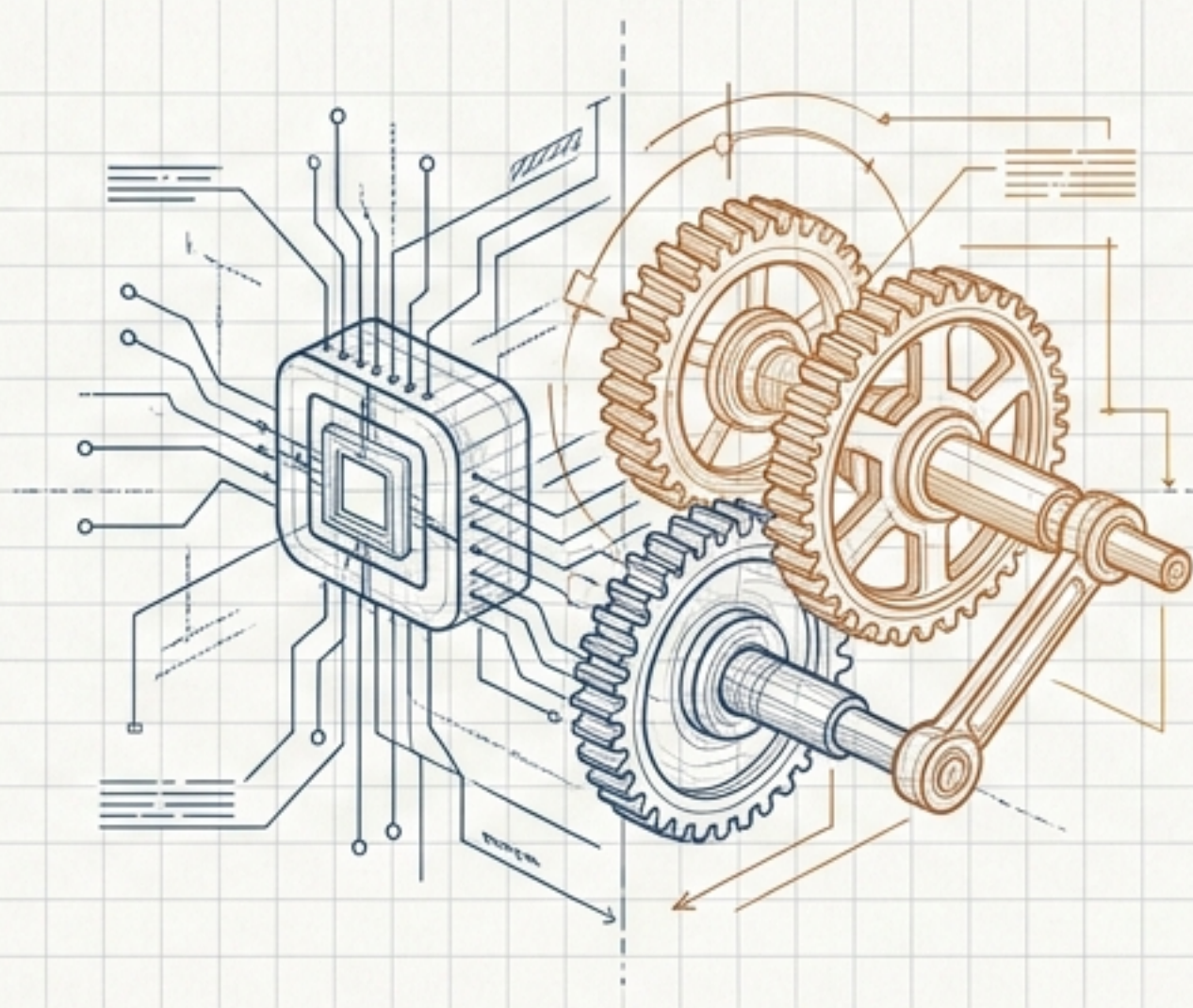


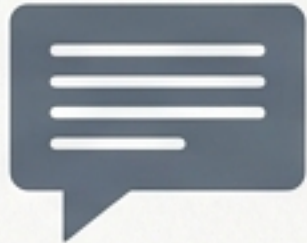
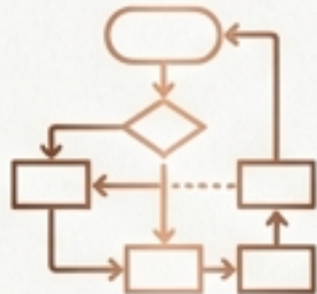
让大模型真正「动手」：OpenClaw 智能体解析



具身智能与物理AI第三讲 · 核心Demo 1 回顾

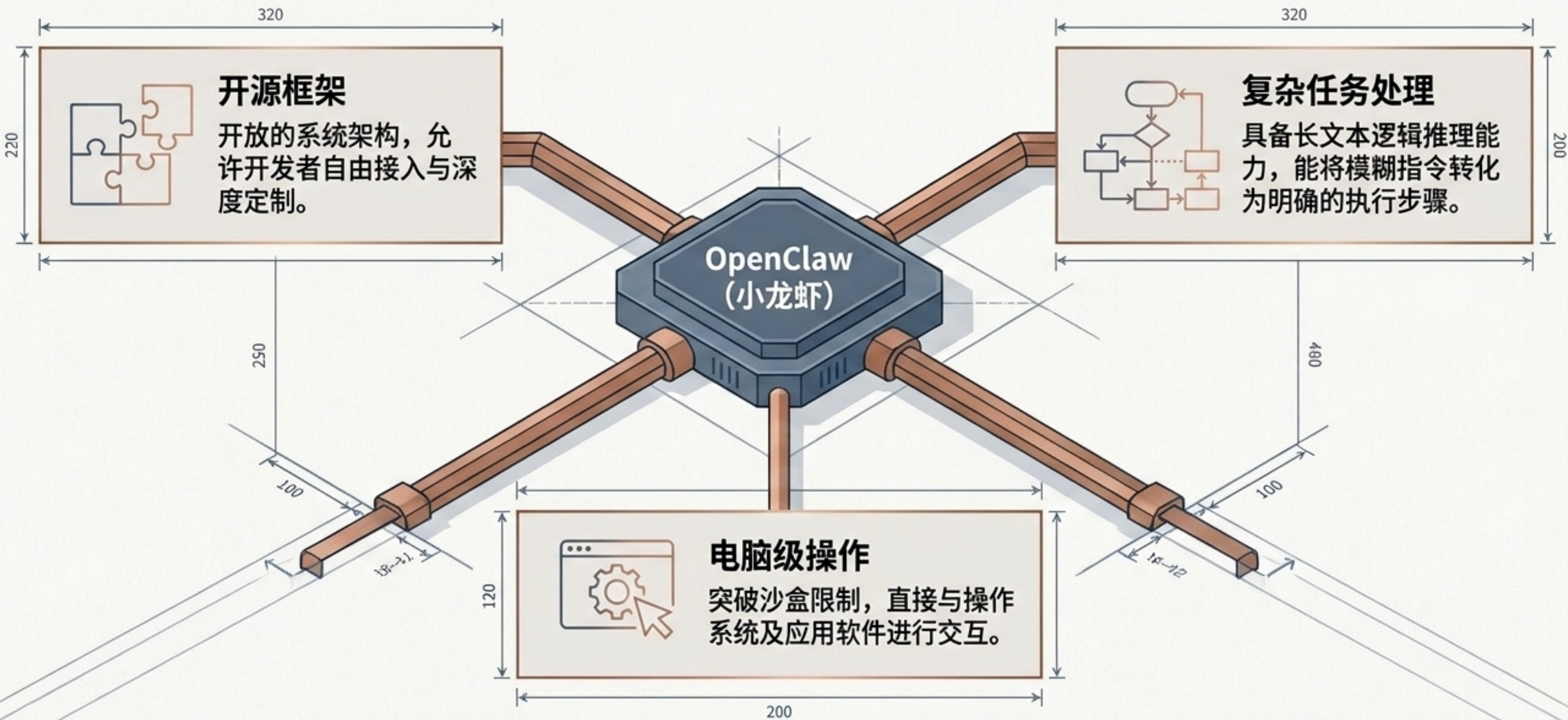
主讲：Michael HUO

范式转移：从「被动对话」到「主动操作」

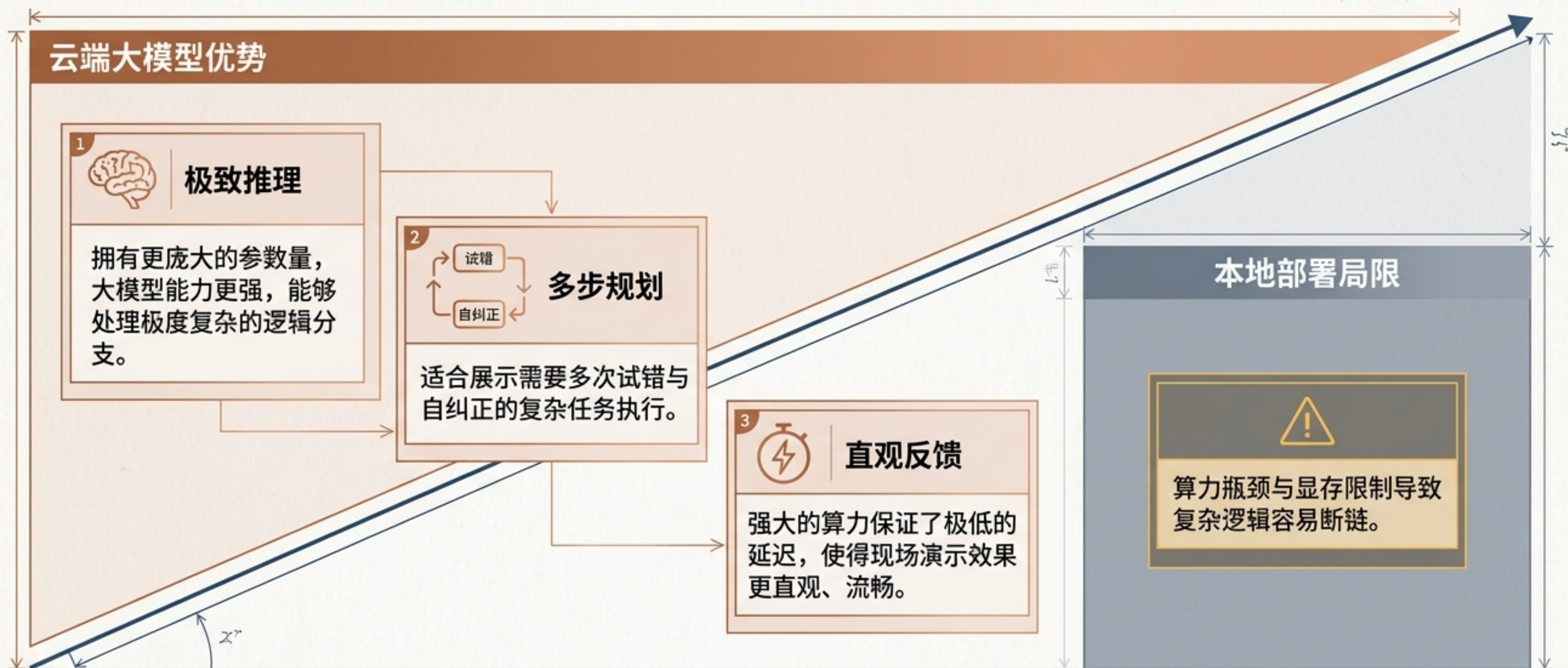
	聊天机器人	智能体（Agent）
核心功能	 文本生成与信息检索	 环境感知与任务执行
输入处理	 单次问答响应	 复杂目标的长期拆解
执行能力	 仅限虚拟对话	 真实操作电脑及工具

核心结论：智能体（Agent）拥有自主决策能力，是连接大模型大脑与物理/数字世界的执行中枢。

认识 OpenClaw（小龙虾）：多步任务的执行中枢

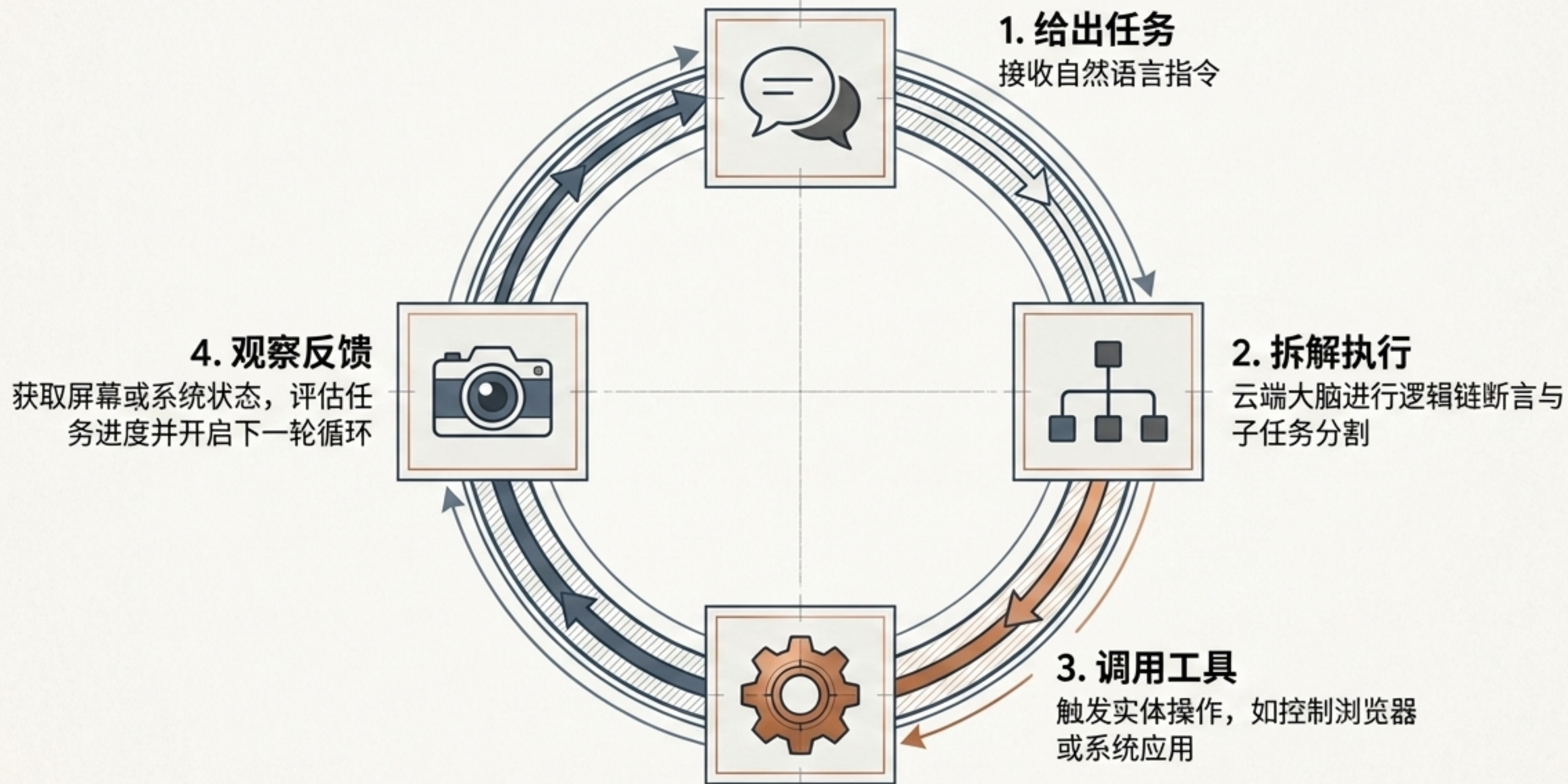


算力与逻辑的博弈：为何选择云端 API 驱动？



核心洞察：复杂智能体的早期验证与演示，必须依托云端 API 的满血算力。

智能体的认知闭环：现场演示的技术拆解



守住行动的边界：系统权限管理是智能体的生命线

内环：动作沙盒

限制智能体只能在特定的浏览器实例或虚拟环境中执行点击和输入。

外环：关键节点确认

涉及文件删除或支付等高危操作时，强制要求人类许可。

核心操作系统

中环：API 熔断机制

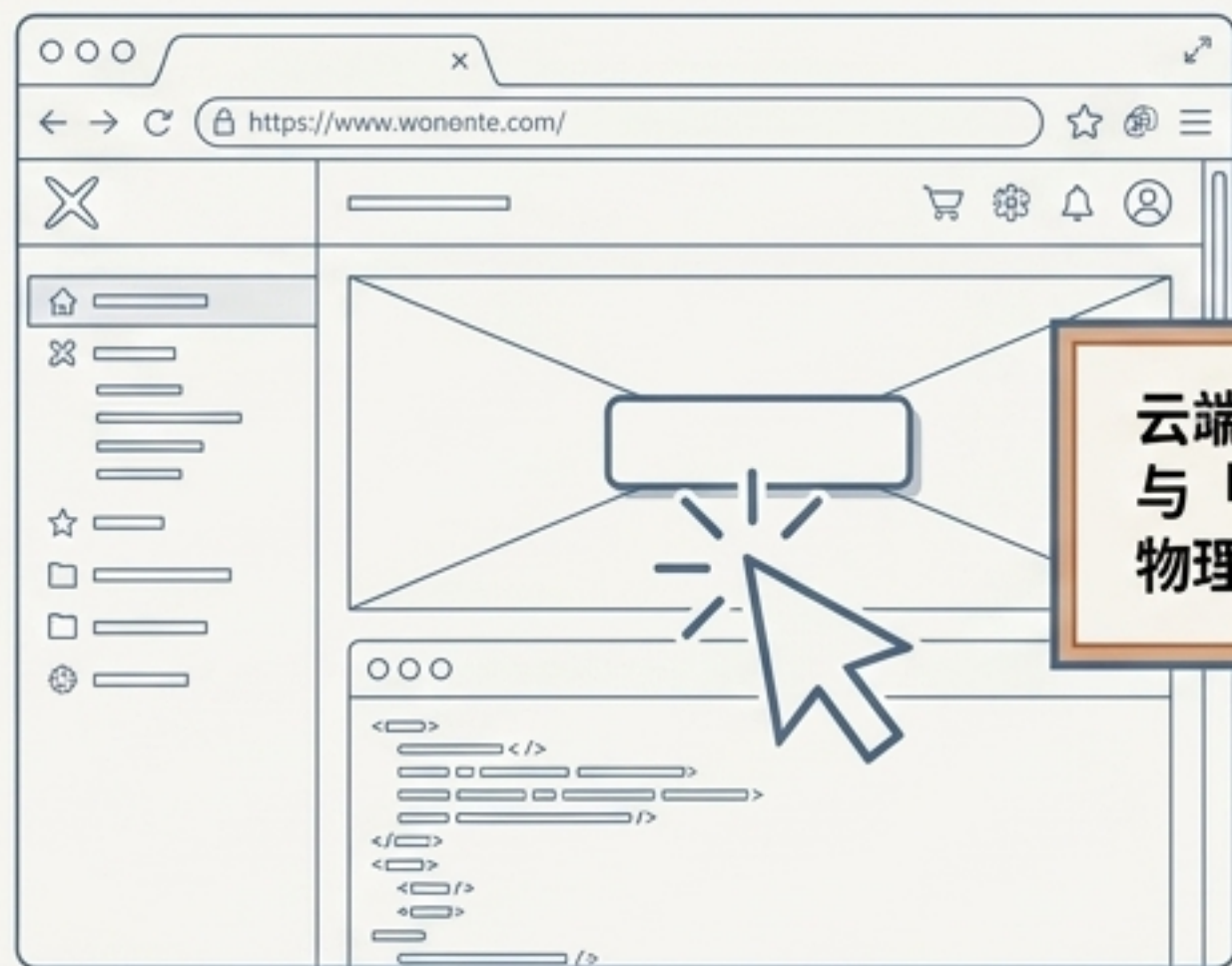
监控异常的高频调用或越权指令，及时阻断风险。

OpenClaw
智能体

赋予智能体行动能力的同时，必须建立多重纵深防御，防止逻辑幻觉引发系统级破坏。

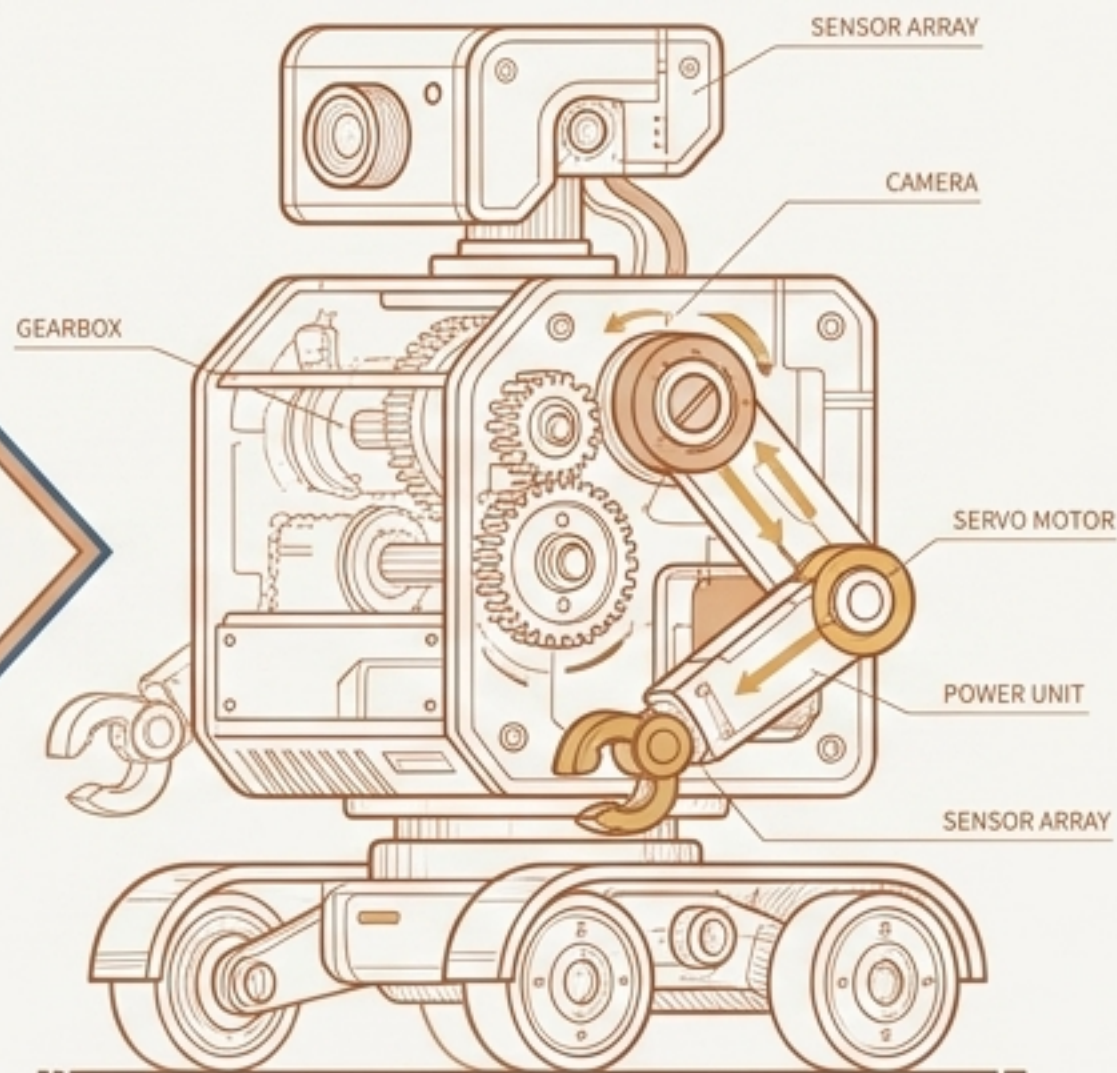
进化的下一步：从「数字底座」迈向「物理具身」

数字空间的执行 (OpenClaw)



云端智能体掌握的「任务拆解」与「工具调用」逻辑，正是驱动物理硬件运转的核心引擎。

物理世界的具身 (StackChan)



逻辑已经跑通，接下来，我们将赋予 AI 真正的物理躯体。