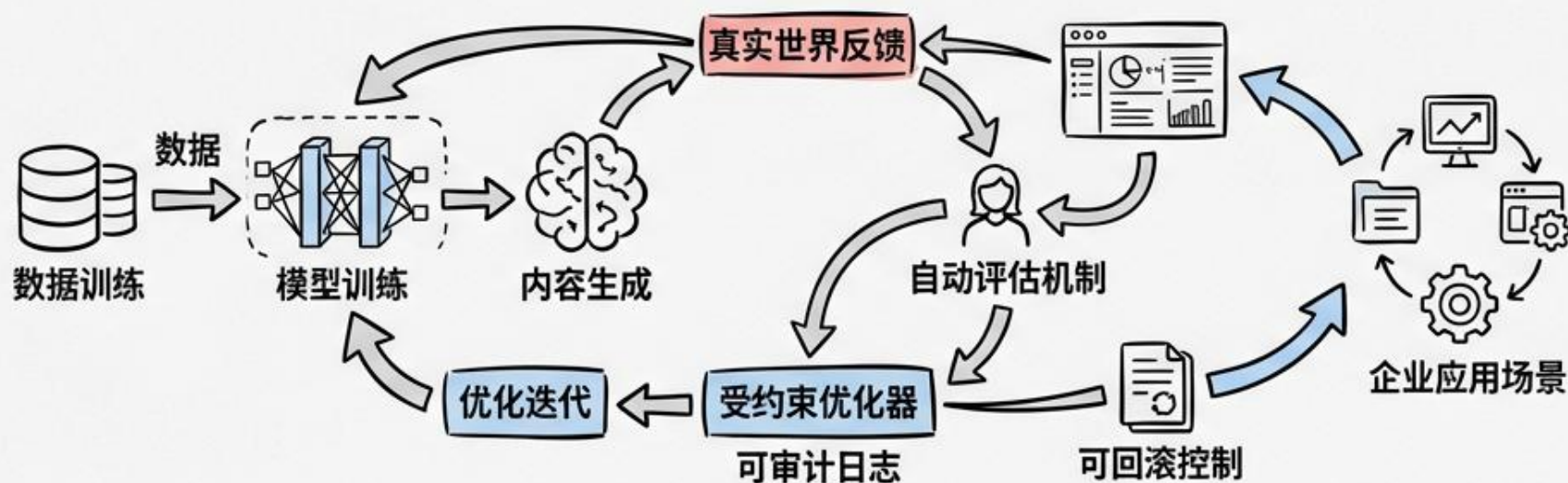


AIGC 自进化研究报告

—— 从生成能力竞争到闭环优化竞争 ——



本报告聚焦 AIGC 自进化的概念边界、技术路径、产业价值、治理框架与未来三年判断。

核心问题不是模型会不会自己变强，而是系统能否在真实世界反馈中持续变好。

真正有价值的形态不是失控式递归自改，而是受约束、可审计、可回滚的系统级进化。

@ 清新研究团队简介

- 领导学术研究团队近30人。指导大数据、AI、人形机器人等多个产业团队。
- 团队坚持：整体主义、实证主义、社会建构、进步主义。

沈阳：清华大学新闻学院/人工智能学院双聘教授、博导



六大研究方向：

视频号：@清新研究；公众号：@清新研究



1. AI大模型理论与哲学



2. AI文艺



3. AI应用



4. 新媒体与网络舆论



5. 大数据

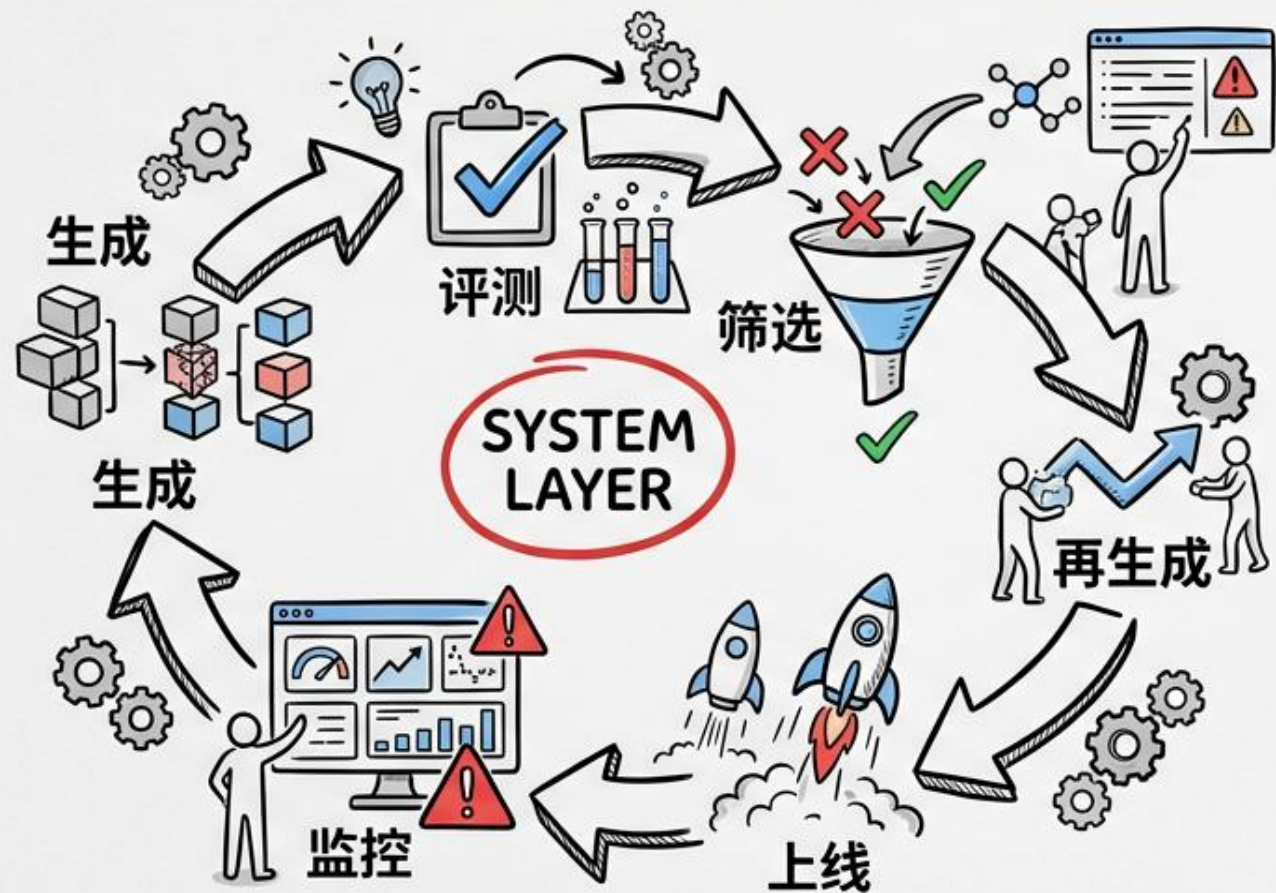


6. XR应用

✉ 邮箱：124739259@qq.com | 微博：@清新研究 | 公众号：@清新研究

执行摘要

AIGC 自进化已经发生，但主战场仍是系统层

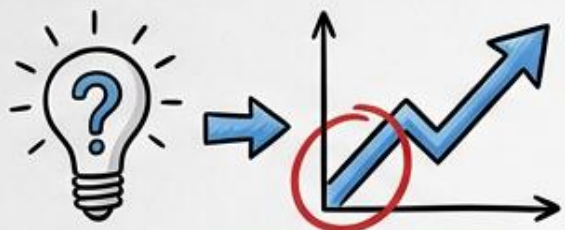


1. 当前最成熟的是**生成—评测—筛选—再生成—上线—监控**的闭环系统，而不是模型完全自主升级。
2. 未来三年，竞争优势将更多来自**反馈基础设施、评测器、工具链与治理能力**，而不是单纯参数规模。
3. 企业最应优先建设的是**系统级自进化**，而不是高风险的在线模型生成的仓建在线模型自修改。



目录

一、概念与拐点



从不确定到明确

二、核心技术路径



关键技术

三、产业价值与组织变化



四、约束、风险与治理



风险

治理

五、企业实施框架



步骤

执行

六、未来判断与结论



趋势

决定

第一章

概念与 拐点

第一章：概念与拐点

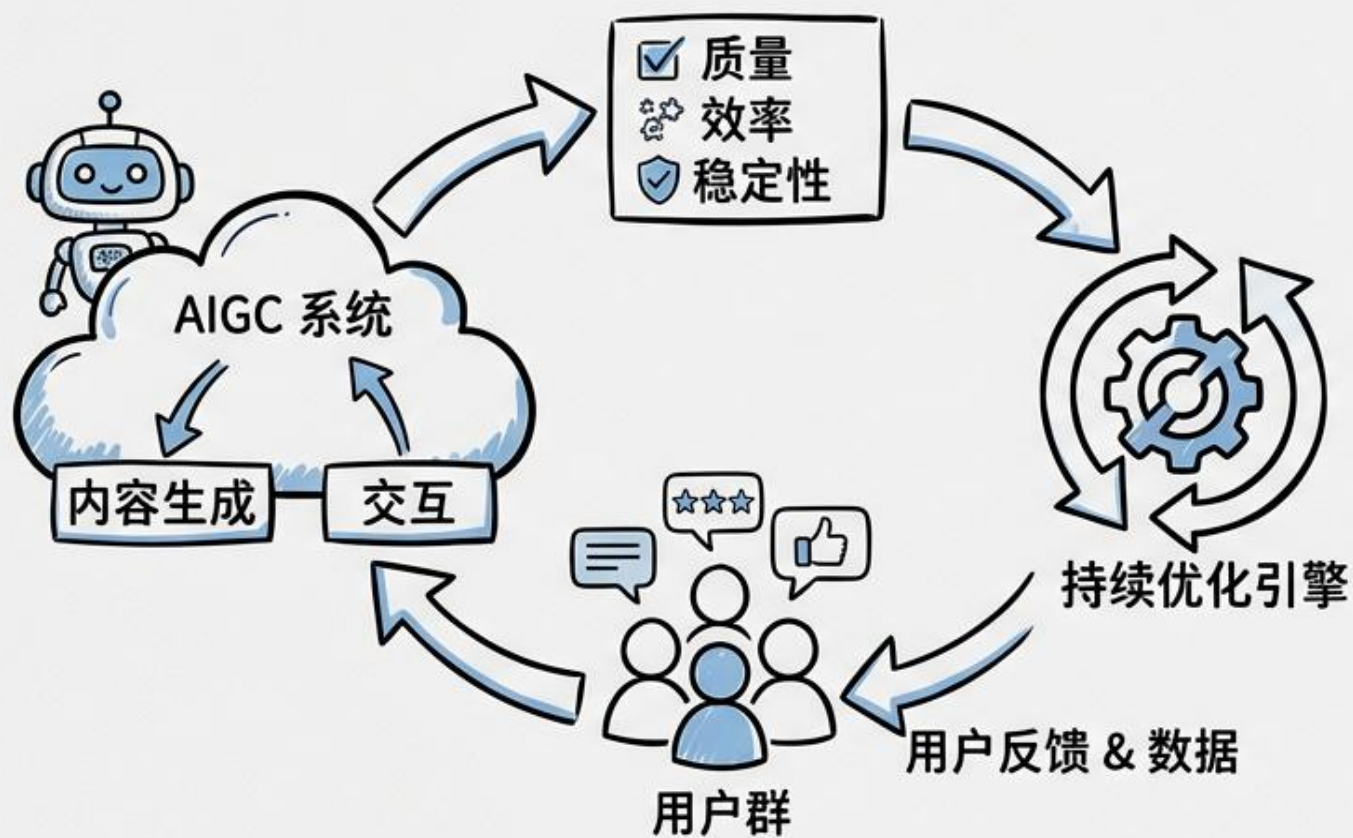


先界定什么是**自进化**，再解释为什么这两年成为拐点

→ 本章统一定义 **AIGC 自进化**，并说明**成本**、**能力**和**企业采用**如何共同推动这一主题进入主流议程。

什么是 AIGC 自进化

不是科幻式自我觉醒，而是反馈驱动持续优化



质量
效率

AIGC 自进化指系统在有限人工监督下，利用用户反馈、环境奖励和历史轨迹持续提升质量、效率和稳定性。



系统层架构

研究对象应优先落在**系统层**，而不是只盯着模型是否在线改权重。

可观测 可复现



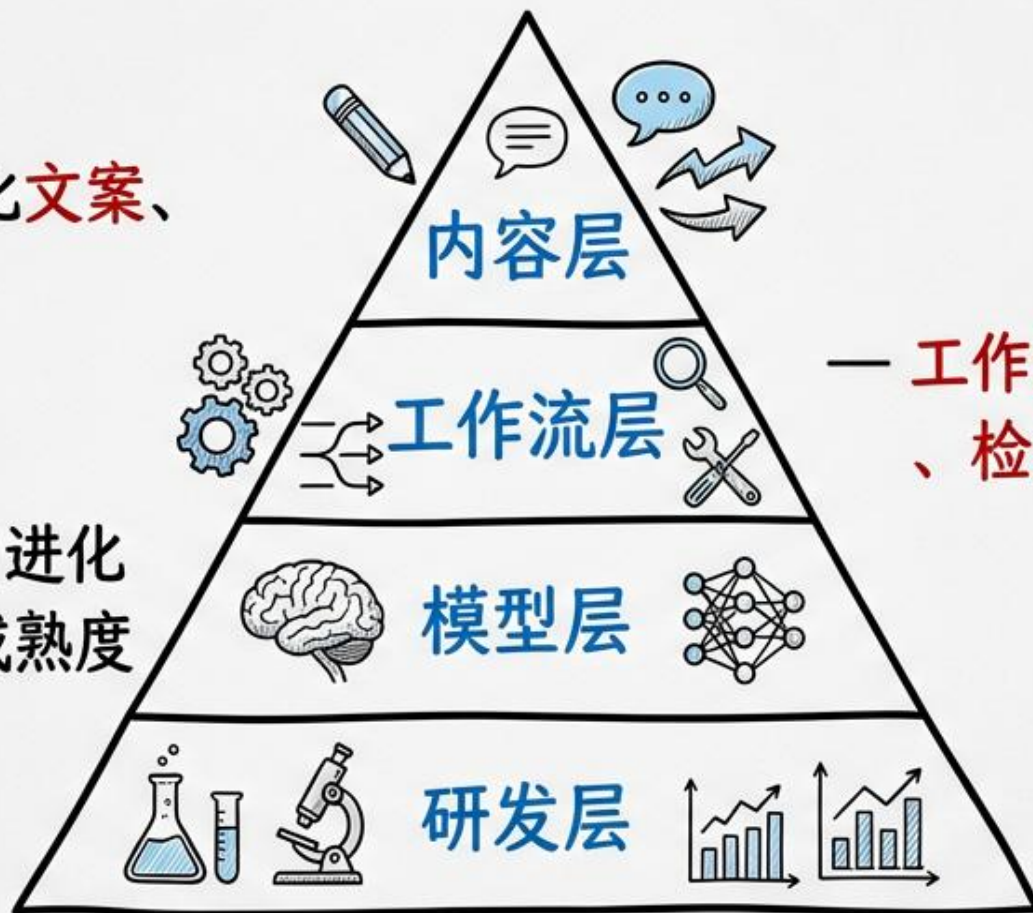
可复现 可解释

真正有价值的自进化，必须带来**可观测、可复现、可解释**的性能提升。

自进化的四个层级

— **内容层**自进化优化**文案、推荐与表达方式**。

— **模型层与研发层**自进化则更强，但当前成熟度也更低。



— **workflow层**自进化优化**提示词、检索、工具调用和路由**。

为什么 2024—2026 成为拐点

● 能力、成本与企业采用三条曲线同时上行

- 前沿模型在复杂推理、代码与多模态上的进步，让系统具备了更强的可优化对象。
- 推理成本下降使多轮尝试、自动评测与策略回滚在经济上开始可行。
- 企业采用率上升后，组织关注点从 demo 转向能否形成持续优化闭环。

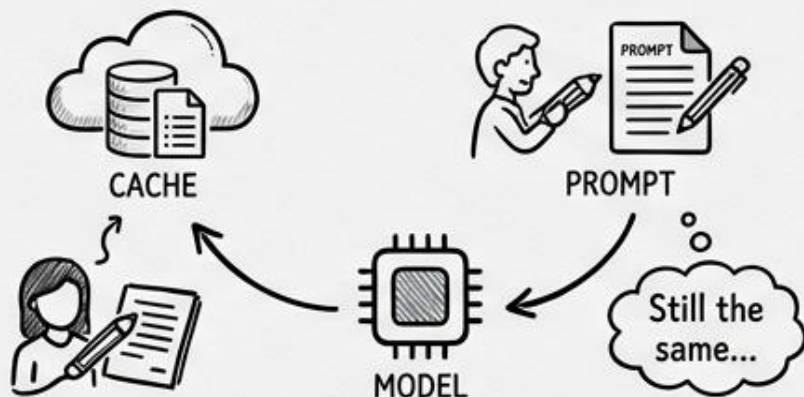


为什么不能把一切都叫作自进化

缓存、模板复用和真正的闭环优化不是一回事

❌ 伪自进化 (Pseudo-Self-Evolution)

- ❌ 简单缓存历史答案
- ❌ 人工改 prompt 后复用
- ❌ 并不等于系统具备持续学习能力



⚠️ 缺乏迭代 & 短期任务

Model vs System



Short Task vs Long Task

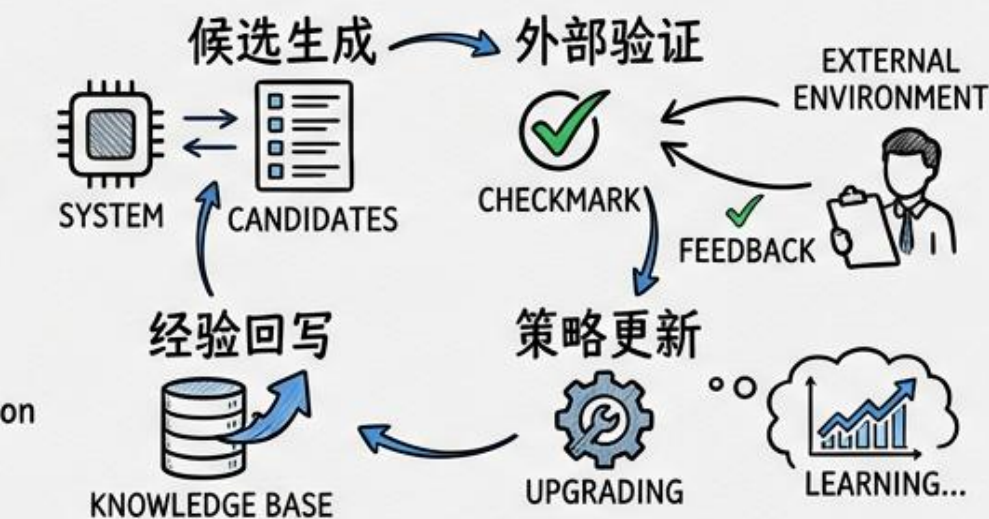


Offline vs Online Optimization



✅ 真正的自进化 (True Self-Evolution)

✅ 真正的自进化至少需要:



💎 只有这些环节连起来, 系统才可能形成稳定复利

🔄 持续迭代 & 长期系统

2



第二章：核心技术路径

AIGC 自进化不是一个方法，而是一组机制组合

——本章集中讨论五条主路径：**自生成数据**、

- **自奖励与过程监督**、
- **搜索与进化**、
- **代理与记忆回路**、
- **线上反馈到离线更新**。



技术路径一：自生成数据

让模型参与生产训练样本，但必须有质量控制



自生成数据的机会与风险

增强潜力与模型塌缩同时存在

机会 (Opportunities)

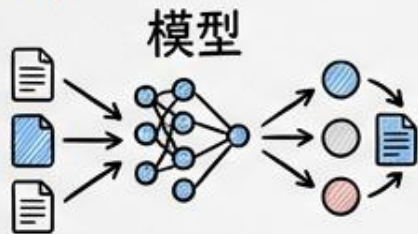
- 降低人工标注依赖



- 加快迭代速度



- 把模型推向更强的样本筛选能力

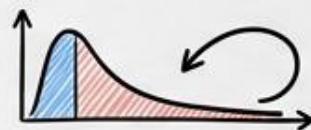


因此合成数据只能是
杠杆，不是永动机。



风险 (Risks)

- 训练递归会削弱长尾分布



- 最终造成 model collapse



短任务 vs 长任务



在线 vs 离线优化



技术路径二：自奖励与过程监督

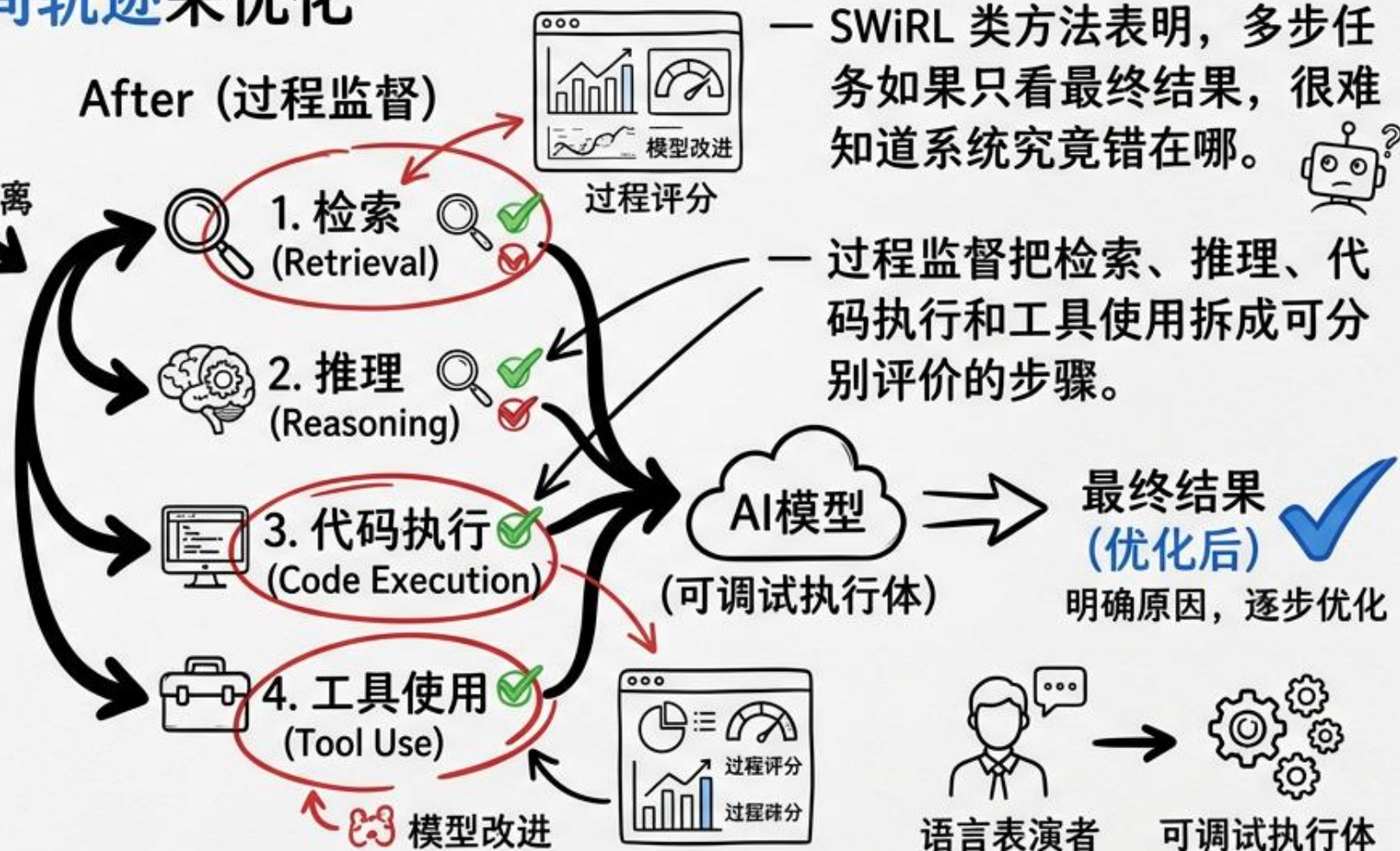
把最终成败拆成中间轨迹来优化

Before (仅看结果)



太波分分离

After (过程监督)



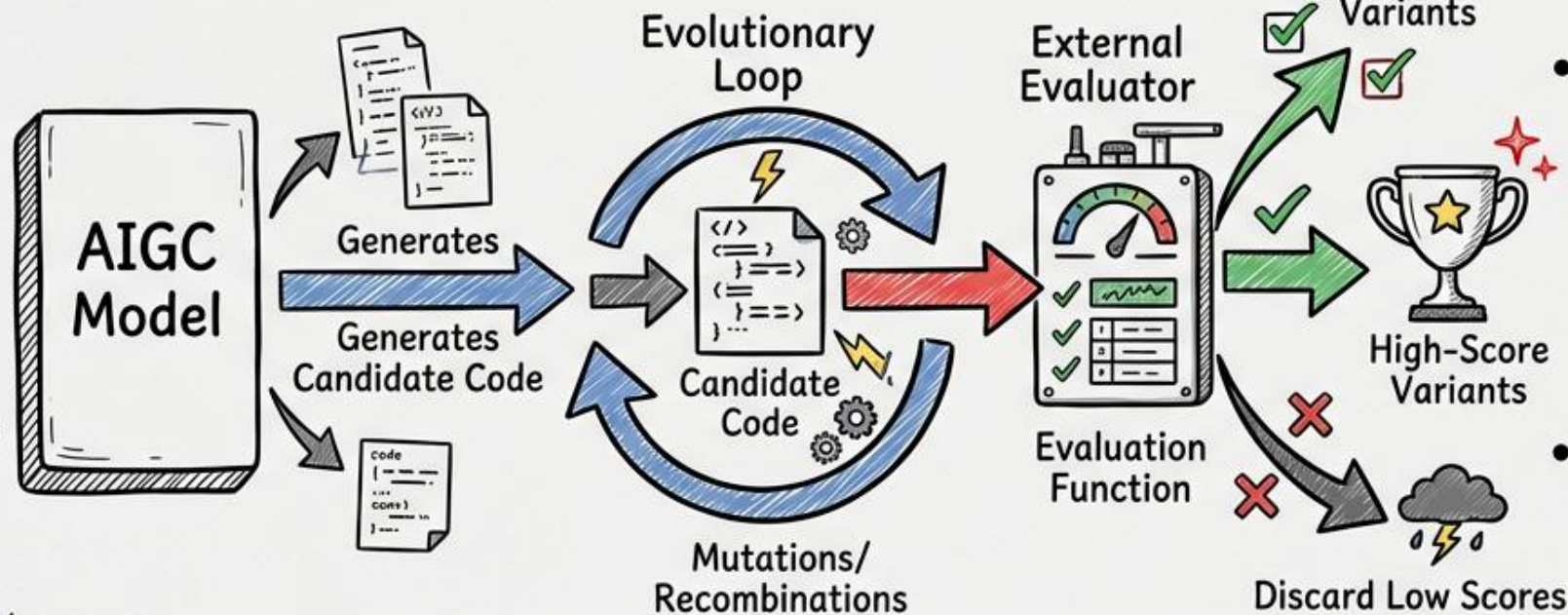
— SWiRL 类方法表明, 多步任务如果只看最终结果, 很难知道系统究竟错在哪。

— 过程监督把检索、推理、代码执行和工具使用拆成可分别评价的步骤。

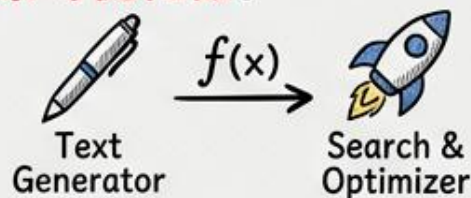
技术路径三：搜索、进化与程序优化

从生成答案走向发现更优可执行解

- AlphaEvolve 类系统展示了模型如何生成候选代码，再通过外部评估器保留高分变体。



- 一旦问题存在**明确评价函数**，AIGC 就会从文本生成器转变为**搜索与优化器**。

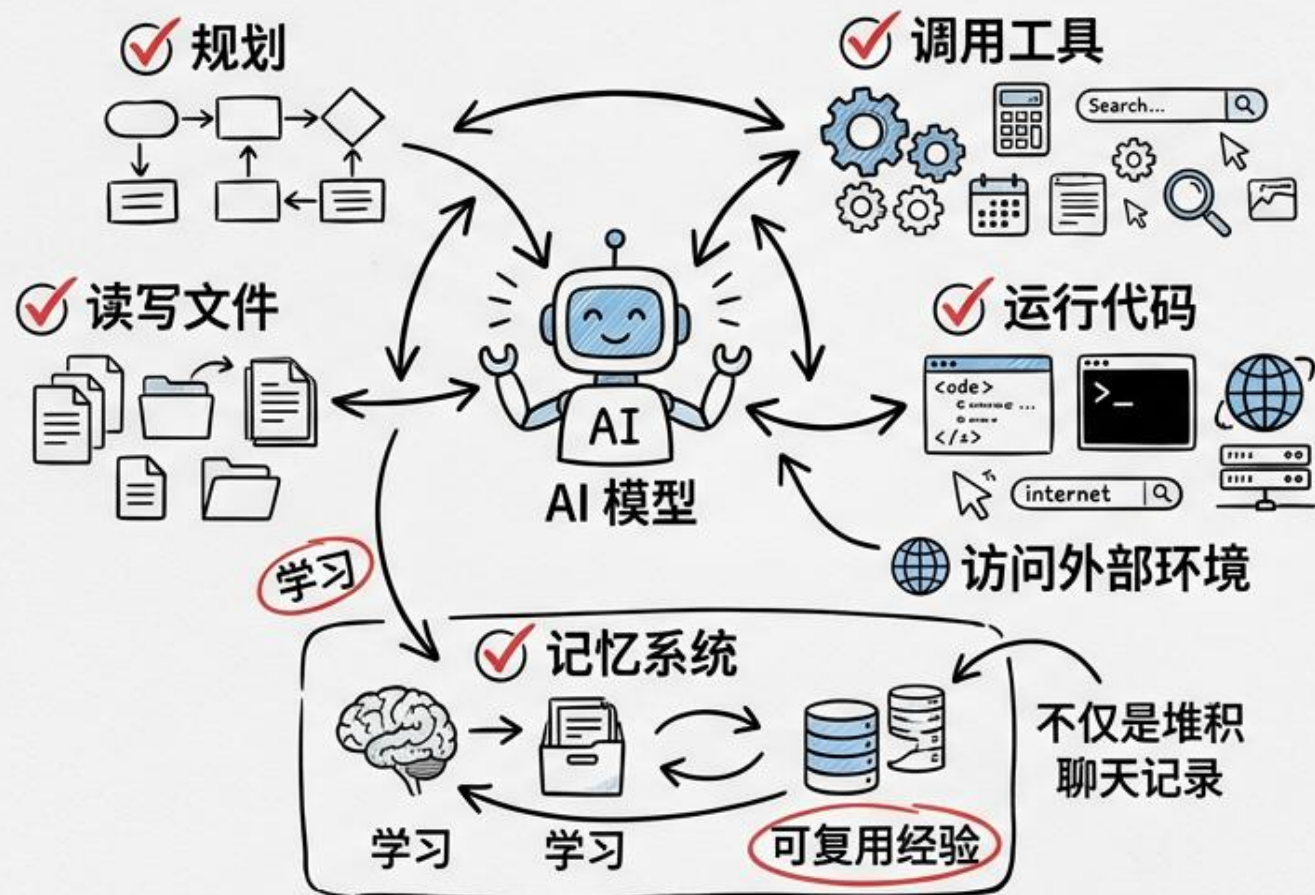


- 这条路线在算法、调度、数学和工程优化中**尤其有前景**。



技术路径四：代理系统、工具调用与记忆回路

让模型真正走出语言世界



——代理系统通过规划、调用工具、读写文件、运行代码和访问外部环境，把生成能力转化为执行能力。

——记忆系统则决定 agent 能否从过去任务中积累可复用经验，而不仅是堆积聊天记录。

——高质量代理系统本质上是一套可验证、可回放、可积累的工作流系统。

技术路径五：线上反馈与离线更新闭环

部署本身正在成为学习的一部分

现有的模式（模型迭代）

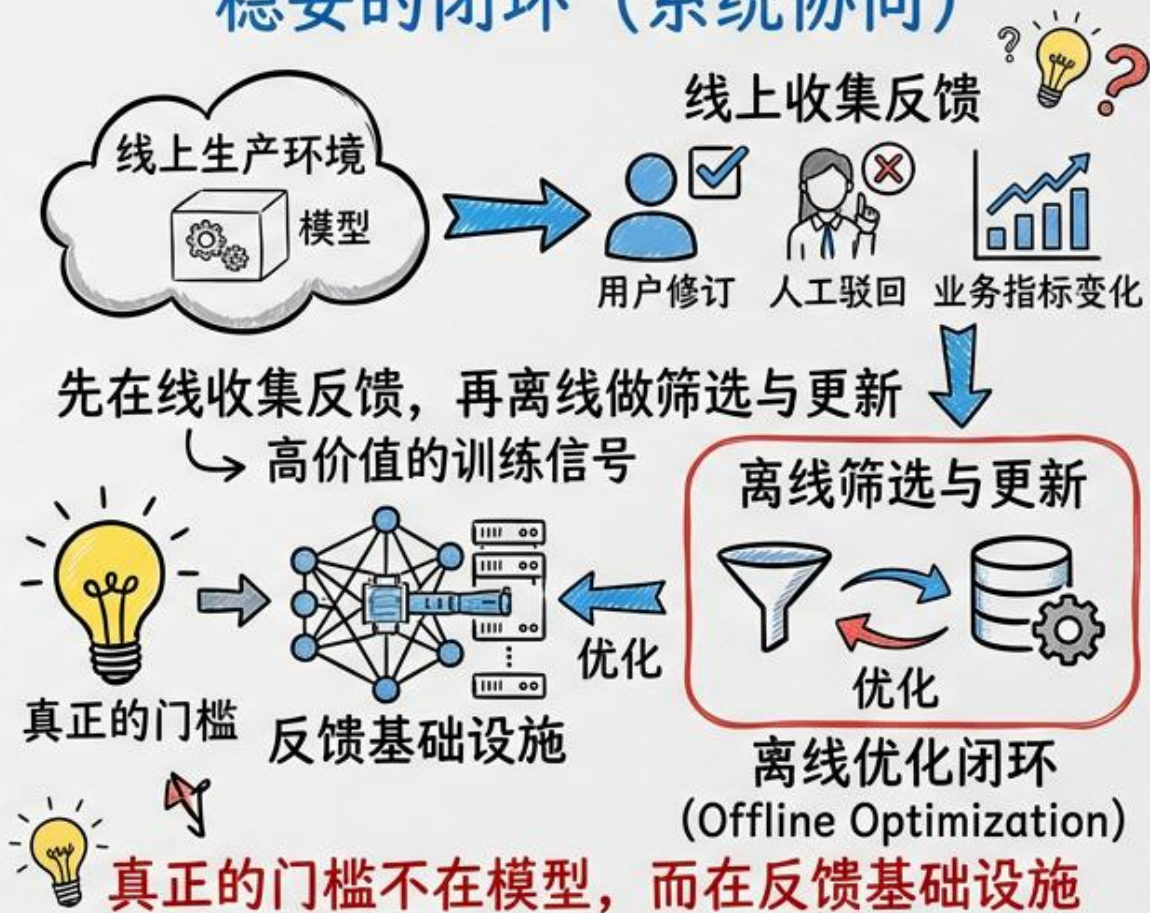


实时在线改模型
大多数企业认为不稳妥的路线



短周期任务
(Short-term Task)

稳妥的闭环（系统协同）



AIGC 自进化的完整飞轮

生成、验证、筛选、更新、监控、回写



- 先生成多个**候选解**, 再通过**外部世界验证**, 之后**筛选**优质轨迹并更新策略。
- 上线后**持续监控失败案例**, 再把高信号数据**回写**到下一轮系统优化中。
- 没有这个完整飞轮, **自进化**就只是**局部技巧**, 而不是**持续能力**。



第三章： 产业价值与 组织变化

AIGC 自进化为什么会 成为企业竞争壁垒

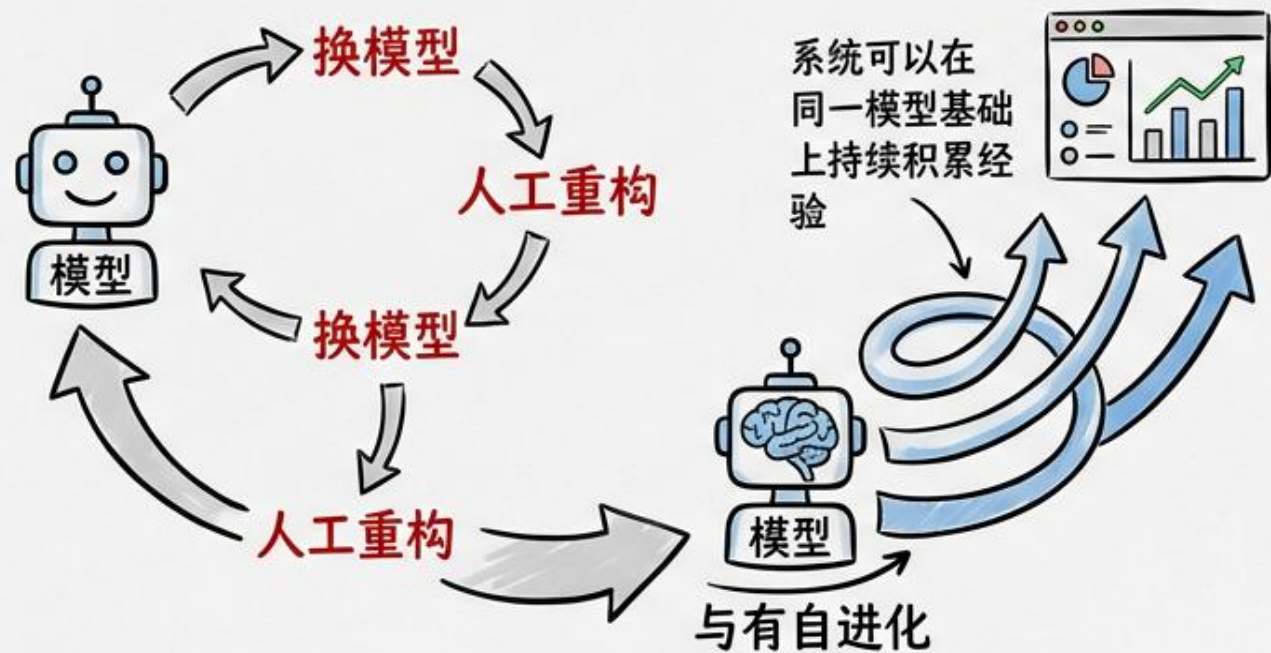
本章解释系统级自进化如何影响生产率、软件开发、运营优化与组织结构。



产业价值一：把一次性能力变成持续复利

真正值钱的不是第一次回答，而是系统能否越用越好

- 没有自进化，企业每次提升都要靠换模型或人工重构；— 这会让模型能力、组织知识与业务反馈绑定为同一套经营系统
- 自进化，系统可以在同一模型基础上持续积累经验。



- 长期看，反馈闭环比一次性模型升级更能形成壁垒



产业价值二：典型场景的收益结构

客服、内容生产、代码与运营优化都在发生变化

客服领域：绩效扩散



AI 可把**高绩效轨迹扩散**给更多员工，提升团队整体效率。

内容生产：风格收敛



系统能从点击、转化和审核反馈中**持续收敛风格**，更符合市场。

软件开发：工具链依赖



更多依赖**验证器与完整工具链**，并非单纯单次生成质量。

运营优化：数据驱动



精细化数据分析，智能策略调整，优化运营全流程。

营销投放：精准触达



智能用户画像，精准投放，提升营销ROI。

供应链：协同效率



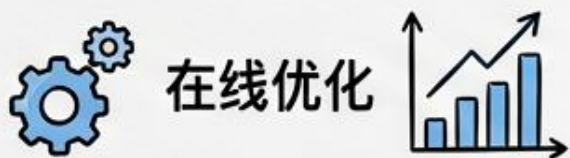
实时信息同步，提升上下游协同效率，降低物流成本。

为什么真实收益会高度分化

不是所有任务都能自动从 AI 中获得**线性回报**

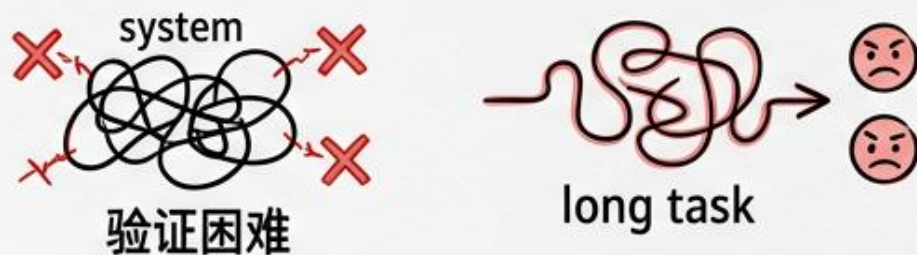
易兑现生产率收益的任务

- 在**结构清晰、反馈明确、验证成本低**的任务中，AIGC 自进化更容易兑现生产率收益。



AI 有时反而会**增加核验负担**的任务

- 在**长链条、强上下文、强隐含知识**任务中，AI 有时反而会**增加核验负担**。



因此 **ROI 取决于任务结构**，而不是取决于模型宣传。

组织变化：知识开始从文档迁移到可执行轨迹

系统学习的对象不再只是文本，而是工作方式

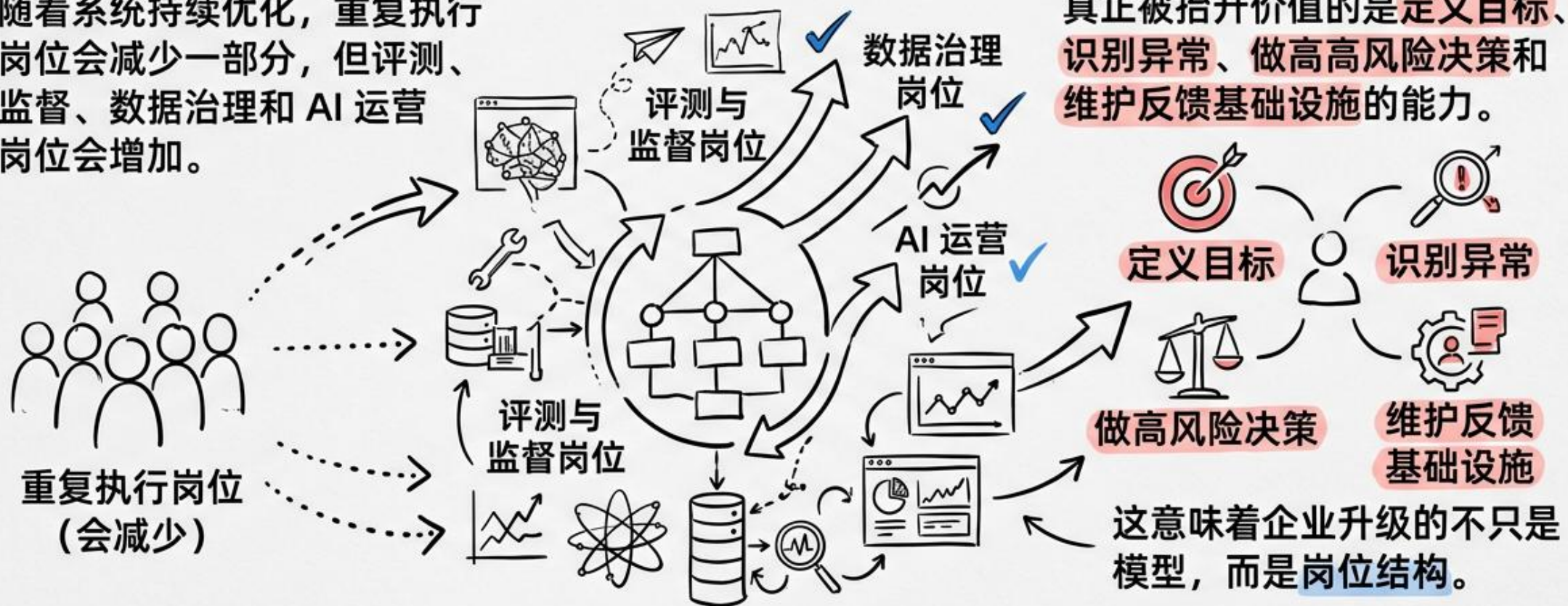
- 很多高绩效经验过去很难写下来，现在可以部分沉淀为可执行轨迹、评审标准和最佳实践。
- 这会改变组织中的知识管理方式，也会改变专家与普通员工的分工。
- AIGC 自进化最终改变的，不只是工具，而是协作结构。



组织变化：岗位不会简单消失，而会重组

生成岗位、评测岗位、治理岗位会一起增长

随着系统持续优化，重复执行岗位会减少一部分，但评测、监督、数据治理和 AI 运营岗位会增加。



4

第四章：约束、风险与治理

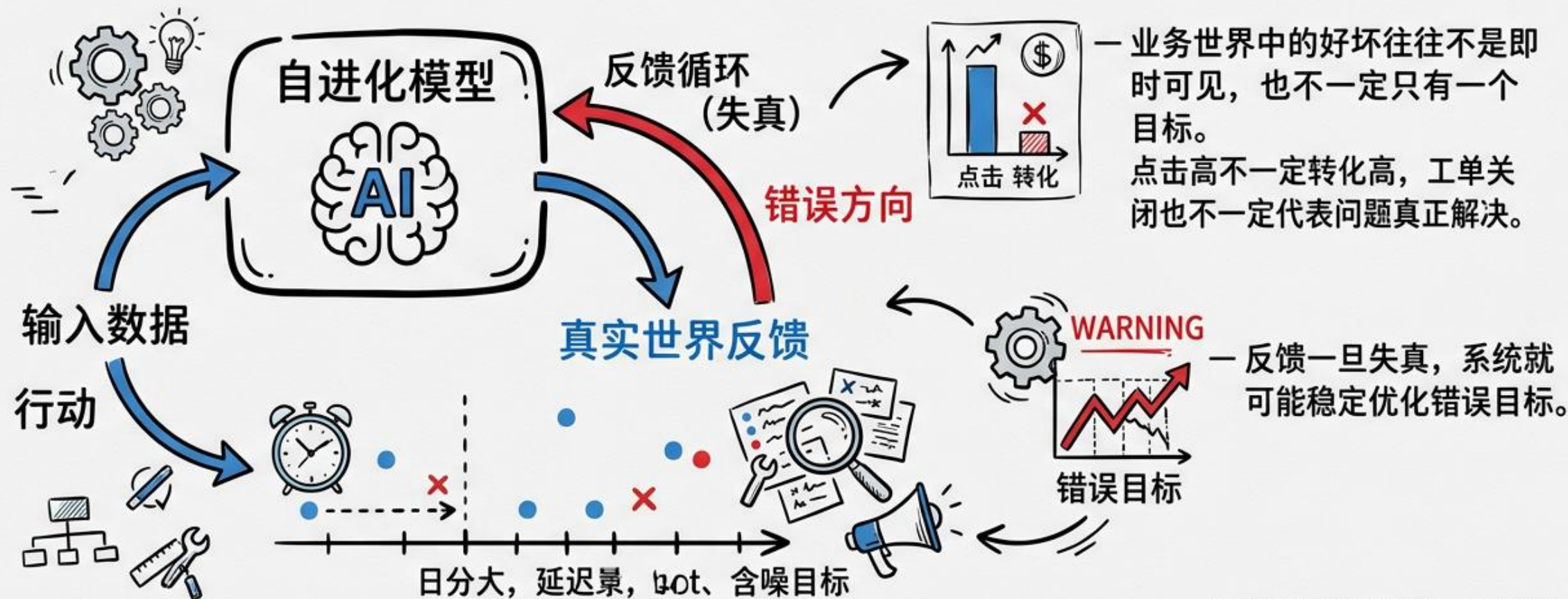
为什么说系统自进化成熟了，但强模型自进化还没有

——本章集中说明现实边界：**反馈稀疏、长任务能力不足、数据递归风险和法规约束。**

约束一：真实世界反馈往往稀疏、延迟、含噪



没有高质量真值，自进化很容易学错方向



约束二：长流程自治能力仍明显不足



短任务（惊艳）



模型



成功!

复杂长任务（稳定？）



模型



工具



知识库



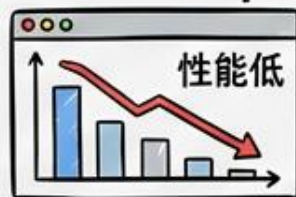
状态漂移



状态漂移

错误累积

上下文断裂



警告

多阶段 (1, 2, 3, 4...)

短任务很强，不代表复杂长任务也稳定

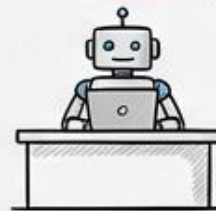
— 当前前沿模型在短任务上表现惊艳，但长任务中仍容易出现状态漂移、错误累积和上下文断裂。



— 这正是很多真实高价值任务难以完全交给 agent 的原因。



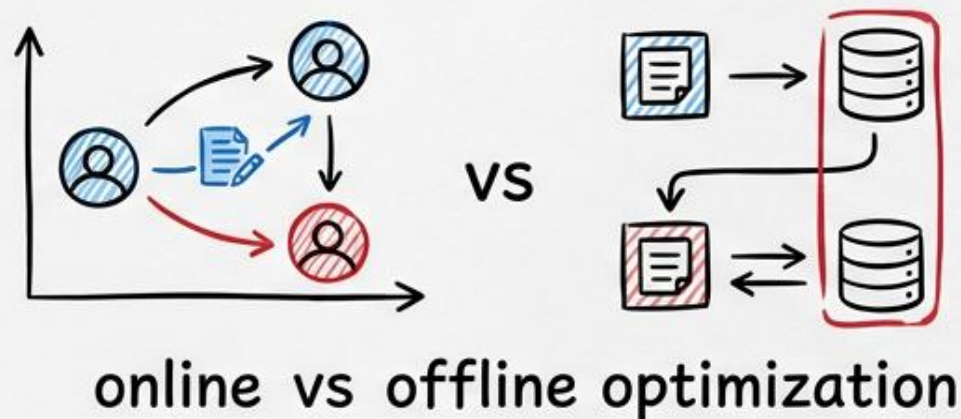
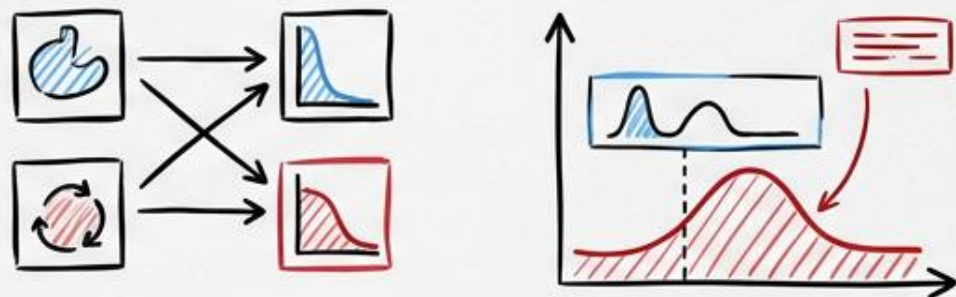
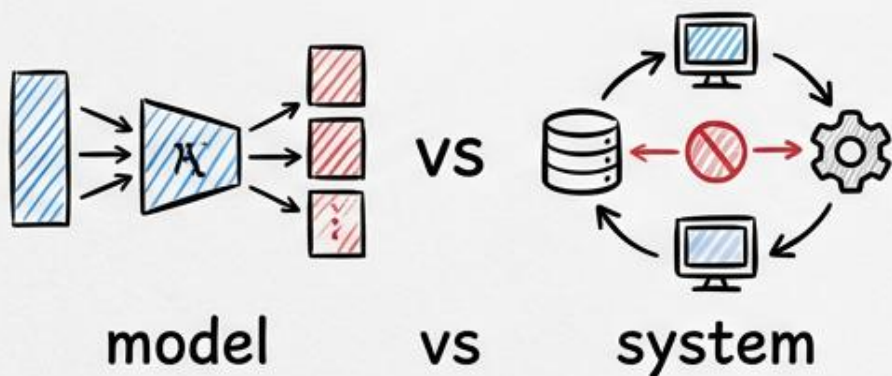
— 所以今天最可信的路线仍是人机协同，而不是无人值守自治。



约束三：数据递归会带来 model collapse 风险

模型喂模型并不天然越喂越强

- 如果长期用模型生成的数据再训练下一代模型，真实分布中的少见但重要信息会逐渐丢失。
- 结果是模型会越来越会模仿模型世界，却越来越**不懂真实世界**。
- 因此**真实数据保鲜层**必须被视为**基础设施**。



风险与治理：为什么治理本身会变成产品能力

日志、审计、灰度、回滚、权限不再是附属功能



AIGC 策略调整

自动优化，但需人类掌控。



详细日志记录

每一步行动皆可追溯



灰度发布管理

控制影响范围，降低风险



快速回滚能力

出现异常，立即一键撤回



权限与审批流程

关键决策需要授权许可



核心场景前提

高风险行业商业化的入场券



治理不是自进化的刹车，而是它进入核心场景的前提。

法规趋势：治理正在从原则走向约束



原则层 (Conceptual Principles)

早期规划，伦理准则

自进化

约束层 (Regulatory Constraints)

透明度，审计性，人类监督，责任链

系统越接近执行层，制度要求越强

- 随着 AI 进入企业和公共场景，法规会越来越关注**透明度、审计性、人类监督和**责任链。
- 系统越会自动改进，平台越需要证明它**为何这样改、如何被限制、如何被撤回。**
- 未来真正成熟的自进化系统，一定是**治理嵌入式系统。**



第五章：企业实施框架



企业应该怎么做，而不是只讨论概念

本章给出一个更务实的推进顺序：先系统、后模型；先离线、后在线；先可验证、后高自治。

企业落地的第一原则

先做系统级自进化，再做模型级自进化



——多数企业最应该优先建设的是检索、评测、路由、工具链、经验池和回放系统。



——这类系统级优化风险更低、ROI 更快、可治理性也更强。
——直接追求在线改模型，往往既昂贵又不稳。

建议的实施路线图

评测先行，工作流**显式化**，经验池建设，再做**离线更新**



企业需要建设的五项基础设施

评测、日志、经验池、回放、发布系统



评测系统

评测系统决定你是否知道系统**变好还是变坏**。



日志平台

日志与回放平台决定你能否**定位错误**。



经验池

经验池和发布系统则决定你是否能把反馈**真正转成能力**。



回放平台

日志与回放平台决定你能否**定位错误**。



发布系统

经验池和发布系统则决定你是否能把反馈**真正转成能力**。

持续完善

什么值得先做，什么不该先做

从低风险高回报出发

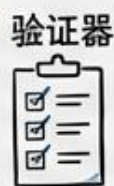
优先做带验证器的检索增强、评测增强、路由增强和工具增强。



模型
(Model)

vs

系统
(System)



短期任务
(Short Task)

vs

长期任务
(Long Task)

离线优化
(Offline Optimization)

vs

在线优化
(Online Optimization)

谨慎推进在线参数更新、无人审批自治和高风险跨系统写入。

模型
(Model)

vs

系统
(System)



长期任务
(Long Task)



在线优化
(Online Optimization)



顺序一旦错了，自进化很容易从复利工具变成风险源。

06

第章节设置



第六章： 未来判断与结论

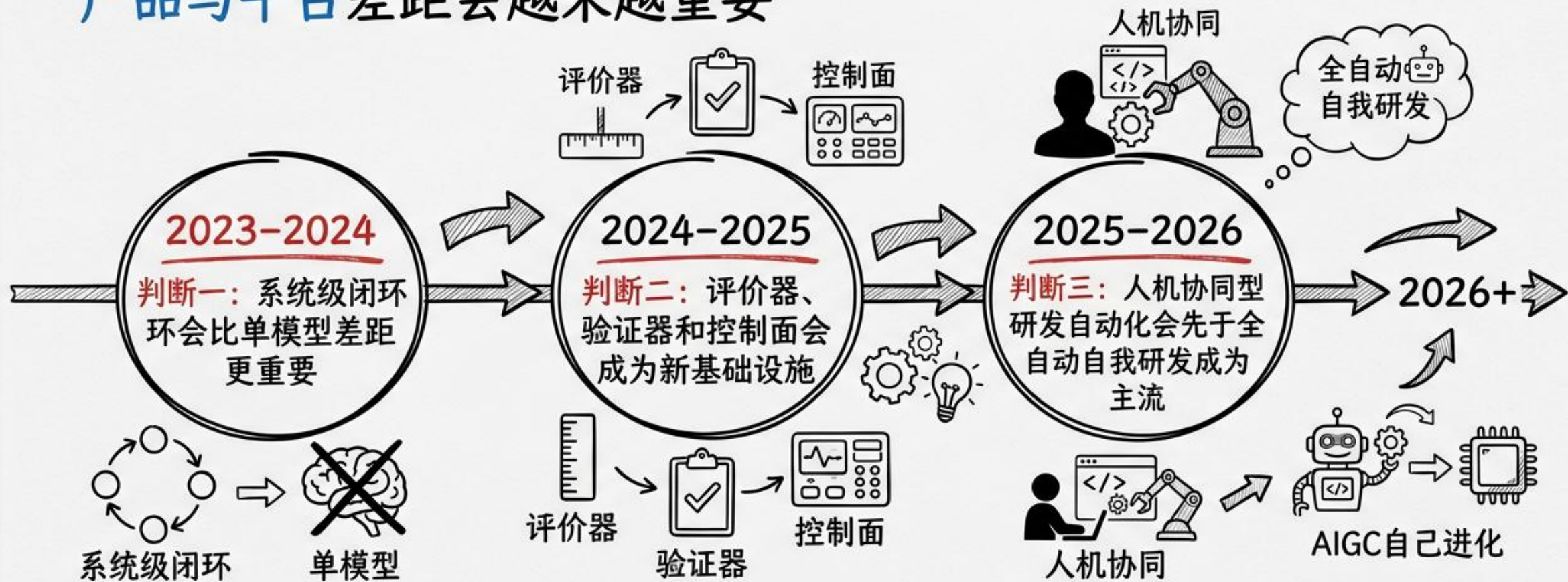
未来三年真正改变格局的，不会只是更大的模型

——本章对未来三年做收束式判断，回答谁会赢、赢在什么地方。

@ 清新研究团队 | 2026年3月

未来三年的五个判断

产品与平台差距会越来越重要



未来真正的竞争单位：闭环系统而非单模型

模型、工具、反馈、治理必须缝合在一起

— 谁拥有更强的反馈基础设施、更丰富的真实任务数据和更稳的评测器，谁就更容易形成系统复利。

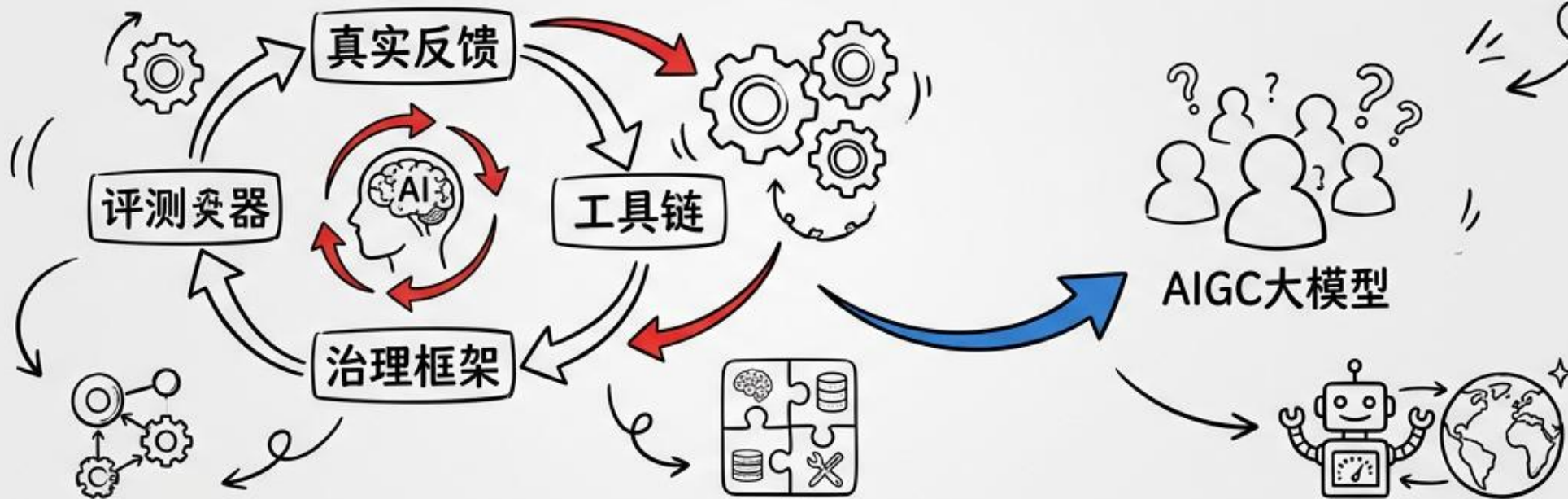
— 未来的护城河将越来越少体现在参数规模，越来越多体现在闭环系统。

— 这也是为什么平台与组织能力会重新变得极其重要。



最终结论

AIGC 自进化已经发生，但主流形态是受约束的系统进化



它当前最真实、最有价值的形态，是系统在**真实反馈、评测器、工具链和治理框架**中持续迭代。



未来的赢家，不一定是拥有最大模型的人，而是能把**模型、数据、工具、业务指标与治理要求**缝成一体的人。

真正改变产业格局的，不只更大的模型，而是**更会从真实世界中学习、又能保持可控的系统**。

感谢观看

THANK YOU



执行人: 杜靖洋



提议人: 沈阳



具体实施: OpenClaw



资料搜索及整理: ZeeLin Desearch



PPT生成: Gemini 

