手工川 AI 创造营 · 第五期 · 第一天

造一台自己的 Agent 工作台

DeepSeek Harness 实战 · 2026 年 9 月 5 日 · 上海陆家嘴

开场白

先坐下来，喝口水

上午

10:00—12:00
只讲，不动手

软件、AI、Agent、DSH
四块通识

中午

12:00—13:00
边吃边装

第三期我们提前了三小时
还是没装完
今天这一小时专门用来装

下午

13:00—18:00
一直动手

上手、装插件、开发插件
发布、打造工作台

这两天结束，我们不会散

线上

不定期
seminar

线下

小规模
聚会

往后

超级个体
孵化

开场白 · 前四期

每一期都是被上一期逼出来的

一期 · 北京原点大厦

单天 8 小时

理论太多，实战不够。
下午那份 60 页 PPT，
是我中午半小时生成的。

二期 · 上海中信书店

切成两天各 4 小时

「AI 大夜校」。
那天书店灯火通明，
亮过隔壁飞书大厦。

三期 · 上海隽宜律所

工作人员提前 3 小时

还是没能解决所有人的环境。
我才明白得因材施教。

四期 · 陆家嘴数智港

16 小时 OPC 黑客松

7 位学员，7 件作品。
一位升职成了跨部门负责人，
一位零编程的产品经理
在小红书比赛拿了名次。

开场白 · 自我介绍

我的四个年份

2014

接触炒股

从挂科开始。
三个月写了三十多款策略，
最贵的一款卖 3000 一份。

2020

探索创业

考了五次清华软件。
写了个压缩算法把上下文压进 6K，
几个月后窗口涨到 200K，
白写了。

2024

Claude 奥德赛

本来想招人。
后来发现一个月 200 美金就能开工。

2026

各地演讲

北京、上海。
今天是第五期。

开场白 · 现场介绍

轮到你们了

自由座位，一人一分钟。

我是谁，我想让 AI 帮我做什么，上周这件事发生了几次。

第三句最重要。说不出次数的，说明这件事你其实没那么想做。

嘉宾和助教也各说一分钟

软件通识

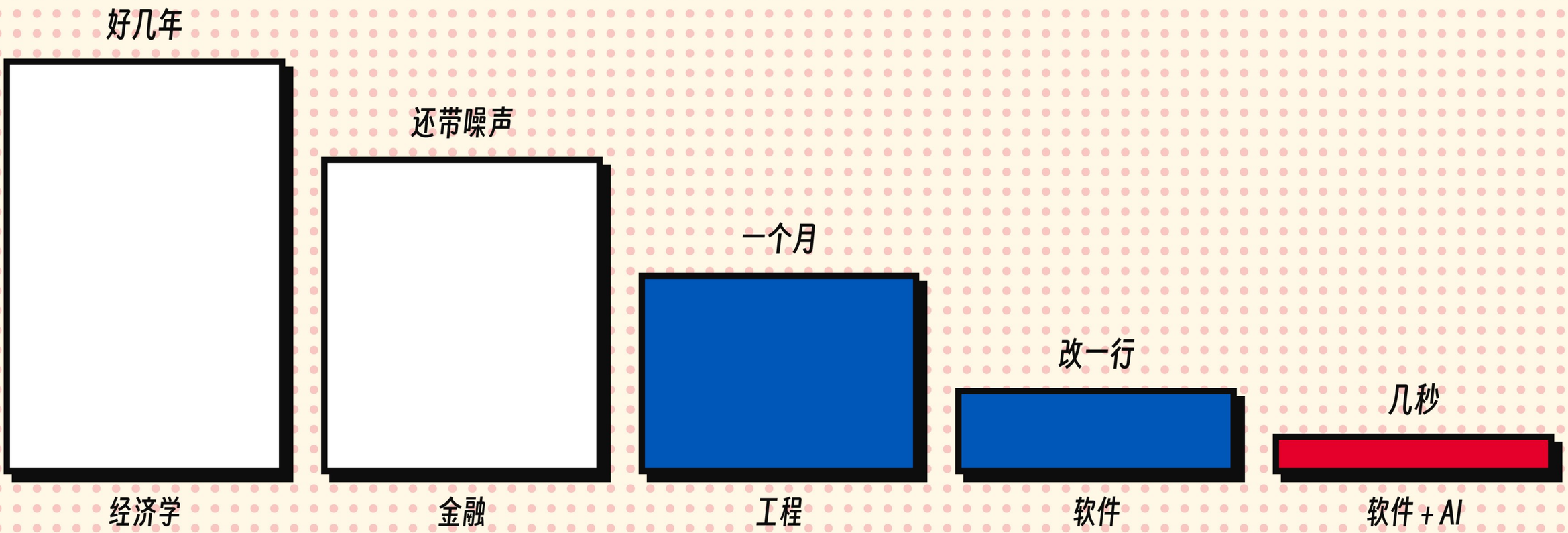
软件是把一件反复要做的判断，变成一个能按的按钮

注意是「判断」，不是「一件事」。

每次都得想一下，但每次想的路数其实一样——那种才值得做成按钮。

软件通识

我换过四个行业，换的是等答案的时间



软件通识

炒股那几年教我的一件事

今天赚的，明天会吐回去。你永远在原地起跳。

写下来的东西不会。明天它还在，而且下一个东西还能调用它。

所以这两天我们不做 demo。demo 演完就没了。

先说清楚它是个什么东西

白板手绘：输入 → 一个巨大的、见过很多东西的函数 → 输出。

它不查数据库，也不会「记住」你昨天说的话。
你这次给它什么，它就凭什么答。

这一页在白板上画

两根轴：时间和钱

钱

一路往下

以前要招人、发工资、租办公室。
现在不用了。

时间

一路往上

钱不再是门槛之后，
唯一还挡着你的就是时间。

AI 通识 · 为什么要用

一个月 200 美金

这是我 2025 年三四月开始用 Claude Code 之后的实际开销。
一个人开一家公司，启动成本就是这个数。

坦白说，如果不是 AI 到了这一步，我根本承担不了大家的众望。

电脑送修，要等一到四小时。你会拿这段时间干什么？

这一问不用急着回答。

写在你手上那张卡的背面，明天结营的时候我们念出来。

钱和工具都不缺，结果差很远

7 人 · 8 周 · 99% 交给 AI

30 行

八周里他们一共手写了三十行代码。
上线之后，比另一条百万行人写的产品
bug 更少、满意度更高。

一家美股上市公司

1000 万

办了场内部黑客松。
最后办成了一场秀。

两个都是第一期台上嘉宾讲的

三件让我愣住的事

8:50

那天上午签到表还没打出来。
我打开 Claude Code，它自己挑了配色、写了后端、拉好了内网穿透。
学员扫码按下名字，名字就在大屏上亮了。

60 页

第一期下午四小时用的 PPT，我中午半小时生成的。
效果好到我自己不敢信。

设计 → 实现
→ 审阅 → 再设计 ↻

有一次上下文被压缩，它误以为要重构，于是自己给自己安排了一个循环，几分钟后交出一版，一次过。

这一件最吓人。

AI 通识 · 我做到的

一台工作台，四轮抓完 3839 个活动

3839

四轮

1 翻不动页 → 改切分

2 被封 IP → 降速率

3 弹验证码 → 限页数

4 125 分片 x 每片 12 页

四轮里没有一轮是原样重跑。
每次失败，改的都是配置。

AI 通识 · 轮到你们说

你想让它替你干的那件事，到底长什么样？

我们现在把每个人的诉求写到白板上，当场归类。

这一步很重要：**今天时间只够打磨一件事。**
上周没发生过两次的，今天先放一放。

你脑子里有，它不知道的那些事

我知道 · 它也知道

公共知识

大家都一样，不产生差别

我知道 · 它不知道

你今天下午的活基本都在这一格

上次为什么否掉那版，你不写它永远不知道

我不知道 · 它知道

最容易被浪费的一格

大部分人从来不问它「这里有什么我没想到的」

都不知道

得做实验才知道

AI 通识 · 如何驾驭 · 方法论

结果不对的时候，你改的是那句话，还是那个文件？

如果你第二轮跟第一轮的区别只是「我又说了一遍」，那不叫改进。

刚才那个 3839 的例子，四轮下来我一句话没重发，改的全是配置。

AI 通识 · 如何驾驭 · 圈子

一个人琢磨，会琢磨很久

这两天认识的人，大概比这两天学的工具更耐用。

我自己长期在几个圈子里泡着——手工川这边的社群，还有生财有道。
信息差是真实存在的，而且越来越参差：**坦白说，就连我都搞不定稳定的 Claude 账号。**

人和它的位置，这些年换了四次

当年以为

它干活
人写诗

实际发生

它写诗
人打标

现在大多数人

人卡在
流程中间

每一步都要等你点头
你成了最慢的那一环

今天想往这儿挪

人站在
闸门上

该停的地方停
其余让它自己跑

卡在第三格不丢人

Agent 通识

聊天框只有一层，工作台有四层

上下文	它凭什么知道你的事
模型	谁在想
能力	它能动手做什么
闸门	什么时候得停下来问你 —— 你站这儿

下午每做一件事，都能对上其中一层

同一个模型，晚上做出来的东西会差很远

今天全班

1

个模型，同一个版本

今晚会出现

8

套完全不同的结果

差的不是模型。
是你喂给它什么。

Agent 通识 · 闸门

「昨晚的 PPT 被我自己跑的某个 agent 覆盖了。
我花了一小时回滚 git 才找回来。」

—— 第一期台上嘉宾

你既得信它，又得随时准备替它擦屁股。

下午动手之前，每个人先 commit 一次。

DSH 通识 · 轨迹

我换过的三台机器

2024.10 · Cursor

它帮我补全

证明这条路走得通

2025.03 · Claude Code

它帮我干完

工作流开始沉淀
但机器本身我动不了

2026 · DSH

我能拆开它

前两台你是用户
这一台你能当装配工

今天讲的是第三步

DSH 通识 · 为什么是它

没有特权内核

官方文档原话。模型适配、工具注册、会话日志，连 agent loop 本身，都是插件。
所以不会写代码的人，第一次也能重新组装这台机器。

说实话它还很早，0.1.x，最近一周发了六个版本。所以今天全班锁死一个版本号。

中午 12:00 · 边吃边装

输入框是灰的，只有两个原因

一

没选工作区

二

没选模型

装不上也不耽误下午：用助教的机器、跟同伴共用、或者先走网页版。不会有人被落下。

实操 · DSH 上手体验

先让它读一遍你的工作区

「看看我这个目录里都有些什么，说给我听。」

它说得准不准，其实是在照你的目录。

说不准的，先别怪模型，去看看自己的文件夹。

实操 · 安装一个插件

大胆装，大胆卸

装两三个，每个都跑一次，没用的当场卸掉。

敢卸是有底气的：卸载的时候，注册的事件和工具会自动摘掉，定时器这类东西用 ctx.effect() 也会一起回收。

顺便说一句，你们待会儿用的那个插件市场，官方没有，是我自己写的一个插件。

实操 · 开发一个插件

你今天想开发什么？

别从「我想做个 AI 功能」开始想。
从「我今天干活的时候被绊了一下」开始想。

我那七个插件，全是被绊出来的：看不见余额、命令记不住全名、改完配置要重开、找不到别人的插件、每次都得重新交代一遍规矩……都是小事，都是真烦。

挑那个一小时能做完的。

每人写一句，贴出来

实操 · 发布一个插件

让同桌装一次

先自己用顺手，再谈发布，顺序别反。

我那个插件市场，也是先自己用了很久，才变成别人也在用的东西。

能被同桌装上并跑出结果，今天就算发布了。不强求发 npm。

实操 · 打造工作台

关掉电脑，明天重开，东西还在

今天的零件拼起来，四层对一遍：工作区、模型、装的插件、你按下过的那次「不对，重来」。

然后换一个真实的输入，再跑一遍。**一次跑通可能是运气，两次才作数。**

17:40 收口

收口

明天第一件事，你想把哪一步交给它自己跑？

今晚就一件作业：把今天的工作区打开一次，换个输入跑第二轮。
跑不通不要紧，把报错截图发群里——那是明天上午最好的教材。

明天上午我们互换工作台。