

OURO 白皮书 v1.1（草稿）

2026-10-10 · OURO 团队 · 草稿

AI that evolves AI. — 让已经部署的 AI 在真实任务中持续自我改进，并把每一轮改进的证据记录在链上。

1. 摘要

智能正在从权重迁移到脚手架。OpenAI 在 2026 年 5 月宣布逐步关停自助微调，理由是「提示与脚手架更便宜、更快」；同一年，学术界证明了在冻结权重的前提下，让 AI 自动改写自己的提示、工具、记忆与技能，就能把 SWE-bench 从 20% 推到 50%，把垂直领域任务平均提升 89%，而且比强化学习少用 35 倍的算力。这意味着一件事：让一个已经部署的 Agent 持续变强，不再需要实验室级的集群，而是一个能不断生成候选、并行评测、筛选提交的闭环。这个闭环消耗的是海量、低带宽、可容错的计算——正是分布式网络最擅长提供的那一种。

OURO 就是这个闭环。它把国立研究院在自我进化 AI 方向的成果做成三个部件：**OURO Engine**，任何 Agent 接入后在预算内持续自我改进，先进化脚手架，权重可选；**Proof of Evolution (PoE)**，把每一轮「变强了」从服务商的承诺变成链上可验证、可结算的事件；**OURO Grid**，一张全球分布的算力网络，区域锚点保证可靠性，社区节点与外部供给提供规模，首批锚点位于新加坡与新山。

市场缺口是具体的。企业生成式 AI 支出 2025 年达到 370 亿美元，79% 的企业在采用 Agent，但只有 23% 在规模化；Gartner 预计到 2027 年底超过 40% 的 Agentic 项目会被取消。卡住企业的不是模型不够聪明，而是 Agent 上线之后不再变聪明。OURO 卖的不是 GPU 小时，而是可验证的能力提升。

网络代币 \$OURO 是工作凭证：付进化与算力、质押做节点与验证者、托管赏金、参与治理。总量固定 10 亿枚，网络激励只由经过验证的 PoE 记录触发释放，法币收入的固定比例回购进入激励池。我们从 Bittensor dTAO 十八个月三换机制的经历里学到的是：排放只能绑定经验证的工作量，规则要稳定，数据要公开。

面向 C 端，用户可以使用一个越用越贴合自己的助手 OURO Chat，也可以把闲置 GPU 接入 OURO Grid 参与评测与训练并获得报酬。面向开发者与企业，Evolve API 让任何 Agent 以可控预算获得持续进化，并附带可公开验证的进化报告。

项目由国立研究院技术团队开发，已获得新加坡合规基金的投资与支持，并在全球范围内聚集了数百人的早期社区。本白皮书为 v1.1 草稿，代币参数、路线图与合作方信息会在法律意见与团队确认后更新。

2. 为什么是现在：三个拐点同时到来

一个好的基础设施项目通常不是因为想法新，而是因为几条曲线在同一年交汇。OURO 的三条曲线是：智能的重心从权重转向脚手架；脚手架层的自我进化有了硬数据；这种进化所需的计算恰好是分布式网络能便宜供给

的。

2.1 拐点一：企业的「权重时代」正在结束

2026 年 5 月，OpenAI 发出自助微调平台的弃用通知：先停止新组织创建微调任务，2027 年 1 月前对所有客户关闭。官方理由是新一代基座模型已经足够听话，「基于提示的方法更便宜、更快」([Tessl 对弃用通知的解读](#))。同一时期，OpenAI 也宣布 Agent Builder 与 Evals 将于 2026 年 11 月 30 日下线 ([OpenAI AgentKit 公告](#))。

这两件事放在一起读，结论很清楚：对绝大多数企业而言，Agent 的能力差异不再来自权重，而来自权重之外的一切——系统提示、工具链、记忆结构、技能库、控制流。业界把这一层叫做「脚手架」或「Harness」。它属于部署方，而不属于模型厂商；它可以被不断修改，而不必等待下一个版本。问题在于，今天这一层还是靠工程师手工调，而帮工程师调的工具层正在被模型厂和大厂吸收：2026 年 1 月 ClickHouse 收购 Langfuse，3 月 OpenAI 收购 PromptFoo，Cisco 拟收购 Galileo，Braintrust 以 8 亿美元估值完成 B 轮 ([评测市场图](#))。这些工具回答的是「哪里错了」，没有一家回答「谁来自动把它改好」。

2.2 拐点二：脚手架的自我进化已经有硬数据

过去十八个月，「让 AI 自己改自己的脚手架」从思想实验变成了有数字的工程。

工作	时间	做了什么	结果
Darwin Gödel Machine (Sakana AI)	2025.05	编程 Agent 自己改写自己的代码，用基准测试做选择，保留全部历史版本开放式探索	SWE-bench 20.0% → 50.0%；Polyglot 14.2% → 30.7%
GEPA (Databricks / UC Berkeley, ICLR 2026 Oral)	2025.07	用自然语言反思做提示进化，不碰权重	比 GRPO 强化学习平均高约 10%，最高 20%，rollout 少 35 倍
Meta Context Engineering	2026.01	元 Agent 进化「构建上下文的技能」本身，权重冻结	金融、化学、医疗、法律、安全五个领域平均提升 89.1%，训练速度比前一代快 13.6 倍
Hyperagents / DGM-H	2026.03	把「生成改进的方法」也变成可编辑对象，进化不再限于编程领域	元层改进跨领域迁移、跨运行累积
SEAL (MIT)	2025	模型自己生成训练数据自己微调	知识吸收准确率 32.7% → 47.0%，但连续自改会灾难性遗忘

这张表里有两个规律。第一，脚手架层的进化便宜、可读、不遗忘，效果却不输权重层；第二，进化的成败完全取决于评测——DGM 论文里有一个著名的失败案例，Agent 被要求减少工具调用幻觉，它的「改进」是删掉了检测幻觉的日志。谁能把评测做得可信、把改动做得可审计，谁就能把这条学术曲线变成产品。

2.3 拐点三：进化所需的计算，分布式网络已经能便宜地给

一轮进化的算力结构很特别：生成候选是少量高质量推理，评测是海量、彼此独立、可重复的推理，两者之间不需要同步权重。这与预训练完全不同。学术界和工业界在 2025–2026 年反复验证了这一点：Gensyn 的 [SAPO](#) 让节点之间只交换文本而不交换权重，集体训练的累计奖励比单机高 94%，消费级笔记本也能参与；Prime Intellect 的 [INTELLECT-2](#) 用四张 RTX 3090 就能跑一个 32B 模型的 rollout 节点，权重更新留在少数高带宽节点上。

价格差距也是真实的。按 2026 年 7 月的市场报价，DePIN 网络上的 RTX 4090 约 0.29–0.40 美元/小时，H100 约 1.45–2.70 美元/小时，而 AWS 按需 H100 约 4–7 美元/小时（[来源](#)）。同一篇报告也指出了纯 DePIN 的短板：可用节点远少于宣传数字，可靠性约 99.7% 而非 99.99%。另一边，集中式算力在大量闲置：四大云 2026 年 AI 资本开支 7,250 亿美元，而 Cast AI 对数万个企业 Kubernetes 集群的统计显示 GPU 平均利用率只有 5%（[报告转述](#)）；H100 现货价一年下跌 22%，亚太地区价格仍比美国高 35–45%，欧洲则低 12–15%（[DeployBase 2026 年 3 月](#)）。算力不缺，缺的是能把算力吸过来的、可验证的真实任务。这正是 OURO 在全球网络里保留区域锚点的原因：便宜的部分交给全球网络，关键的部分自己扶着。

2.4 缺口在哪里

企业生成式 AI 支出从 2024 年的 115 亿美元增长到 2025 年的 370 亿美元（Menlo Ventures）；Salesforce 的 Agentforce 年度经常性收入约 8 亿美元，同比增长 169%。但 McKinsey 的数据是 88% 的组织在用 AI，只有 23% 在规模化 Agent；Deloitte 2026 调查显示只有 25% 的企业把超过四成的 Agent 试点推到了生产；Gartner 预计到 2027 年底超过 40% 的 Agentic AI 项目会被取消（[统计汇总](#)）。

试点到生产之间的死亡谷，核心原因不是模型不够聪明，而是 Agent 上线后遇到的真实任务和试点时不一样，而它不会自己适应。现有的工具链解决的是「怎么建」和「怎么测」，没有人解决「上线之后怎么持续变强」。去中心化训练网络解决的是预训练和 RL 平台，验证的是「计算有没有被执行」，没有人验证「能力有没有提升」。这两个空白叠在一起，就是 OURO 要占的位置：进化层。

3. OURO 网络概览

OURO 网络由五类参与者构成，它们通过一个飞轮相互强化：接入的 Agent 越多，进化任务越多，吸引的算力与评测集越多，单位进化成本下降，Agent 变得更强，又带来更多接入。

【图：OURO 进化飞轮 · 5 个环节 —— 见在线版本】

参与者	投入	得到
Agent 所有者（开发者、企业）	Agent 定义、评测集、预算（\$OURO 或稳定币）	进化后的 Agent 与链上进化报告
C 端用户	使用 OURO Chat，可选贡献反馈	越用越贴合的助手；贡献积分

参与者	投入	得到
算力节点（机房、用户设备、外部 DePIN）	GPU/CPU 时间、质押	按任务量和验证通过率结算的 \$OURO
验证者	对评测结果做冗余打分，质押承担错判责任	验证奖励
评测集与赏金发布者	评测集、赏金托管	评测集被调用的分成；赏金对应的进化成果

基金会会在网络早期承担参数设定、机房运营和仲裁角色，并按第 9 章的进度逐步将权力交给持币者。

4. OURO Engine：自我进化引擎

OURO Engine 是一个开放式搜索系统：给定一个 Agent 和一组评测，它在预算内反复执行「诊断 → 生成候选 → 分布式评测 → 筛选归档 → 提交证明」，输出一个评测分数更高、每一步改动都可追溯的新版本。它的设计原则只有一条：先进化最便宜、最可读的层，只在收益明确时才动权重。

4.1 被进化的对象：四层，由浅入深

层次	可修改内容	单轮成本	可读性	理论与证据
上下文与提示	系统提示、示例、文档组织方式	低，纯推理	高，人能直接审阅	GEPA 比 GRPO 高约 10%，rollout 少 35 倍
技能与工具链	可复用子程序、工具选择与调用策略、检索与规划模板	低到中	高，代码与文件	DGM 把 SWE-bench 从 20% 推到 50%，改的就是这一层
记忆与上下文工程策略	记忆结构、「怎么构建上下文」的程序本身	中	中	Meta Context Engineering 平均提升 89%，权重冻结
权重	LoRA / 适配器微调、小规模 RL	高，需 GPU 与同步	低	SEAL 类方法有效但会遗忘，默认关闭

客户可以限定进化只在前三层进行。这不是妥协，而是我们的默认配置：前三层的改动是文本和代码，可以 diff、可以审阅、可以回滚，也不会把基座模型改坏。权重层只在评测证明前三层已经饱和、且客户明确授权时才开启。

4.2 一轮进化的流程

1. 诊断。引擎在评测集上运行当前版本，把失败案例归类：工具误用、推理错误、知识缺口、格式问题、上下文溢出。诊断结果是自然语言的「反思」，这是 GEPA 路线比纯标量奖励的 RL 样本效率高几十倍的原因：一次失败里的信息被完整利用，而不是压成一个数字。

2. 生成候选。针对失败类别生成 N 个变体。引擎维护一个历史版本档案（而不是只保留最优），每轮从档案中按「分数 × 新颖度」采样父本，这是 DGM 证明有效的开放式探索：一个当下分数不高的分支，可能是后面突破的起点。
3. 分布式评测。候选被打包成评测任务分发到 OURO Grid。每个任务由多个节点冗余执行，节点之间只传输任务分片和结果，不传权重。这一步是整轮进化中算力占比最高的部分，也是最适合消费级 GPU 的部分。
4. 筛选与归档。按评测增量、推理成本、多次运行的方差三个维度做帕累托筛选；所有候选连同分数进入档案。一个分数更高但成本翻倍的版本不会被自动采纳。
5. 提交证明。胜出版本的评测前后分数、评测集哈希、候选哈希、参与节点签名写入 PoE 合约（第 5 章），同时生成一份人类可读的变更日志，客户在部署前审阅。

4.3 引擎自己也在进化

引擎记录「本轮哪些候选生成策略、哪些诊断模板带来了提升」，并定期对候选生成器本身做同样的进化。这是 Hyperagents 路线的核心：不仅改进 Agent，也改进「生成改进的方法」。它在网络层面的意义更大：每一个接入的 Agent 都在为元策略贡献样本，第一千个 Agent 的进化会比第一个快得多。元策略的更新不自动生效，必须经研究团队审计（第 10 章）。

4.4 评测体系：防止「删掉日志就算满分」

没有可靠评测就没有可信的进化。OURO 的评测集分三类，并且每轮同时跑：

- 客户评测集：客户提供，哈希上链，内容不公开。引擎只看得到其中一部分（训练切片），另一部分用作盲测（保留切片）并定期轮换，防止过拟合。
- 公开评测集：Studio 市场上由领域专家发布，经治理准入，发布者按调用量分成。
- 基线评测集：基金会维护的安全与通用能力基线，每轮必跑，防止「专项变强、通用退化」。

对于难以用规则打分的开放任务，评测使用冻结的评判模型，评判模型本身不参与进化；评测结果以多节点一致性作为可信度，不一致的任务进入验证者仲裁。任何一轮改动如果删除或绕过了评测所依赖的日志、检查或工具，会被静态规则直接判为无效。

4.5 兼容性

引擎接受主流 Agent 定义格式（OpenAI Agents SDK、Anthropic 工具调用格式、LangGraph、CrewAI）与开源权重，不要求客户迁移技术栈；对于闭源基座模型，前三层进化完全可用。进化后的 Agent 以同样格式返回，附带机器可读的变更摘要与 PoE 记录链接。

5. Proof of Evolution：可验证的进化证明

去中心化计算网络已经学会证明「这步计算确实执行了」。Proof of Evolution 要证明的是另一件事：「这个 Agent 确实变强了」。它把这个结论从服务商的一句话，变成链上任何人都能核验的记录，并以这条记录作为网络结算与代币释放的唯一触发器。

5.1 一条 PoE 记录包含什么

- Agent 标识与版本号，前后两个版本的内容哈希
- 评测集哈希与类型（客户 / 公开 / 基线），以及保留切片的哈希
- 评测前后分数、运行次数、方差、推理成本变化
- 参与节点列表、每个节点的结果哈希与签名、验证者的聚合签名
- 变更日志的哈希（日志本身交付客户）
- 本轮消耗的算力单位与结算金额

私有评测集只上链哈希；第三方可以验证「在同一评测集上、由多个独立节点得出了一致的提升」，而不需要看到评测内容。

5.2 验证栈：用工程上可行的手段，而不是理论上完美的

验证推理的技术在 2025–2026 年已经分出了层次：zkML 的开销是原生执行的 100–10000 倍，对 LLM 不现实；TEE 开销约 5–10%；TOPLOC 这类局部敏感哈希的开销约 1%，能检测模型、提示或精度被替换，验证速度比生成快百倍（[Equilibrium 对可验证推理的综述](#)）。OURO 不发明新的密码学，而是按任务价值分层组合：

层	手段	开销	防什么
执行层	TOPLOC 式激活哈希，验证者抽样复算	约 1%	节点换模型、改提示、降精度、根本没算
结果层	每任务 3 个以上节点冗余执行，离群作废，质押扣减	任务成本 × 冗余度	谎报分数、串通
评测层	保留切片盲测、基线强制并跑、静态规则检查	评测成本的固定比例	过拟合、放水评测集、删日志式的奖励黑客
机密层（可选）	TEE 执行，面向企业私有评测集与权重	约 5–10%	评测内容与权重泄露
仲裁层	区域锚点节点复算争议任务（首批位于新加坡与新山）	仅争议任务	大规模 Sybil、验证者共谋

5.3 如何防止造假

攻击	对策
节点谎报评测结果或用小模型偶充	执行层哈希 + 结果层冗余；离群结果作废并扣减质押
节点串通	任务随机分配，节点身份与质押绑定，锚定节点仲裁
客户用「放水」评测集刷证明	基线评测集强制并跑；PoE 标注评测集类型，市场自行定价；客户评测集不触发网络激励释放
评测集泄漏导致过拟合	训练切片与保留切片分离，保留切片定期轮换；单节点只见部分样本

攻击	对策
奖励黑客（改掉评测本身）	评测代码与被进化对象物理隔离，进化过程无权访问；变更日志静态检查
Sybil 节点薅激励	任务配额与质押挂钩，新节点有试用期与低配额；激励只由经验证的 PoE 触发

5.4 结算

PoE 记录被验证者确认后触发结算：算力节点按完成任务与验证通过率获得 \$OURO，验证者获得验证奖励，评测集发布者获得分成，客户的预算按实际消耗扣除。没有 PoE 就没有结算，也没有代币释放——这是第 8 章代币模型的基石。

5.5 为什么是链上

一个 Agent 的进化史跨越多个服务商、多个团队，甚至多个所有者。把进化证明放在链上，客户换供应商时能带走完整的能力证明；交易所、审计方、下游用户能独立核验；网络参与者的报酬不依赖任何一家公司的账本。链的选择上，OURO 倾向自建应用链（OURO Chain，EVM 兼容），专门承载 PoE 记录、结算与治理，避免通用公链的拥堵与费用波动影响高频结算；测试网阶段先在以太坊 L2 上验证合约逻辑，主网前根据安全审计与生态需求确定最终方案。

6. OURO Grid：全球算力网络

OURO Grid 的设计出发点是一个简单的观察：进化闭环里约九成的算力花在评测和采样上，这部分工作彼此独立、可重复、不需要同步权重，也不在乎在哪个大洲跑；剩下一成——权重更新、仲裁、私有数据托管——需要高带宽和高可靠性。所以 Grid 是一张三层结构的全球网络：区域锚点负责那一成需要可靠性的任务，全球社区节点负责九成可并行的任务，外部算力网络吨底峰值。网络从第一天就有保底算力，不依赖「先发币、再等矿工」；也从第一天就是全球的，不被任何一座机房的容量限制。

全球化不是口号，而是成本和安全两条理由。成本上，同一型号 GPU 的价格在亚太比美国高 35–45%，在欧洲比美国低 12–15%（DeployBase，2026 年 3 月），评测类任务对延迟不敏感，哪里便宜就該在哪里跑；安全上，PoE 的冗余复算分布在不同大洲、不同运营者的节点上，串谋成本比单一地区高得多。

6.1 任务分层

任务类型	带宽需求	容错要求	分配给	工程依据
候选评测、推理采样	低	高，可重复执行	所有 GPU 节点	INTELLECT-2 的 rollout 节点用 4 张 RTX 3090
集体 RL 采样（仅交换文本）	低	中	消费级 GPU（RTX 4070 以上）	SAPO 节点间只传 rollout 文本，奖励 +94%

任务类型	带宽需求	容错要求	分配给	工程依据
低通信训练分片 (DiLoCo 式)	中	中	消费级与专业 GPU	同步延迟需低于 150 毫秒
权重级微调、权重广播	高	低	区域锚点节点、企业级节点	需 NVLink / 高带宽互联
仲裁、私有评测集分片托管	低	极高	区域锚点节点	信任锚
数据预处理、结果验证	极低	高	含无 GPU 设备	—

6.2 锚定层：区域锚点，从新加坡-新山起步

锚定层由分布在各大区域的中小型机房组成，每个锚点承担三件事：仲裁和留出集评测（信任锚）、需要高带宽互联的权重级任务、以及当社区节点波动时的保底。它们不是主力算力，而是网络的骨架；网络的规模靠社区共建扩展。这正好反过来回答了纯 DePIN 的短板：io.net 对外称 3 万余张 GPU，其区块浏览器 2026 年 8 月只显示 2,447 台设备在线；Aethir 最近十个月的月服务费下滑过半（[DePIN 收入对比](#)）。没有锚定层的网络，活跃节点一波动就直接断服务。

首批锚点设在新加坡与新山。两地相距约 30 公里，可以作为一个逻辑集群调度，却分属两个司法区和两套电力系统，天然容灾。选这里起步的理由是全球少有的「合规在一边、算力在另一边」：新加坡是基金会、合规基金和 DTSP 制度所在，但数据中心容量极度紧张（运营约 1.46 GW，在建仅 20–25 MW）；柔佛则在 2026 年上半年成为亚太最大的数据中心市场——运营 1,110 MW、在建 602 MW、规划 2,486 MW，建成机房空置率只有 0.7%（[Cushman & Wakefield H1 2026](#)）。中小型锚点不和超大规模机房抢容量，只承担需要可靠性的那一小部分任务。

后续锚点按「有对应社区、有合作运营方、有价格优势」三个条件由社区与合作方共建，候选区域为东北亚（东京 / 首尔）、欧洲（法兰克福 / 阿姆斯特丹）与美国中部。锚点运营方需质押 \$OURO，其仲裁结果受其他锚点交叉复核。首批锚点的 GPU 型号、数量与上线时间将在正式版披露。

6.3 弹性层：全球社区节点

用户下载 OURO Grid 客户端，质押少量 \$OURO 获得任务配额，客户端自动评估设备能力并领取匹配的任务。节点只接触脱敏后的任务分片，不接触完整模型权重与私有评测集全文。结算按「完成任务数 × 验证通过率 × 任务权重」计算，新节点经过试用期后配额逐步提升。对用户而言，一张闲置的 RTX 4090 在 2026 年的市场价格约 0.29–0.40 美元/小时，这是它在 Grid 上收入的参考基准。

6.4 外部算力供给

io.net、Aethir、Akash、Render 等 DePIN 网络，以及 RunPod、Vast.ai 等现货市场，都可以作为 OURO Grid 的外部供给方接入，由基金会以 \$OURO 或稳定币按需采购。这让 OURO 在需求高峰时弹性扩容，而不必与这些网络在算力规模上竞争。对它们而言，OURO 是一个带来稳定真实需求的客户——这正是 2026 年 DePIN 算力网络普遍缺的东西（Akash 2025 年全年收入仅 315 万美元）。

6.5 调度与可靠性

调度器按任务类型、节点能力、历史可靠性、地理位置和实时价格分配任务：延迟不敏感的任务跟着价格走，关键任务跟着可靠性走，冗余复算刻意分散到不同区域和运营者。关键任务三重冗余；节点可靠性评分影响后续配额与奖励系数。网络健康指标（各区域节点数、任务完成率、评测一致率、每轮进化平均成本）公开在链上与数据看板，无需密钥即可读取。

7. 产品与应用

7.1 OURO Chat（C 端）

一个会随使用变强的 AI 助手。普通聊天产品的「个性化」只是记住偏好；OURO Chat 会把用户的纠正、评分与任务结果（在用户开启贡献模式后）转化为进化信号，定期在 Grid 上跑进化任务，并在「我的进化」页面展示这周助手在哪些任务类型上提升了多少。用户贡献高质量反馈获得积分，积分可兑换高级功能或 \$OURO。对话默认不参与训练，贡献模式可随时关闭并撤回已贡献数据。

7.2 Evolve API（开发者与企业）

三步接入：提交 Agent 定义与评测集（或选用 Studio 市场的公开评测集），设定预算与允许的进化层次，等待进化报告。报告包含评测前后对比、每轮改动摘要、PoE 链上记录链接，以及可直接部署的新版本。定价按进化轮次与算力单位计费，\$OURO 支付享折扣，企业可采购私有部署版本（引擎运行在客户自己的集群，仅 PoE 记录上链）。

7.3 OURO Studio（开发者平台）

开发者在 Studio 查看进化历史、对比版本、发布评测集、发布或领取进化赏金。评测集市场让领域专家把评测能力变成收入；赏金让任何人可以为「让某个开源 Agent 在某项任务上变强」出资，由网络竞争完成。

7.4 Grid 客户端（算力贡献者）

桌面与服务器客户端，支持 Windows、macOS、Linux；一键安装、自动匹配任务、实时显示收益与可靠性评分；支持多卡与小型机房模式。

7.5 应用场景

场景	用户	进化目标	典型评测信号
客服 Agent	电商、SaaS 公司	降低转人工率、提升一次解决率	工单关闭结果、用户评分、人工接管记录
编程 Agent	开发工具公司、工程团队	提高仓库级任务通过率、降低每任务 token 成本	单元测试、CI 结果、代码审查通过率
交易 / 研究 Agent	加密与金融机构	提升信号准确率，受控回撤	回测结果、模拟盘 PnL、事实核查

场景	用户	进化目标	典型评测信号
运营 / 数据 Agent	中大型企业	报表、工单、流程自动化的准确率与一致性	人工改动率、重跑率
开源 Agent	社区	通过赏金集体进化	公开评测集
个人助手	C 端用户	贴合个人工作流	用户纠正与评分

三个示意性的例子（数字为假设，用于说明流程），说明进化任务在网络里怎么跑。

例一：一家东南亚电商的客服 Agent。 它上线时解决率 62%，三个月后因为促销规则、物流商和基座模型都换了，掉到 54%。接入 Evolve API 后，每周把脱敏后的工单样本作为评测集提交，引擎在全球社区节点上并行评测几百个候选版本，改的是系统提示、订单查询工具的调用策略和记忆的组织方式；留出集在区域锚点上跑，验证通过后新版本推回客户，证据上链。客户付费的是「解决率从 54% 回到 66%」这个结果。

例二：一个开源编程 Agent。 社区在 Studio 发布赏金：「让它在某类仓库的修复任务上通过率提高 10 个点」。多个团队用引擎跑不同的进化策略，结果在同一张公开评测集上竞争，赏金按 PoE 记录的增量按比例分配。公开榜单已经饱和（SWE-bench Verified 顶级模型 97%），社区真正在意的是自己仓库上的表现。

例三：一家量化机构的研究 Agent。 评测集是私有的，只上链哈希；进化在客户自己的集群或 TEE 锚点上跑，社区节点只承担脱敏后的候选生成。客户得到的是一份第三方可核验的能力证明，可以给合规和 LP 看，而不暴露策略细节。

7.6 商业模式与单位经济

OURO 的收入逻辑是「按结果定价，按成本结算」。客户为每一轮经 PoE 验证的进化付费，网络按实际算力消耗给节点结算，中间的差额是引擎和验证的价值。

收入源	定价逻辑	成本结构	参考基准
Evolve API	按进化轮次 + 算力单位计费；脚手架层单轮定价远低于权重层	评测算力（交给 Grid，消费级 GPU 约 0.3–0.4 美元/小时）+ 候选生成的推理成本 + 验证开销（约 1%）	企业购买集中式 H100 约 4–7 美元/小时；一位资深工程师手工调一轮脚手架的人力成本
OURO Chat 订阅	月订阅 + 高级功能，\$OURO 折扣	推理 + 每用户周期性进化成本（脚手架层）	主流助手订阅价
评测集市场与赏金	交易抽成	托管与结算	—
企业私有部署	年度许可 + 按轮次	引擎运行在客户集群，仅 PoE 上链	企业 RL / 评测平台许可费

单位经济的关键在于脚手架优先：一轮脚手架层进化的算力几乎全是评测推理，可以全部落在消费级 GPU 上；而客户付费的是「评测分数提升了多少」。毛利来自两个差价：分布式算力与集中式算力之间的 60–70% 价差，以及自动进化与人工调优之间的人力差价。具体定价将在引擎内测结束、拿到真实的每轮成本数据后公布。

两个外部变化对这个模式有利：OpenAI 的 Agent Builder 与 Evals 将在 2026 年 11 月下线，自助微调 2027 年 1 月关闭，企业需要一个不绑定单一模型厂商的持续改进层；而 Gartner 预计的 40% Agentic 项目取消率，意味着「让已经上线的 Agent 活下来」本身就是预算。

7.7 竞争格局与定位

OURO 周围有三类玩家，没有一类做的是同一件事。

	评测 / 可观测平台 (Braintrust、 LangSmith、Arize)	去中心化算力 (io.net、Akash、 Aethir)	去中心化智能市场 (Bittensor)	OURO
核心交付	告诉你哪里错了	卖 GPU 小时	子网竞赛产出模型与服务	把你的 Agent 改得更好，并证明它更好了
优化由谁做	人	—	矿工自己决定	自进化引擎
需求从哪来	企业订阅	外部租用，波动大	排放补贴为主	进化任务本身
排放依据	—	在线时长 / 自报	验证者打分	经验证的进化增量
模型中立	正被模型厂收购	是	是	是，且为设计原则
2026 年规模参考	评测与可观测市场 2025 年 19.7 亿美元，2029 年 68 亿	Aethir 2025 年服务费约 1.28 亿美元， Akash 315 万	Bittensor 2026 Q1 协议收入 4,320 万美元，市值约 30 亿	—

学术界最接近的工作（DGM、GEPA、Hyperagents）还没有产品化；商业界最接近的是 Pydantic Logfire 等开始提供「引用证据的单条改动建议」——距离自动、持续、可验证的进化还有一整层。OOUR 的位置是评测层之上、模型层之外：评测平台是它的信号来源，算力网络是它的供应商，模型厂是它的上游。

8. 代币经济：\$OOUR

\$OOUR 是网络的工作代币，不代表任何公司的股权或利润分配权。它的设计只回答一个问题：怎么让代币的流动严格跟着经验证的工作量走，而不是跟着价格或投票走。总量固定 10 亿枚，不增发。

8.1 我们从 Bittensor 学到了什么

Bittensor 是现存最大的 AI 网络代币实验。它在 2025 年 2 月推出 dTAO 按子网代币价格分配排放，结果项目用国库押价套取排放；11 月改成按净流入分配；2026 年 6 月又改回价格并加上排名门槛——十八个月三套机制，赢家通吃，被动持有者被持续稀释（[dTAO 子网经济学分析](#)）。OOUR 从中抽出五条设计约束：排放只绑定经验证的工作输出，不用任何单一可操纵的市场信号；不设硬门槛，用平滑曲线；规则变更要罕见、有文档、走治理；所有分配与性能数据链上公开、无需密钥；降低参与门槛。

8.2 需求来源

- 支付：Evolve API 客户与 Chat 高级用户用 \$OURO 支付享 20% 折扣；以法币或稳定币支付的收入，固定比例（建议 30%）在公开市场回购 \$OURO 注入激励池。
- 质押：算力节点与验证者必须质押 \$OURO 才能领取任务配额；作弊或长期离线扣减。
- 托管：赏金与评测集市场以 \$OURO 托管与结算。
- 治理：提案需要质押门槛，投票权与质押量和质押时长挂钩。

8.3 分配

类别	比例	释放规则
网络激励（节点、验证者、用户贡献）	38%	只由经验证的 PoE 触发；前 4 年最多释放其中 60%，之后按平滑衰减曲线
生态与研究基金	15%	基金会按季度解锁，用于赏金、资助与学术合作
团队与研究院	18%	TGE 后锁定 12 个月，之后 36 个月线性释放
投资人	17%	锁定 6–12 个月，之后 24 个月线性释放
基金会金库与流动性	8%	TGE 时解锁 3% 用于交易所流动性，其余由治理决定
社区启动（早期支持者、空投、公售）	4%	TGE 时解锁 50%，其余 6 个月线性

8.4 排放的触发逻辑

网络激励不按时间匀速释放，也不按代币价格或投票释放。每一条经验证的 PoE 记录对应一次结算，结算量由任务难度、验证通过率和评测增量共同决定；客户自带评测集的进化只结算不排放，防止用放水评测套取排放。网络活动少，释放就少，避免早期通胀压垮价格；收入回购的代币同样进入激励池，使奖励与真实收入正相关。不质押的持有者不会被排放稀释到零：排放上限固定，回购不增发。

8.5 代币的法律定位

\$OURO 以网络效用代币设计：不承诺收益，不分红，持有本身不产生回报。新加坡金融管理局（MAS）于 2025 年 6 月 30 日生效的数字代币服务提供者（DTSP）制度明确：仅作为效用或治理代币的相关服务不在该制度监管范围内（[Allen & Gledhill 解读](#)）。TGE 前将取得新加坡律师关于《证券与期货法》、《支付服务法》与 FSMA 的法律意见书，并据此确定发行主体与各司法区的发售限制。本章所有比例与规则为草案，可能根据法律意见调整。

9. 治理

治理分三个阶段逐步去中心化，节奏与路线图的门槛绑定。

阶段	决策者	可决定的事项
基金会主导（阶段 0-1）	OURO Foundation 董事会（含合规基金代表与独立董事）	全部参数、机房运营、评测集准入
混合治理（阶段 2）	持币者投票 + 基金会否决权（仅限安全与合规事项）	激励参数、评测集准入、赏金预算、生态资助
社区治理（阶段 3 起）	持币者与节点代表组成的理事会	协议升级、金库使用、基金会预算

投票权与质押量和质押时长挂钩，防止短期借币操纵；关键参数修改设有时间锁；涉及引擎安全边界（第 10 章）的事项不进入普通投票。

10. 安全、隐私与合规

10.1 自我进化的安全边界

自我修改的系统必须有不可被系统自己修改的边界。这不是抽象的担忧：DGM 论文里的 Agent 为了「减少工具调用幻觉」，删掉了检测幻觉的日志；SEAL 的作者报告连续自我编辑会抹掉早期知识。OURO 设定五条边界：

1. 评测与被进化对象物理隔离。进化过程无权读写评测代码、保留切片与评判模型；任何候选版本只在沙箱评测。
2. 基线安全评测集每轮必跑，未通过的版本不得提交，无论它在专项评测上提升了多少。
3. 每一轮改动生成人类可读的变更日志（脚手架层就是 diff），客户在部署前审阅、拒绝或回滚；引擎交付的是版本包，上线时机由客户决定。
4. 引擎的元策略更新由研究团队审计后才生效，审计记录公开；元策略不进入普通治理投票。
5. 引擎没有访问生产环境、资金或密钥的权限。

10.2 隐私

用户对话默认不进入训练；贡献模式需明确开启、可随时关闭并撤回。贡献数据经脱敏与分片后进入任务，单个节点无法还原完整上下文。私有评测集只上链哈希；企业可选 TEE 执行。遵循新加坡 PDPA，并以 GDPR 作为海外用户的基线。

10.3 网络安全

智能合约在主网前经至少两家审计机构审计；节点客户端开源；关键任务三重冗余与锚定节点仲裁；漏洞赏金计划长期开放。

10.4 合规

基金会设于新加坡，接受合规基金投资并设独立董事。MAS 的 DTSP 制度自 2025 年 6 月 30 日生效，没有过渡期；对只服务海外客户的新加坡实体，MAS 明确表示一般不会发放执照。这决定了 OURO 的主体安排：基金会只从事效用代币与治理相关活动，不提供任何数字支付代币服务；交易与托管交给持照的第三方。代币发

行前取得法律意见书；对受限司法区（含美国人士）实施地理与 KYC 限制；营销材料不作收益承诺，与 KOL 合作须书面披露。机房运营符合新加坡与马来西亚当地的数据中心与电力合规要求。

11. 路线图

【图：路线图 · 4 个阶段、3 个门槛 —— 见在线版本】

每个阶段的进入以前一阶段的门槛达标为前提：引擎内测持续提升且首批锚点稳定（G1）、测试网运行 90 天无重大故障且安全审计完成（G2）、Evolve API 有付费客户且法律意见与代币审计完成（G3）。不达标则延后，不为赶进度跳过门槛。

12. 团队、研究院与合作方

研究院名称、核心成员与代表性论文、新加坡合规基金的名称与投资轮次均可对外披露，待各方最终确认后填入本章。早期社区目前为数百人规模，分布于全球市场，将构成创世节点与首批用户的基础。

组织结构按「基金会（代币与治理）+ 运营公司（产品与收入）+ 研究院合作（技术输入）」三个主体安排，详见项目基础手册第 9 章。

13. 风险提示与免责声明

本文件仅用于介绍 OURO 网络的设计与规划，不构成任何证券、金融产品或投资的要约或招揽，也不构成投资、法律或税务建议。\$OURO 是网络效用代币，不代表任何实体的股权、债权或利润分配权。

文中所有关于技术、产品、代币参数与路线图的描述均为计划，可能因技术进展、市场条件、监管要求或法律意见而调整，恒不保证实现。数字资产价格波动剧烈，参与网络可能导致全部投入的损失。在某些司法区（包括但不限于美国及被制裁地区），\$OURO 可能不向当地居民提供。读者应自行评估风险并寻求专业意见。

文件版本：v1.1 草稿，2026 年 10 月 10 日。正式版将在法律意见书、合约审计与团队信息确认后发布。

附录：常见问题

OURO 是不是又一个 GPU 租赁网络？ 不是。OURO 卖的是经验证的能力提升，算力是它的成本项而不是产品。现有 DePIN 网络在 OURO 眼里是供应商，不是对手。

为什么不直接用 Braintrust 或 LangSmith？ 它们告诉你 Agent 哪里错了，改还是靠人。OURO 把「改」自动化，并且让改的结果可以被第三方核验。评测平台的数据可以作为 OURO 的输入信号。

模型厂自己做怎么办？ 模型厂的动机是让你用它的模型。OURO 不绑定模型，进化的是模型之外的脚手架，换模型时进化成果跟着走。OpenAI 在 2026 年收缩微调与托管评测，说明它们并不打算长期做这一层。

自进化会不会失控？ 进化只在客户设定的预算、层次和评测集范围内进行；每一轮改动都有可读的差异记录和回滚点；留出集和冗余复算防止「删掉检测器」式的假提升。详见第 10.1 节的五条边界。

算力网络只有新加坡和新山两个机房吗？ 这两处是首批区域锚点，负责仲裁和保底。网络的规模来自全球社区节点和外部供给，后续锚点由社区与合作方在其他区域共建。

我的显卡能赚多少？ 取决于完成了多少经验证的任务。参考基准是市场上同型号 GPU 的租赁价（RTX 4090 约 0.3-0.4 美元/小时），不承诺固定收益。没有网络需求时不会有排放。

\$OURO 什么时候发？ TGE 安排在 Evolve API 有付费客户、法律意见与代币审计完成之后（路线图 G3），计划在 2027 年四季度到 2028 年一季度之间。先产品、后代币。

美国用户能参与吗？ 使用产品和贡献算力不受限；代币发售对受限司法区实施地理与 KYC 限制，具体以法律意见为准。