# 高鹏（熊布朗）

## Agent Harness 产品经理 / AI Agent Builder

foreveryh@gmail.com | 18600080486 | 微信：xiaoxia | 𝕏: 熊布朗 | 巴黎&杭州 | 首尔大学 CS 本科 | 英语&韩语 工作沟通

每个项目可点开看演示视频与架构拆解：**resume.deeptoai.com**

## 专业概述

长期围绕一个问题做产品与工程实践：**如何把模型能力转化为可托付、可观测、可恢复的 Agent 任务系统**。

过去两年，长期高强度使用 Claude Code、Cursor、Codex、Hermes 等 Agent / AI Coding 工具，并将其用于真实产品设计、代码实现、调试、交付和自建 Harness 实验。我的主责是 Agent Harness 产品定义，但保持足够强的工程实践能力，用来快速验证想法、理解模型和工具边界、与工程 / 研究团队高质量协作。

相比传统 AI 产品经理，我更关注模型在真实任务中的行为边界：什么时候是模型能力问题，什么时候是上下文组织、工具调用、权限边界、任务拆解、运行环境或交互控制问题。我的工作方式是从真实任务和失败场景出发，定义 Harness 产品机制、用户控制感、数据反馈指标和可迭代的 Agent 工作流。

## Agent Harness 产品判断

| | |
|---|---|
| **可托付：**用户是否愿意把真实任务交给 Agent，而不是只让它回答问题 | **可观测：**用户能否理解 Agent 做了什么、用了什么工具和上下文、成本如何 |
| **可恢复：**长任务中断、工具失败、上下文丢失或模型偏航后，系统能否恢复 | **边界感：**Agent 何时可自主推进，何时必须请求确认，何时应该停止 |
| **失败归因：**区分模型能力、上下文、工具定义、权限环境、任务拆解和交互设计问题 | **共同进化：**把真实任务中的失败和反馈沉淀为 Harness 机制、评测数据和模型改进信号 |

## 核心能力

| | |
|---|---|
| **Harness 产品定义：**工作台、工具治理、会话状态、上下文注入、权限边界、失败恢复和人在环机制 | **模型行为判断：**从输出质量、工具调用、上下文保持、规划能力和错误类型判断模型与 Harness 边界 |
| **AI-assisted Engineering：**使用 AI Coding 工具完成原型、调试、系统集成和交付验证 | **用户体验与产品设计：**把复杂模型能力转化为可理解、可操作、可控制的任务流程 |
| **数据与反馈方法：**任务完成深度、工具调用成功率、人工接管率、中断恢复率、成本和失败归因 | **跨团队推进：**在产品、工程、用户、社区之间翻译问题，快速形成原型、验证假设并推动迭代 |

## 代表项目

### Kin - 客户侧部署的 Co-work Agent / 小团队 Agent Harness | 个人开源项目 | 2026

Kin 是我自建并上线的 Co-work Agent 产品，目标不是做单人聊天工具，而是探索：**当 Agent 进入小团队真实工作流时，如何让它既能长期执行任务，又能被多人共享、接力、观察和控制**。

Kin 主打部署在客户侧环境，例如 Mac mini、私有服务器或团队内网节点，让小团队在自己的数据和运行环境中使用 Agent。产品支持会话共享、多人协作、任务过程可见、会话续跑、工具调用、知识库上下文、权限模式、Preview 沙箱、多模型接入和自托管运维。

核心判断：小团队使用 Agent 时，真正困难的不是让模型多做一步，而是让任务过程可以被团队理解、共享、接力和收束。Agent 的运行状态必须成为团队资产，而不是停留在某个成员浏览器里的临时上下文。

- **共享任务现场：**团队成员围绕同一个 Agent 会话观察、接力和协作，而不是每个人各自与模型对话。
- **客户侧部署：**支持在客户设备或私有环境运行，适配小团队对数据、权限、成本和运维可控性的要求。
- **工具与权限边界：**通过 Skills、MCP、allowed tools、权限模式和沙箱，把“给模型自由”和“让用户可控”放在同一个产品框架里。
- **长任务状态管理：**支持会话续跑、过程可视化、中断恢复和运行状态回传，让 Agent 不依赖单个浏览器连接。
- **可观测与反馈指标：**围绕任务完成深度、工具调用成功率、会话中断/恢复、上下文命中、人工接管率、token 成本和失败归因判断 Harness 是否提升 Agent 能力。
- **关键工程实现：**基于 Claude Agent SDK 构建多用户 Agent 工作台，使用 WebSocket 与每会话独立 worker 承接模型流式事件、工具调用和运行状态；支持 MCP / Skills 管理、知识库上下文注入、Preview 沙箱、多模型 gateway、自托管部署、健康检查、审计日志和用量观测。

### 某城商行分行“客户 360 智能体” | 独立交付 | 2026

面向银行客户经理的真实业务 Agent。用户需要通过自然语言理解客户画像、查询经营与资金趋势、问知识库、跑名单和动账查询；系统同时受到多租户、三级权限、行级安全、审计和可解释性约束。

核心判断：**在金融业务里，Agent 的核心不是“回答得像人”，而是可验证、可追踪、可控**。

- 将自然语言入口拆成文档问答、SQL 查询、客户画像和普通对话等任务路径，避免用一个通用 Prompt 处理所有问题。
- 设计“统一对话入口 + 结构化 Artifact + 双路问答引擎”：文档路径负责检索、融合、重排和带引用回答；SQL 路径负责 NL2SQL、模板/表白名单、安全校验和 RLS 执行。
- **把信任机制作为产品能力设计：**答案可追溯到表/字段或文档/页码，全量写入审计，减少用户把模型回答当成不可验证黑盒的风险。
- **处理真实业务失败场景：**越权查询、SQL 注入、追问丢上下文、画像数据与 SQL 模板串扰、检索误导、结构化输出和文本回答混合返回。
- 通过模板白名单、参数化查询、临时视图、权限隔离和上下文隔离，控制模型自由生成带来的业务风险；使用 4-8 个 Agent 并行推进需求拆解、产品方案、编码、联调和验证。

**Jumpxai AI 实战训练营 / AI PPT Studio** | 联合创始人 & 主讲 | 2026

创办并主讲 AI 实战训练营，同时把课程、demo、Skill 和 Web 工具做成可复用的教学产品系统。核心不是做课程，而是验证复杂模型机制如何被普通用户理解、操作并转化为真实产出。

- 通过 4 周 AI 实战训练营，帮助零基础用户理解机器观、上下文工程、Agent 和 Vibe Coding，并最终做出可运行项目。
- 设计神经网络、Transformer Self-Attention、ChatGPT X-Ray 等交互 demo，把抽象模型机制变成可操作界面。
- 将 PPT 生成能力拆成 jumpx-ppt-forge Skill 引擎，沉淀输入契约、质量门禁、风格体系、角色手册、渲染规范和 demo 样例。
- 在 Skill 外层设计 AI PPT Studio Web 操作台，覆盖多格式输入、人工确认、HTML 预览、导出和演示模式；通过真实用户使用反向修正产品流程、交互节奏和提示边界。

## 其他 Agent / Harness 实践

**Neuxnet.AI 产品线 / NEOM 企业 Agent | 2023-2026：** 负责 AI 产品方向规划、项目落地与团队建设，覆盖 ToB / ToC 双线。带 5 人核心团队，按阶段协同 5-15 人跨职能团队，推进 RAG、Deep Research、Character AI、类 Manus 智能体、行业 Agents 等产品。代表项目包括 NEOM 企业 Agent：以企业 RAG 为底座，覆盖 Chat 智能问答、合规检查、数据 Dashboard 和图纸检测等多模态场景。

**mentis / MentisSandbox | Multi-Agent 与 Agent 沙箱 | 2025：** 围绕 Multi-Agent / Subagent 做的研究型产品实践，配套 Agent 代码执行沙箱。核心判断：Multi-Agent 的难点不在多几个角色，而在任务拆解、上下文隔离、结果回收、错误传播和协调成本。任务线性、上下文共享强、延迟或成本敏感时，单 Agent + 好工具 + 好上下文往往更稳定。

**小红书自动化运营 Agent | 2025：** 面向内容运营团队的浏览器自动化 Agent，用于辅助低风险、可审计的重复运营任务，关键发布与风险动作由人确认。产品重点是行为前置判断、风控状态机、健康/限流信号监控、异常降速/隔离/恢复、全程审计和人在环机制。

## 数据与评测方法

- **任务级日志：** 把用户意图、上下文来源、工具调用、模型输出、人工接管和失败恢复组织成可复盘记录。
- **指标设计：** 围绕任务完成深度、工具调用成功率、上下文命中、人工接管率、中断恢复率、成本消耗和失败归因衡量 Harness 价值。
- **反馈闭环：** 把真实用户任务中的失败案例转化为产品机制、评测数据、标注策略和模型/工具改进线索。

## 公开项目与社区信号

**Kin：** 客户侧部署的 Co-work Agent / 小团队 Agent Harness

**langgraph-deep-research：** Deep Research 场景的多阶段推理与资料整合工作流

**Awesome-LLM-RAG-tutorial：** 原创 RAG 教程站，面向学习者和开发者解释 RAG / Agent 基础问题

**cloneui：** 从网页结构提取到可复用前端代码生成的 AI 辅助原型工具

**mentis / MentisSandbox：** Multi-Agent / Subagent 编排与 Agent 代码执行沙箱

**jumpx-ppt-forge / AI PPT Studio：** AI PPT 生成 Skill 引擎与 Web 操作台

**JumpX-Labs AI Bootcamp Demos：** 神经网络、Transformer Attention、ChatGPT X-Ray 等课堂交互 demo

## 可提供验证材料

- **Kin：** 线上环境、源代码、 Agent 教程、架构说明、关键模块代码、客户侧运行与自托管路径说明。
- **银行 Agent：** 在脱敏前提下展示产品方案、任务链路、权限/审计设计、RAG / NL2SQL 安全机制与上下文隔离方案。
- **AI Coding 工作流：** Claude Code / Cursor / Codex / Hermes 在真实项目中的任务拆解、代码实现、调试与联调样例。
- **课程与工具链：** Jumpxai 训练营、AI PPT Studio、PPT Skill、模型机制交互 demo 与学员反馈记录。

## 工作经历

**独立 AI Agent 项目负责人 / Jumpxai 联合创始人** | 2026.01 - 至今

独立推进 Agent Harness 产品、企业级 Agent 交付、公开项目和 AI 实战训练营。

**Neuxnet.AI | AI 产品线负责人** | 2023.08 - 2026.01

负责 AI 产品方向规划、项目落地与团队建设，覆盖 ToB / ToC 双线。主导 RAG、Deep Research、Character AI、类 Manus 智能体、行业 Agents 等产品从需求调研、方案定义、研发协作到上线迭代。

**LINE Plus Corporation（韩国） | 中国区负责人 / 法人代表** | 2013.04 - 2018.07

负责 LINE（IM） 及相关产品在中国市场的本地化、用户增长、商务合作和团队管理，参与 B612 等产品中国区落地，形成跨国协作、平台产品、本地化增长和团队管理经验。

**［两次创业］空瓶集 （定制化护肤） / 途客圈（定制化旅行）** | 2018 – 2022 / 2011 – 2013

2018 创办数据驱动型美肤选品平台，负责产品设计、运营规划、团队搭建和商业化闭环；2011 移动互联网初期从事定制化旅行类创业项目，为后续产品、工程和创业实践建立基础。

## 教育与语言

**首尔大学 Seoul National University | 计算机科学与技术 | 本科**　　英语：工作沟通 | 韩语：工作沟通