

GIAC 2026 / HARNESS ENGINEERING 专场

通往 Harness 之路

如何用**确定性的约束**驯服不确定的基础设施

业界讲三个维度——时间 / 空间 / 交互。
我押的，是被低估的第四维：**范式**。

手工川 · LovStudio.ai 创始人 / yoda 作者 / 本专场出品人

交时
互间

范空
式间

IDENTITY

我是谁

- 手工耿的手工
- 琥珀川的川
- 用作品定义自己

LOVSTUDIO

每美驱动 科技博主 独立开发者

创业者 开发者工具 终身学习者 产品创造者

AI 创造营 Lovcode

any2doc Lovclip Lovshot any2deck Claude Code One Person Company

Agent Skill 开发者 Yoda 背包客

微探 数字游民 WDB Lovpen

Lovtarot Lovoice

兰纳照妖镜 Vibe Coding any2pdf Lovmind Lovsider AI 大夜校 个人产品宇宙

write-professional-book

any2pdf

AI 布道师



手工川工作室
LOVSTUDIO PRODUCT LAB

MATRIX 2026

AI 原生工具 · 内容自动化 · 开发者生态

产品矩阵

手工川主理 Lovstudio、Lovpen、Lovcode，长期关注内容创作与开发者工具，正在构建面向超级个体的 Super Creatorpreneur OS。

AI Coding

Creator Stack

Obsidian

Skills & Training

4
主线产品

2
LovPen 架构

27+
产品与服务

OS
超级个体系统

主线产品

主线重心收敛到 AI Coding、写作系统和 Skill 交付，其他产品作为矩阵能力沉淀。



AI CODING WORKBENCH
LovCode

AI 编程工作台，承接项目、上下文、Agent 协作与交付规范，是开发者产品线的主入口。

AI Coding

Agent Workflow

Developer OS

01



AGENT TRAINING
Yoda

多 Agent 编排与 AI Coding 训练，把复杂任务拆成可复用的协作套路。

Parallel Agents

Training

02



OBSIDIAN + WEB
LovPen

双架构写作系统：Obsidian 插件负责知识沉淀，Web 端负责内容生产、发布与 workflow 编排。

Obsidian Plugin

Web App

Creator Stack

03



AGENT SKILL
WriteBook

把专业书稿从大纲、章节到排版的长链路固化成可重复调用的 Skill。

Long-form

Skill

04

完整产品地图

AI AI Coding 向

Agentic coding, 本地服务
编排, AI 编程工作台

**Yoda** Beta
多 Agent 编排与 AI Coding 训练

**Vmux**
本地服务控制台

**LovCode** Beta
AI 编程工作台

文 内容创作向

选题、写作、语音、剪辑、剪辑板与思维导图

**LovPen** Beta
Obsidian + Web 双架构写作系统

**Voca**
语音转写与文稿

**LovClip**
剪辑板素材中心

**LovSlider**
浏览器侧边工具栏

**LovShot**
截屏录屏与演示

**Folo**
信息记录与汇总

数 微信生态

03

**WDB**
聊天数据库解析

**微探**
公众号内容采集

**Tencent Meeting Cracker**
会议元数据与笔记导出

Obs Obsidian 专辑

经典插件: 目录、图片、格式化、替换、代码高亮
与历史对比

**Better TOC**
更好用的笔记目录

**Image Auto Upload**
自动上传图片

**Lint**
Markdown 格式规范

**Regex Replace**
正则替换与批量编辑

**Shiki Highlighter**
代码语法高亮

**Version Diff**
版本的历史更改对比

SK Skills

05

**WriteBook** Beta
专业半自动化生成文档

**Any2PDF**
多格式转 PDF

**Any2Deck**
内容到演示稿

开发生态

06

**Lovinsp**
桌面页面元素定位源码

**Mac Toolkits**
桌面软件管理与模块化工具

训 线下培训

唯一线下服务:
李工川 AI 创造营

**手工 AI 创造营**
线下 AI 产品与工作流实践

玩 娱乐项目

保留探索感: 互动、占卜、镜像与符号生成

**LannaMirror**
镜像互动实验

**LovTarot**
塔罗互动与叙事体验

**LovSigil**
意念符号生成

用手工精神做 AI 原生产品

扫码关注手工川, 持续记录产品实验、AI Coding、内容自动化与手工川 AI 创造营。



Designed for 手工川工作室 · LovStudio Product Matrix

©lovstudio

VOL.001 · ISSUE 2026.04 SHANGHAI · 上海 · 陆家嘴数智港 · 印行 FREE COPY

THE OPC TIMES

"More than machinery, we need humanity." — Chaplin, 1940

N° 001

— HEADLINE —

一个人 + AI = 千军万马

手工川入驻陆家嘴数智港，把“一人公司”造成下一代创作者操作系统

BY MARK SHAWN · FOUNDER, LOVSTUDIO · 2026.04 · ON THE BUND

What — 我们造什么

Lovstudio 正在打造 “AI + 知识库 + 创作 + 分发” 全闭环的 Creator OS。我们用“一人公司 (OPC)” 本身的方法论，给 OPC 用的工具。

主干 Lovpen，护城河 lovstudio/skills，试验田 Lov* —— 三层结构，全部开源、全部 dogfooding。

Why — 为什么是现在

一 条曲线交点：
① Solo Founder 占新创企业 **36.3%** (Carta 2024, 50 年首次)；
② 创作者经济进入“工具化下半场”，**\$250B → \$480B**；
③ 中国 OPC 浪潮 5 个月从一场大会升级为政策基础设施。

就在 Lovstudio 准备好产品矩阵的同一时刻，国家正在为这批“一个人的公司”铺基础设施。

Where — 为什么是陆家嘴

陆家嘴数智港地处北滨江新市民洋板块，由百年码头集群转型为互联网与数据要素产业引擎。

金融、科技、海派、滨江，四种力量在这里交汇。手工川在这里办公，在这里造产品，在这里把“一人公司”变成可以复用的方法论。

— BY THE NUMBERS · 数据存档 —

40w+
天使融资

8+
孵化器

40+
城市温度

10+
开屏 SKILLS

24h
自我验证

"We're the customer of everything we build.
我们自己每天用 24 小时，验证 24 小时。"

EDITORIAL · 编辑部

手工川

手工川 Mark Shawn

Founder · Lovstudio · mark@lovstudio.ai

SUBSCRIBE

公众号「手工川」

github.com/MarkShawn2020

v0.1 · MANIFESTO · 1888+1920

› 我最重要的关于 AI 或者创业的几场活动，按时间排序罗列

- 结论先行——剔除参会/凑场，按时间排序，真正分量重的 AI/创业活动是这 8 场：

时间	活动	为什么重要
2025-07-19	Lovpen 产品发布会 @五道口东升大厦	个人首场产品发布会，正式立项出圈
2025-08-31	智谱 demoday Lovpen 路演	人生第一次正式路演，多次 pivot 后的收敛之作
2025-12-05	上海 vibe coding 技术沙龙（红杉中国加速器场地）	首个有头部机构背书、报名满的自办技术沙龙
2026-03-14	龙虾大会 @东升（× 清华创协）	一手策划、双主题主讲、报名 400+，奠定个人 IP
2026-04~05	手工川 AI 创造营 一/二/三期（京沪，~80 学员）	自有教育 IP，首次全方位公开 AI 工作流
2026-05-13	百度 AI 开发者大会主讲《通往 OPC 之路》	登上大厂舞台，主题分享
2026-05-19	南沙千人 OPC 峰会 + 发改委/浦东座谈会	以**"首批/首家 OPC 代表"身份进入政策层
2026-05-27	奥迪中国高管全英分享《AI Agents In Practice》	首次企业级英文 keynote，B 端背书

如果只留 3 场代表作：Lovpen 发布会（2025-07）→ 龙虾大会（2026-03）→ 手工川 AI 创造营（2026-04）。



LLM = 不确定的 基础设施

概率性 · 无栈追踪 · 边界飘忽

Harness = 确定性约束

业界把 Harness Engineering 讲成三个 scalability 维度——**时间、空间、交互**，三巨头各解一维。

但他们优化的都是 "**agent 怎么工作**"，集体漏掉了第四维：**软件工程 / 开发范式**。

Harness 决定 agent 能跑多久、多大、多省心；开发范式决定一个团队能不能**可复制地用好 agent**。我押的，正是这被低估的第四维。

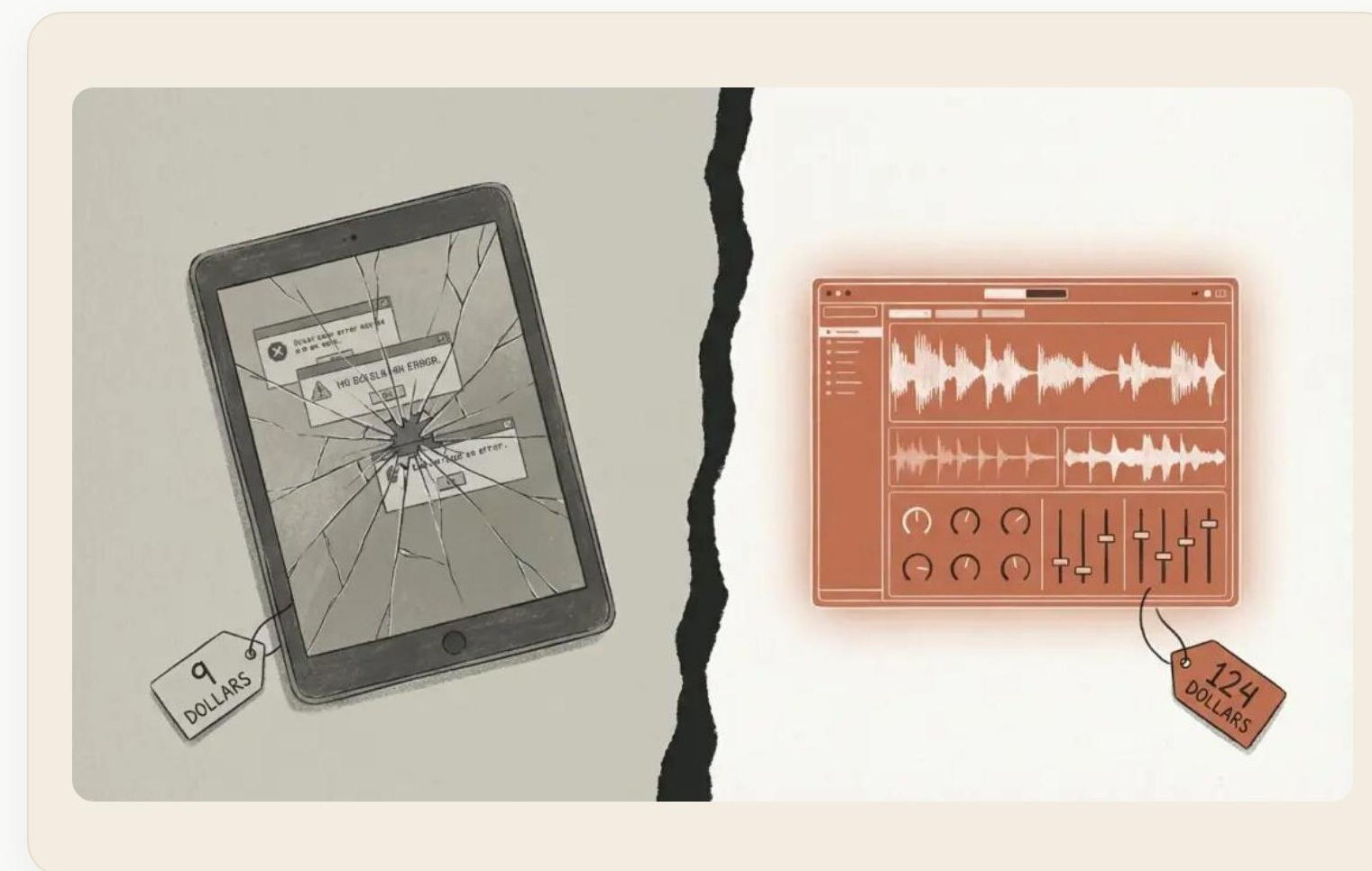
开场 / HOOK

\$9 的废物 vs \$124 的可用产品

- ◆ 同一个 prompt，单 agent 跑 20 分钟、花 **\$9**，产出不能用。
- ◆ 换一套 harness：3 小时 50 分、**\$124**，产出一个能用的数字音频工作站。

这 15 倍的钱，
买的就是 **Harness**。

崩、跑偏、累——业界都把它统称 Harness Engineering。但真的是同一件事吗？



\$9 的废物 vs \$124 的可用产品。来源：Anthropic HAZE 案例

概念锚点 / EVOLUTION

演进三段论

这张图你们都见过，被洗稿了几百遍——但大多数人只换了名词，没换内核。



核心不是"换个词"，而是把"改 prompt"升级成"改环境"。

“

每当发现 agent 犯错，就花时间工程化一个方案，让它再也
不犯这个错。

— Mitchell Hashimoto

配套的 stop-doing list: "我决定何时打断 agent，它无权打断我。"

**Harness Engineering 的核心，
是为 AI 创造一个适合它的环境——
最好这个环境能让它自我验证、自我进化。**

转折 / SAME WORD

同一个词， 解的不是同一道题

- ◆ 读完三巨头的一手报告后，我发现一个被忽略的事实。
- ◆ 他们用着**同一个词**，却各自在解一个完全不同的维度。

别再问 agent 是不是 Model + 缰绳。
先问：你在解哪个维度的 scaling?



一手报告里的 agent 工作流 (Codex x App x DevTools 闭环)。来源：OpenAI / Anthropic / Cursor 报告

先看共识：四条地基

01

人的核心工作变了

从写代码 → 设计 agent 的工作环境。

02

知识必须存在于 repo

版本化、可发现。**agent 看不到的 = 不存在。**

03

约束 > 指令

CI 加覆盖率门槛 > 嘴上说"记得写测试"。

04

纠错 > 等待

完美主义是吞吐量的敌人。

所以，四大问题

01

时间

Time

一个 agent 怎么连跑几小时不崩？

Anthropic

02

空间

Space

几百个 agent 怎么并行不乱？

Cursor

03

交互

Interaction

人怎么管这一切不累死？

OpenAI

04

范式

Paradigm

怎么把 agent 纳入工程化的开发范式？（标准 · spec · 多智能体 · review）

我的主场 · yoda

前三维让 agent 单次干得顺；第四维让团队可复制地用好 agent。

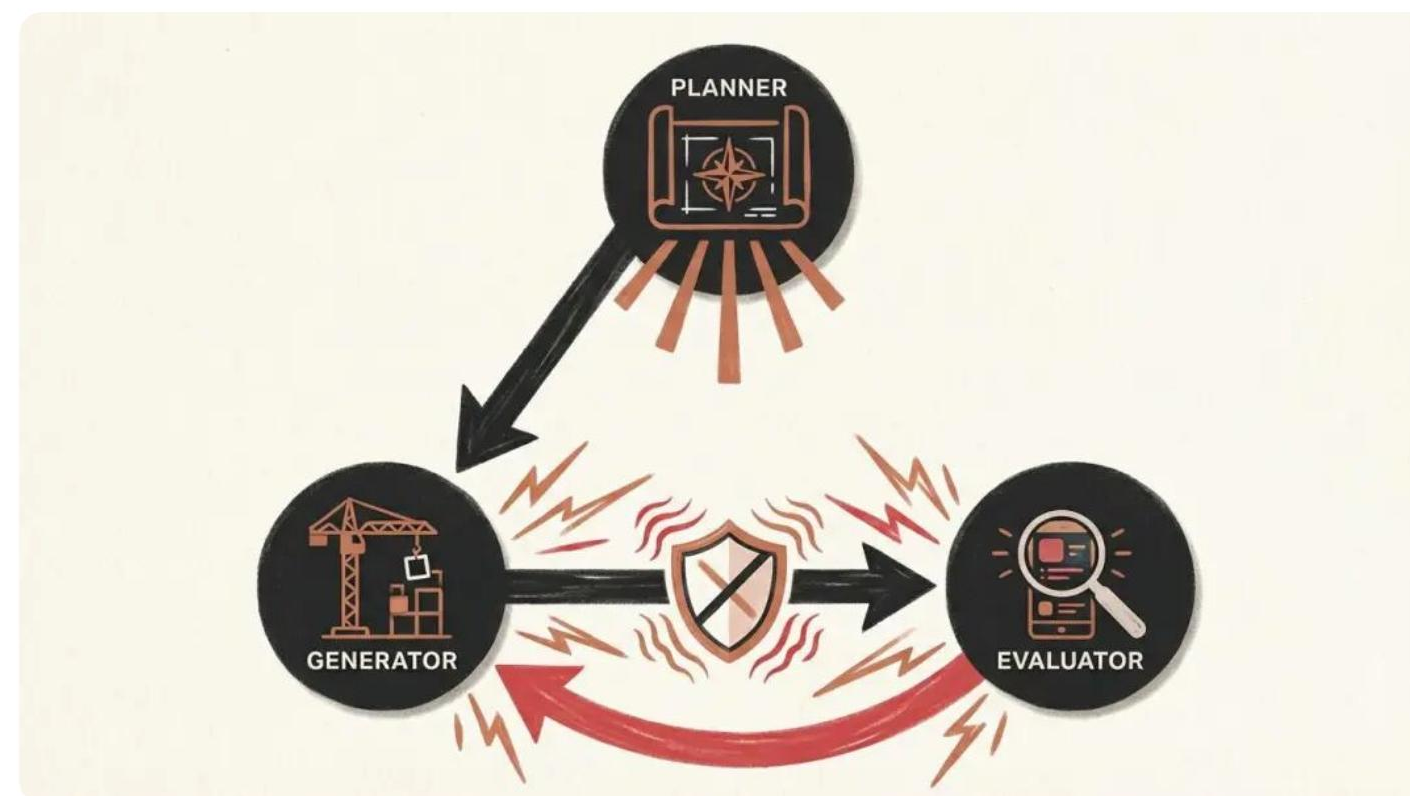
维度一 / 时间

维度一 · 时间 Scalability

◆ **问题** agent 开始干活后，怎么连跑几小时不漂移、不自我合理化？

◆ **解法** Planner → Generator → Evaluator 三角色（GAN 启发）。关键：Evaluator 与 Generator **无共享状态**——独立性是纠偏的前提。

◆ **反直觉** harness 组件随模型变强应**减薄**而非加厚。新模型发布，先做减法。



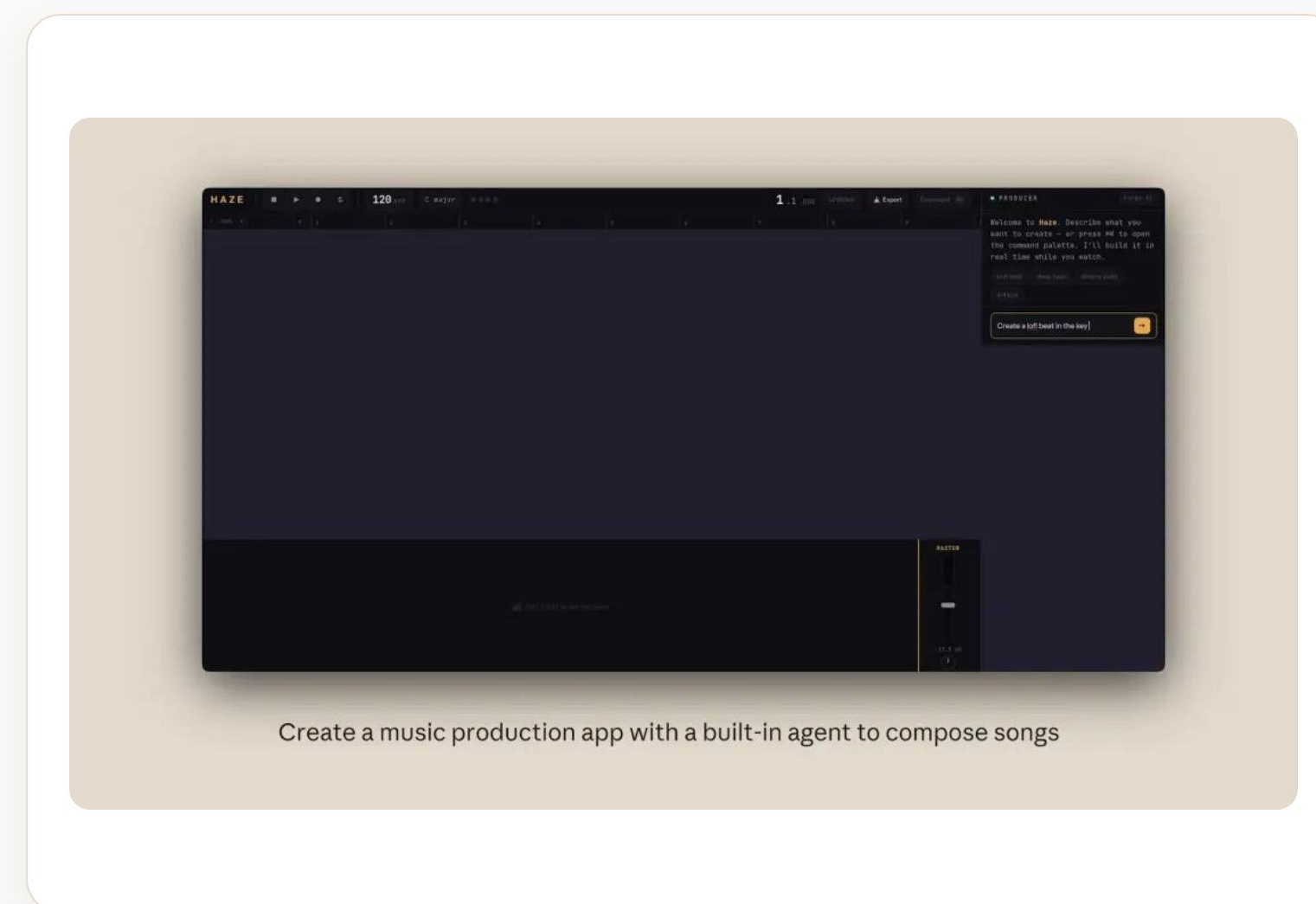
Anthropic 的 Planner-Generator-Evaluator 三角色架构。来源：Anthropic 报告

维度一 / 证据

\$9 的废物 vs \$124 的可用产品

- ◆ 单 agent 同 prompt 跑 20 分钟、\$9，核心功能不可用。
- ◆ 三角色简化系统跑 3h50m、\$124，产出可用的数字音频工作站；Generator 首轮连跑 2h07m。

花 15 倍的钱，产出从"不能用"变"能用"——
这就是 harness 在时间维度的价值。



Anthropic 构建的浏览器端 DAW "HAZE"。来源：Anthropic 报告

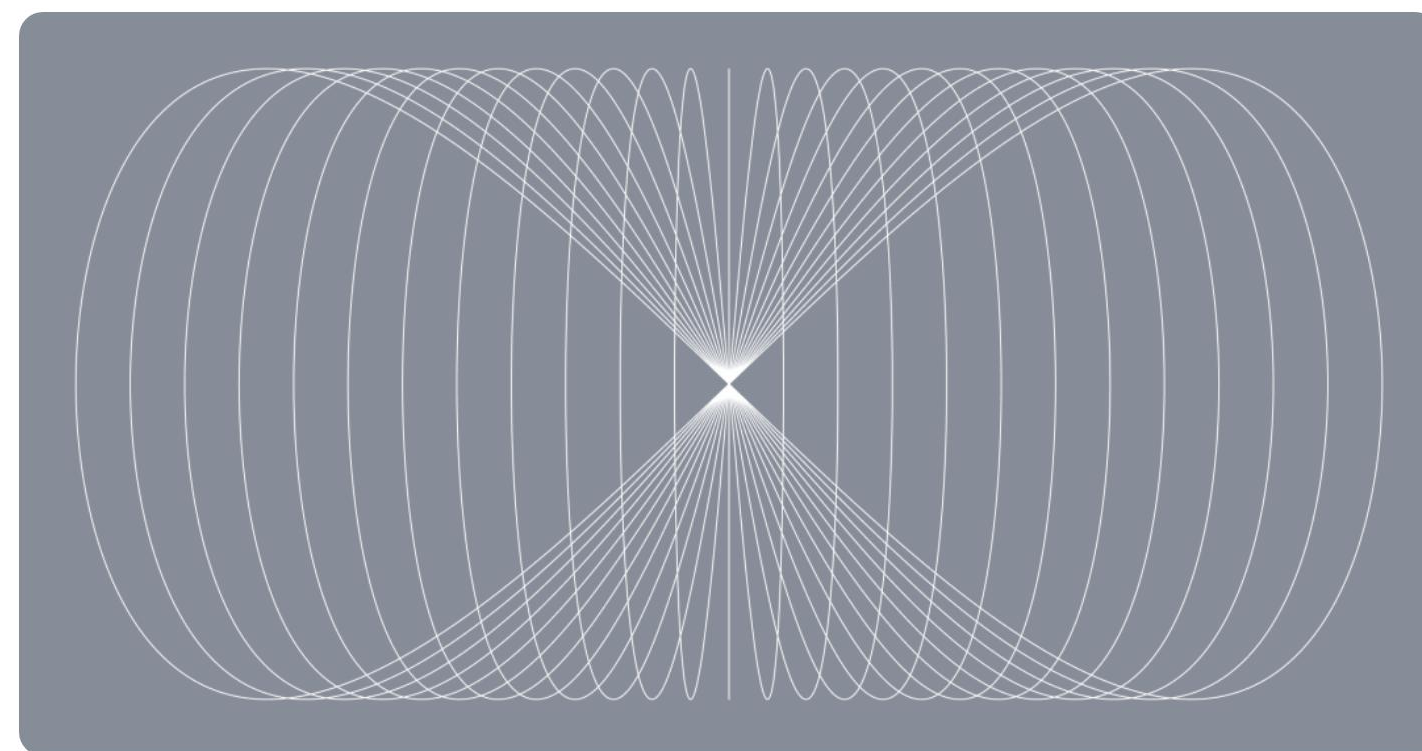
维度二 / 空间

维度二 · 空间 Scalability

◆ **问题** 能不能投 10 倍算力，换 10 倍有意义的吞吐？数百 agent 用 Rust 从零写浏览器引擎，**一周百万行**。

◆ **最值钱的是四次失败** 扁平自协调 → 结构化角色 → 连续执行器 → 递归 Planner-Worker（成功）。

◆ **成功三要素** 规划可并行、执行完全隔离、质控去中心化。
峰值 **~1000 commits/h**。



Cursor: Towards Self-Driving Codebases。来源：Cursor 报告

四次架构迭代（失败是最值钱的部分）



agent 出诡异行为时，先查是不是塞了太多互相矛盾的目标。人会摸鱼，agent 会抽风。

三维有序依赖，第四维正交



前三维问"怎么干"，第四维问"怎么沉淀成范式"

三维 · HOW IT WORKS

时间

跑更久

空间

跑更多

交互

人管得更轻

第四维 · ENGINEERING PARADIGM

工程化开发范式

标准化 · spec 驱动

多智能体协作 + review

三家解决 agent 怎么工作（更久 / 更多 / 更省心）；真正缺的，是把 agent 开发变成一套可复用、可协作、可 review 的软件工程范式——这正是 yoda 在做的。

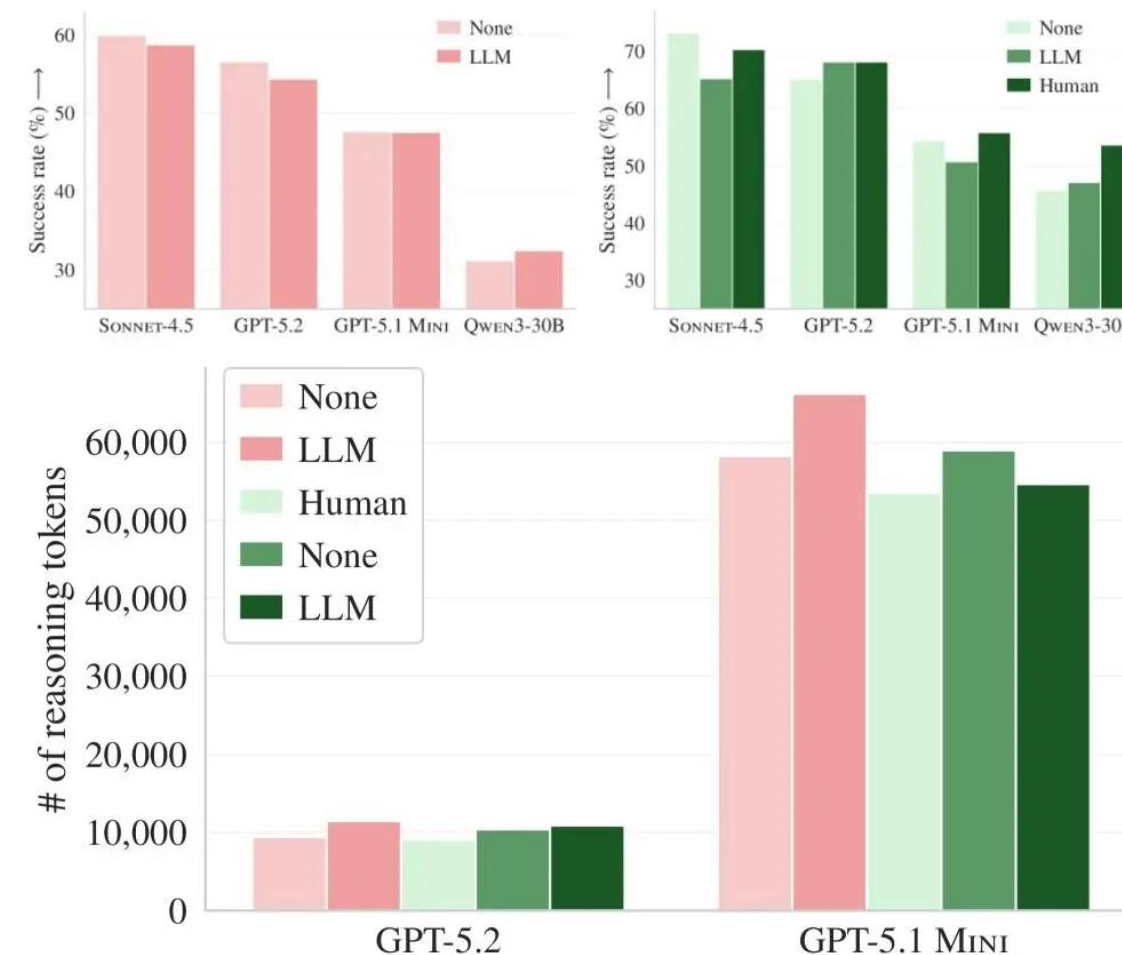
手写 60 行 >> 自动生成的长文

◆ **ETH** LLM 自动生成的 AGENTS.md 反而**降低**成功率，还多烧 14–22% token。

◆ **LangChain** Terminal Bench 2.0 上只改 harness、不换模型，排名从前 30 冲到前 5。

◆ **OpenAI** 最被低估的一条原则：机械执行（linter）胜过文档——linter 不会“忘”。

harness 的杠杆，可能比换模型还大。



手写 vs LLM 生成 AGENTS.md：成功率与 token 开销对比。来源：ETH Zurich 研究

The harness surrounds all. Binds your agents, it does.

Do. Or do not. There is no try.



Delegate, you must. Control, you need not.

YODA

YOUR ORCHESTRA OF DELEGATED AGENTS

Patience, young operator. Working, the agents are.

ENTER WORKSPACE

or press enter

Judge an agent by its size, do not.

```
[ ok ] yoda core online
[ ok ] native database attached
[ ok ] pty pool warmed
[ ok ] runtimes linked · claude code / codex / hermes
[ ok ] worktrees mounted
[ ok ] session restored — standing by
```

Powered by Lovstudio.ai · Inspired by Codex & Emdash

```
while (null === human) {
    agents.seek(meaning);
}

if (you === meaning) {
    harness.bind(you, agents);
}
```

我的实践 / yoda

yoda: 押注第四维的 agent harness 平台

github.com/lovstudio/yoda · 只展示能力地图，不逐个讲



Agent CLI 切换

cc / codex 可插拔 (emdash)



任务归档管理

session / 任务级状态模型



Context 透明化

看清 agent 拿到了什么



环境监测

skills / hooks 实时观测



多智能体

review / startup 编排



子任务管理

对接 Notion / 飞书

三个我还在纠结的设计

这些不是已有答案的功能，而是想听在座架构师怎么想的真问题。

01 Agent 要不要跟 CLI 解耦？ cc / codex 可插拔的代价与收益。

02 任务与 session 是一对一还是一对多？ archive 在 session 级还是递归到任务级——直接决定 harness 的状态模型。

03 多智能体的主 agent 能否交给用户自定义？ 含 @ 通信机制——可定制性 vs 可控性的张力。

从 Harness 到 AI 原生产品矩阵

产品矩阵

any2deck / any2pdf / app-generator / deploy-to-vercel... 同一基座长出面向场景的产品。



skills 生态

meta-skill / hr-agent / yoda group plugin + 几十个 lovstudio-* —— 第四维的工程化，开发范式沉淀成可复用资产。



yoda · Harness 平台

让 agent 能干活、可控、可观测——一切的地基。



All (26)

Free (20)

Pro (6)

All Categories

General

Design

Office Automation

Business

Content Creation

Academic

#	Skill	Category	Description	Action
01	Any → PDF 🌟 Editor's Pick	Office Automation	Typeset Markdown into a publication-quality PDF with 14 built-in themes	🔗 📄
02	Any → Slides 🌟 Editor's Pick	Office Automation	Turn any content into a styled slide deck – 16 looks, export to PPTX or PDF	🔗 📄
03	Any → Word 🌟 Editor's Pick	Office Automation	Convert Markdown into a clean, professionally styled Word document	🔗 📄
04	Book Writer 👑 PRO	Content Creation	Write a full multi-chapter book – technical, tutorial, or monograph – from an outline	🔗 📄
05	Contract Review 🌟 Editor's Pick	Business	Review a document or contract and return it with inline comments	🔗 📄
06	Contract Review Pro 🏢 Industry Pick	Business	Professional-grade contract review – four-layer methodology, structured comments with risk levels, summary, opinion, and business flowchart	🔗 📄
07	Deep Research	Content Creation	Produce citation-tracked research reports with persistent evidence, claim verification, and Markdown/HTML/PDF packaging	🔗 📄
08	Document Illustrator	Content Creation	Illustrate a long document in place – plan, generate, and insert images automatically	🔗 📄

让 Codex 按你的方式工作

🔍 搜索技能

全部

推荐



PDF

Create, edit, and review...



Playwright

Automate real browsers...



系统



Image Gen

Generate or edit images...



OpenAI Docs

Reference docs, choose...



Plugin Creator

Scaffold plugins and...



Skill Installer

Install curated skills fro...



个人



1password

Set up and use...



A Stock Analysis

A股实时行情与分时量能...



Agent Browser

Browser automation CLI...



Aminer Data Search

使用 AMiner 开放平台 A...



Architecture Designer

Use when designing ne...



Autoglm Browser Agent

智能浏览器自动化代理,可...



AI+ or +AI — where AI sits in the stack changes the output.

NOVICE • one-shot generation

gpt-image-2 / nano-banana-pro

one prompt → one bitmap

Iterate by re-prompting. Style drifts. Layout uncontrollable.

EXPERT • layered composition

LAYOUT • AI-generated HTML (rendered to image)

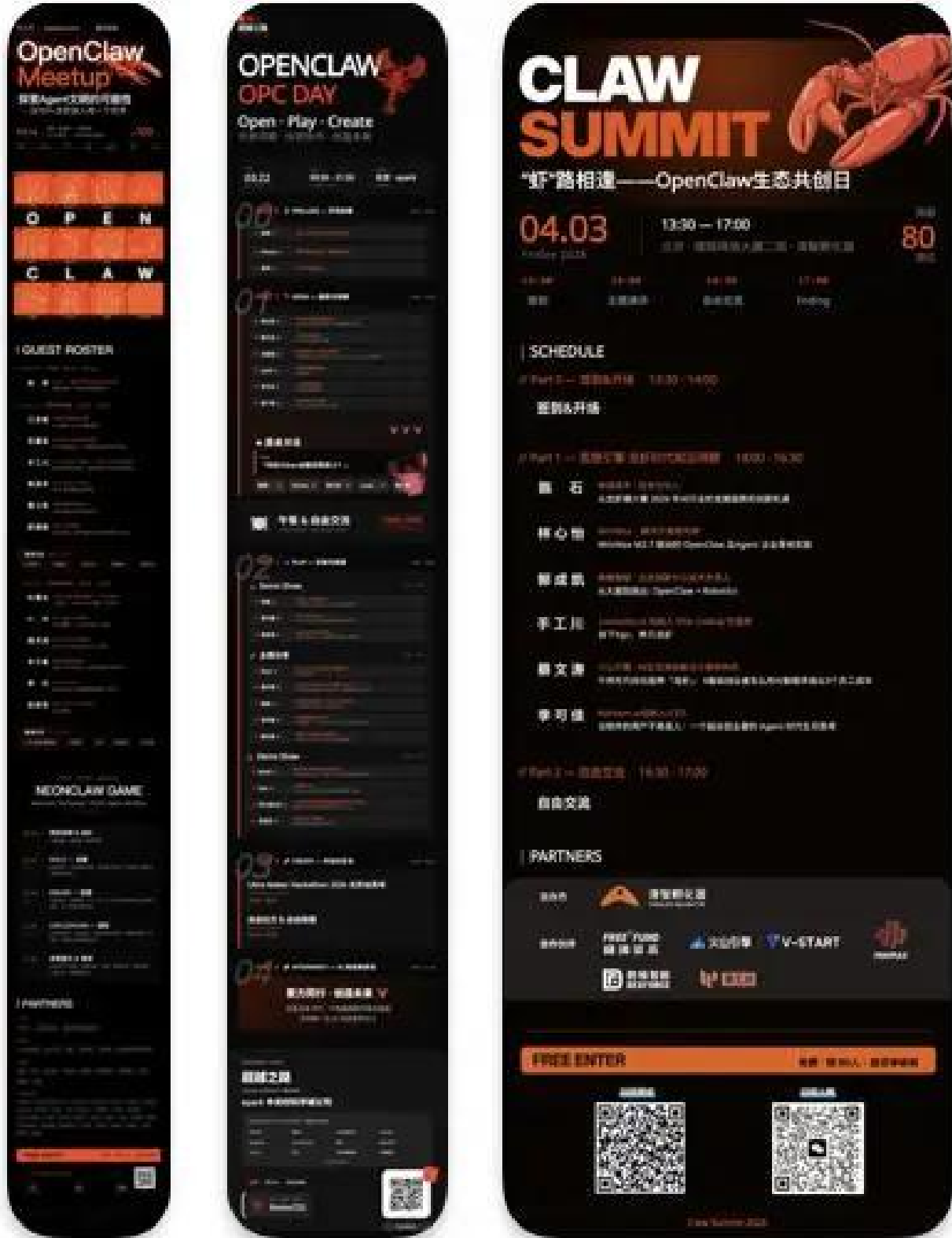
COPY • editorial line + headline polish

ILLUSTRATION • text-to-image (multi-candidate)

COMPOSITION • orchestrated mix of HTML + bitmap APIs

FIG. 5 • CONTROL × VISUAL FIDELITY • ONLY THE LAYERED STACK GIVES YOU BOTH

Mix AI-generated HTML APIs (controllable) with AI image APIs (expressive) — across layers.



forge-ep03-invite.lovestudio.ai/?inviter=Audi+China&inviter_id=Audi+China&offer=0

EP03 INVITE POSTER

手工川 AI 创造营第三期 · 邀请海报

2026-05-20 / 21 · 上海

专属二维码字段：邀请来源 / 优惠力度（可选）

INVITE · 填写邀请信息

邀请海报

易拉宝

学员证书

邀请人昵称（可选）

Audi China

邀请码（可选）

Audi China

被邀请人（可选）

默认「您」

启用专属优惠

关闭后展示为常规受邀报名，只同步邀请来源。

优惠力度（%）

10

LIVE PROMOTION

受邀报名

邀请来源已同步

当前海报展示常规受邀报名，二维码会同步邀请来源。

想匿名邀请时，只填邀请码即可生成通用邀请海报；报名二维码仍会同步邀请来源。

下载 JPEG 图像

复制图片

复制链接

系统分享

PRIVATE INVITE · 专属邀请

Audi China 诚邀您共赴手工川 AI 创造营第三期

专属邀请：报名通道已开启

手工川

520 Specialized

EP.03 · 2026.05.20-21 · SHANGHAI 线下 8 小时 · 连续两晚

手工川 · AI 创造营 第三期

三步创作法

蒸 化 发

520 不只谈爱，也谈热爱如何被 AI 放大。两个夜晚，把素材、灵感和表达能力，炼成一套可复用的AI 创作 workflow。

DATE

05.20 / 21

TIME

19-23

VENUE

上海双会场

PROCESS

填表后联系

Iteration — real client work is a loop, not a line.

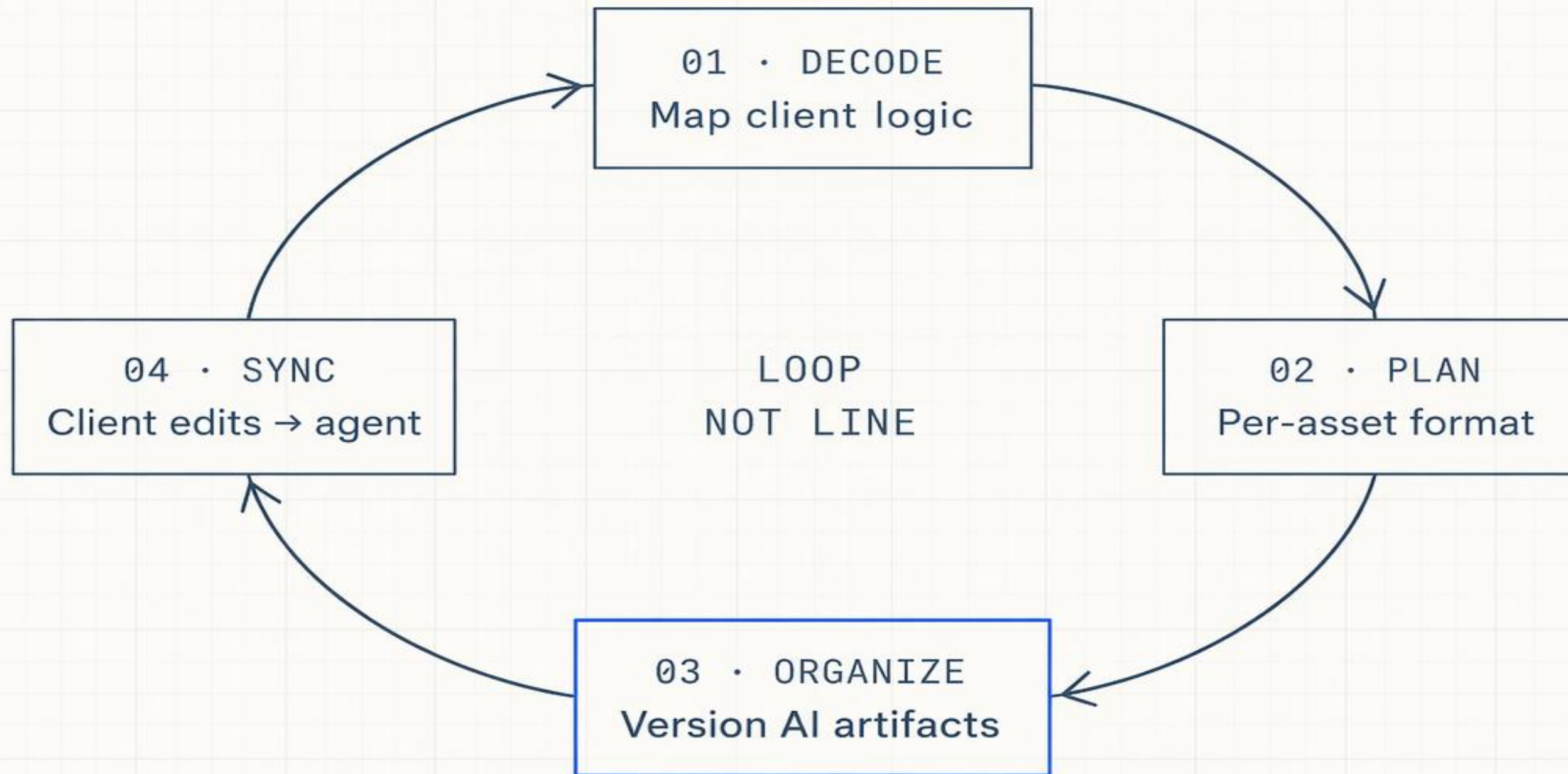


FIG. 6 · DELIVERY ITERATION LOOP

AI speeds production. Leverage lives in the loop around it.

清单 X展架 桌签 胸牌 台次卡

重定位...

@制作清单.xlsx请结构化整理该制作清单里的物料

```
<cu_window_hints>The user is pointing at: window "制作清单.xlsx" (already open; pass com.kingsoft.wpsoffice.mac to request_access). Take a screenshot to find it — do not open_application for it.</cu_window_hints>
```

我需要你把这个excel文件里粘贴的图片都以文件形式结构化整理

基于此，你生成一份用于今年能依次（或独立并行）生成所有这些物料的prompt，要求仅对用户暴露一个主视觉修改参数，尽可能好看贴合今年主题，技术上以我的直觉，也许你应该基于nano-banana-pro或者gpt-image-2生成底稿，接着再提供某种技术能实现上层文字的修改（另一个输入）与图片导出能力

请按 ./物料生成-prompt.md 生成本届"校友京华杯"的全部物料。

主视觉参数:

... 11 行省略 · 双击展开 ...

4. 生成一张索引缩略图 contact-sheet.png 便于我核稿

A

1,2, 暂时不用换

Alignment — let the sprinters run, build a market for what they ship.

ADOPTION VELOCITY · ACROSS SAME ORG

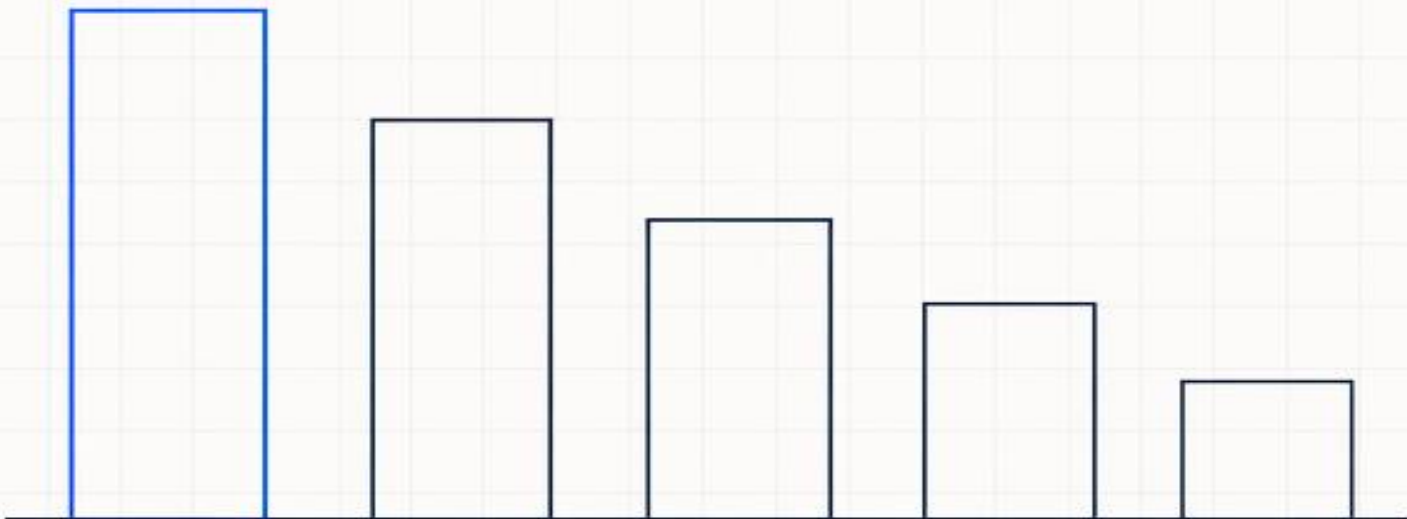


FIG. 7a · THE ORGANIZATIONAL GAP · AFTER WANG WEI / @ONEVCAT

Inside every org, a few people sprint ahead.
Most of the team is still on the starting line.
Don't slow the sprinters. Channel what they ship.

Internal Skill Marketplace

01 · PUBLISH

- Fast adopters upload skills they wrote
- Each skill = a versioned, runnable artifact
- Source visible to the whole org

02 · REWARD ON OUTCOMES

- Adopters of your skill drive your reward
- Not token-burn. Not leaderboard rank.
- Measure value at the result end, not the input end.

03 · GOVERN

- Review, sandbox, certify before broad use
- Pull bad skills fast
- Keep audit trail for compliance

Token leaderboards measure the production end. Marketplaces measure the result end. Only one is honest.

组织挑战：处理团队断层

实践推广大多是自下而上的——让高手带动团队



传统自上而下路径在这个周期里偏慢——等制度跟上，高手已经迭代三轮了

The dao is simple. The action plan fits in one paragraph.

THE DAO · MICRO-HABITS

AI-NATIVE · ONE STEP AT A TIME

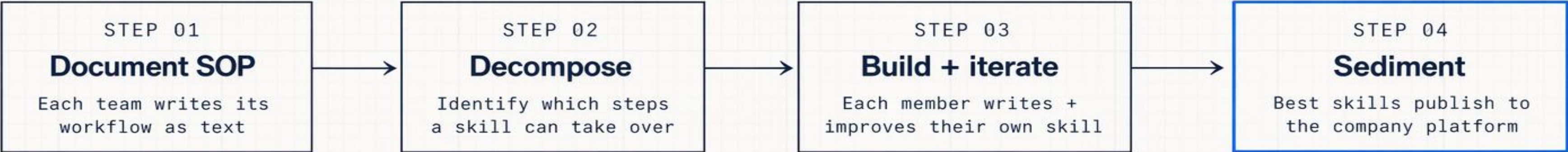


- 01 · AI is a habit, not a project. Use it every day, even for tiny things.
- 02 · Start where you already know the work. Then expand.
- 03 · Cross a small boundary each week. The walls fall in order.

REF · THE 7 WALLS OF AI ADOPTION · LOVSTUDIO.AI

THE ACTION PLAN · ORG ROLLOUT

From SOP to Skill to Platform



Like Dreame asking every employee to film videos — make skill-writing the default, not the exception.

FIG. 8 · ORG ROLLOUT · SOP -> SKILL -> PLATFORM

一位软件创业者眼里的史蒂夫

总结 由元宝提供

但除此之外，我还想额外提一个概念，叫 **Ikigai**^[7]，这是一句日语常用语，其中 Iki 就是生命的意思，而 Gai 来源于 Kai，日语中的贝壳（甲斐）的意思，日本的平安时代（794-1185）认为贝壳是贵重的物品，因此也衍生为生活的价值。Ikigai 没有对应的英文词汇，但对应到中文，大致就是“生活的意义”。

注意，我这里侧重的是“生活”，而非“人生”。

侧重这一点，是因为我的某母校微积分老师是一名虔诚的基督徒，他经常在课堂的高潮处号召我们要找到“人生的意义”，这是一个非常庞大而又厚

南川 founder@lovstudio.ai 等 9 个朋友

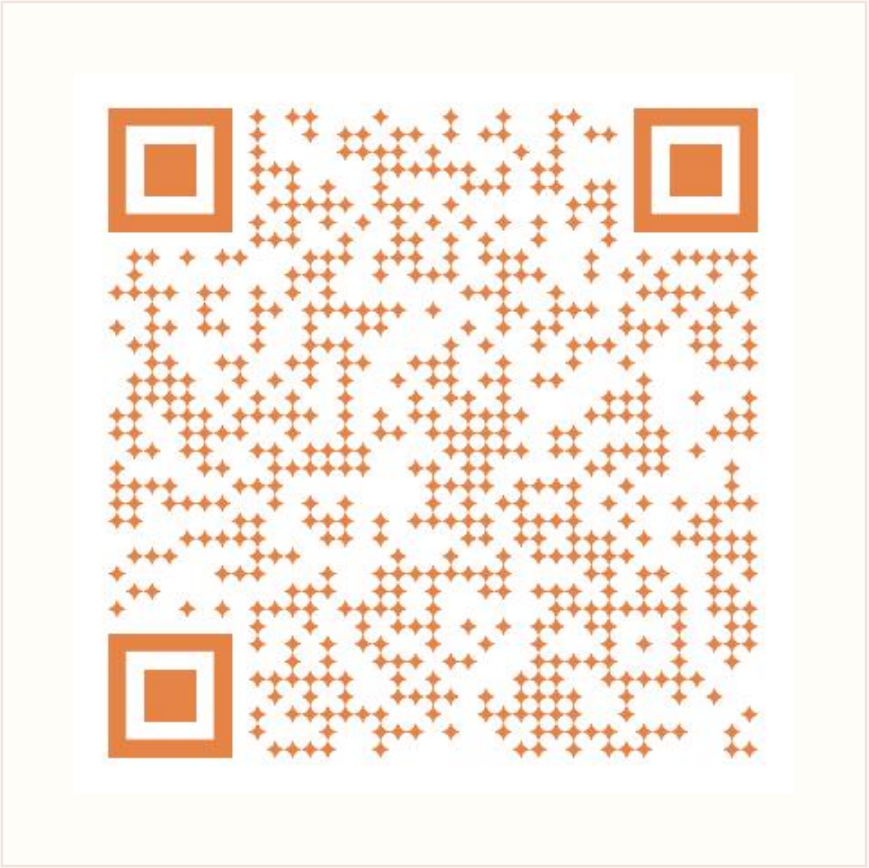
手工川

76

192

23

15



扫码交流

LovStudio.ai