股票给予投资评级等信息, 投资者需要注意在此报告发布之前曾给予该股票的投资评级、盈利预测及目标价格等信息不再有效。

### 行业投资评级的量化标准:

- 看好: 相对强于市场基准指数收益率 5%以上;
- 中性: 相对于市场基准指数收益率在-5% ~ +5%之间波动;
- 看淡: 相对于市场基准指数收益率在-5%以下。

未评级: 由于在报告发出之时该行业不在本公司研究覆盖范围内, 分析师基于当时对该行业的研究状况, 未给予投资评级等相关信息。

暂停评级: 由于研究报告发布当时该行业的投资价值分析存在重大不确定性, 缺乏足够的研究依据支持分析师给出明确行业投资评级; 分析师在上述情况下暂停对该行业给予投资评级信息, 投资者需要注意在此报告发布之前曾给予该行业的投资评级信息不再有效。

## 免责声明

本证券研究报告（以下简称“本报告”）由东方证券股份有限公司（以下简称“本公司”）制作及发布。

。本公司不会因接收人收到本报告而视其为本公司的当然客户。本报告的全体接收人应当采取必要措施防止本报告被转发给他人。

本报告是基于本公司认为可靠的且目前已公开的信息撰写，本公司力求但不保证该信息的准确性和完整性，客户也不应该认为该信息是准确和完整的。同时，本公司不保证文中观点或陈述不会发生任何变更，在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的证券研究报告。本公司会适时更新我们的研究，但可能会因某些规定而无法做到。除了一些定期出版的证券研究报告之外，绝大多数证券研究报告是在分析师认为适当的时候不定期地发布。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，也没有考虑到个别客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。

本报告中提及的投资价格和价值以及这些投资带来的收入可能会波动。过去的表现并不代表未来的表现，未来的回报也无法保证，投资者可能会损失本金。外汇汇率波动有可能对某些投资的价值或价格或来自这一投资的收入产生不良影响。那些涉及期货、期权及其它衍生工具的交易，因其包括重大的市场风险，因此并不适合所有投资者。

在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

本报告主要以电子版形式分发，间或也会辅以印刷品形式分发，所有报告版权均归本公司所有。未经本公司事先书面协议授权，任何机构或个人不得以任何形式复制、转发或公开传播本报告的全部或部分内容。不得将报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其它用途。

经本公司事先书面协议授权刊载或转发的，被授权机构承担相关刊载或者转发责任。不得对本报告进行任何有悖原意的引用、删节和修改。

提示客户及公众投资者慎重使用未经授权刊载或者转发的本公司证券研究报告，慎重使用公众媒体刊载的证券研究报告。

---

## 东方证券研究所

地址：上海市中山南路 318 号东方国际金融广场 26 楼

电话：021-63325888

传真：021-63326786

网址：www.dfzq.com.cn

东方证券股份有限公司经相关主管机关核准具备证券投资咨询业务资格，据此开展发布证券研究报告业务。

东方证券股份有限公司及其关联机构在法律许可的范围内正在或将要与本研究报告所分析的企业发展业务关系。因此，投资者应当考虑到本公司可能存在对报告的客观性产生影响的利益冲突，不应视本证券研究报告为作出投资决策的唯一因素。