

证据与附录

这一份只回答三个问题：凭什么做这个产品、技术上现在到底做到哪、风险看见了多少。所有结论给来源，不吹。

版本 v1 · 2026-10-19 来源 调研 / 工程仓库 / AF4 诊断 边界 二手调研与一手实测分开标注

证据与附录

项目：Launchpad / App-IPO 完整项目交付 · 05-证据 版本：v1.1 | 2026-10-19 12:50

(+08) 口径：唯一事实源 = 交付-2026-10-19/_工作/10-产品/00-产品基线-v2.md (下称《基线 v2》)。本文出现的本平台数字全部取自《基线 v2》§8；旧口径 (\$100K/\$350K 毕业线、5%/10% 押金、团队份额/vesting、另发平台币、5% 交易费) 一律标注已废弃，不作为任何依据。用途：回答三个问题——这个方向不是拍脑袋 (A-C)、技术不是画饼 (D)、风险已经看见 (F-H)。证据分级：一手实测=今天在本机/线上实际跑过、看过；二手调研=调研文档转述的官方文档/推文/第三方数据；未验证=只有设计或转述，没有独立证据。文末「本附录的边界」逐项列明。

A. 一页结论：凭什么做这个产品 (5 条)

- 需求侧已经成立，发行本身已商品化。近两个月至少 **40+** 家新发币台涌现 (Robinhood Chain / Solana / BSC / Arc / Ink / GIWA 合计)，差异化全部集中在费率、规则、策展、Agent——没有一家在讲「发行方收入是否真实」。来源：调研-1006-竞品最新/others.md §1、§1 末句。
- 空位可验证，不是我们没找到。对 205 条高互动推文 + 公开网络做专项排查，「zkTLS/密码学收入证明接进发币流程」零命中；最接近的 EDMA/Prism 是「文件审查 + 人或机构签字」，Prism 自认 demo；ONLYS 的收入分成币没有任何验证机制；Dokimo/Zolvency 只做

验证、不做发行。来源：[调研-1006-竞品最新/others.md](#) §3.1-§3.3（该结论仅在已读 205 条范围内成立，详见边界）。

3. 有人真的愿意为「真实收入」付钱，但现方案都缺可信验证。ONLYS 把 AI 模特月入 \$30K 的 10% 卖给持有人（项目自述）；COMETAIL 把未来链上手续费直接证券化；Pons 30 天费用自述 **\$137M**（第三方口径 \$97.1M，两口径冲突已记录）。来源：[调研-1006-竞品最新/others.md](#) §3.2、§5。
4. 技术可行性是实测的，不是 PPT。TLSNotary 对 Stripe / Apple ASC / RevenueCat / Paddle / GA4 / AdMob / Google OAuth / OpenAI / X / GitHub / httpbin **11 个主机 TLS 实测通过**，真实 API 证明跑通、端到端约 **0.65 秒**（同机下界）；2026-10-19 复跑 zkTLS 仓库 **104 项测试 / 0 失败**、Vela TEE 可验证加总 40 项通过、合约 46 项测试通过（复跑见 D 节）。来源：[正式文档/0918-zkTLS-最终方案.md](#) §四/§十、[~/projects/launchpad/zktls/](#)（commit [419e73c](#)）。
5. 窗口正在关闭，而我们在正确的位置。Hookr 近 **45 天**未发新币（Harmonic 官方自述，10/04；第三方 9/22 口径为 116 发行/67 毕业，两口径并存）、Hookdaq 域名 10/06 起解析失败、Noxa 于 7 月停运（累计费用约 \$12M）；同时 Uniswap v4 约 **87%** 成交量仍走无 hook 池子，hook 是叙事领先、采用滞后。验证端（Dokimo/Reclaim/zkPass/Primus/DIA）与发行端（Hookr/Pons/EDMA）任何一端往中间走一步就会撞上我们，护城河只能钉在「证明→定价→持续披露」这个缝合处。来源：[调研-1006-竞品最新/others.md](#) §4.5-§4.6、§3.3。

一句话：发币台已经过剩，可信的「收入证明」是稀缺品。我们不是再做一个发射台，是把「收入验证」做成发行流程的闸门。

B. 市场空位：25+ hook launchpad 排查结论

B.1 排查方法（先说清楚边界）

- 覆盖：[调研-1006-竞品最新/others.md](#) 点名 **25+** 家 hook / 发币平台（§1.1 列表，实际 40+ 家），读了点赞 Top 205 条推文（全量 221 条中第 206-223 行未读）+ 官方站点/文档/GitHub 交叉核对；Hookr / pools / PONS / Long / Arcus 另有专项拆解（来源见本节表格与 I.1）。
- 判定：凡「项目自称」标自述；官方文档/合约写明标已证实；我们的判断标推测。

- 核心结论：hook 生态没有任何人在做收入验证——Hookr 官方文档中 zkTLS / attestation / completeness 全部零命中；Hookr 说的「可验证」只指链上结算事件（"合约状态和已结算事件日志是首要来源", hookr.fun/methodology）；其他 hook 台（Hooked / Ember / Hookdaq / Programmable / Hookit / Flap Hook / Avax Hook）在已读材料里全部只讲「交易费怎么分」。

B.2 代表项目：做成了什么，留下了什么空位（竞品参数，非本平台口径）

项目 / 阵营	做成了什么（可引事实）	留下的空位	来源
Hookr (RH Chain, v4 hook)	发币时最多拼 5 个 hook 积木、规则开盘焊死；拍卖路径地板 0.22 ETH、毕业门槛 1.1 ETH，未达标全额退款+销毁+不开池；合约 MIT 开源（ Hookr-fun/hookr-contracts ），但明确未审计 ("No independent audit of Hookr 1 has been completed")	「可定制」不等于「可信」：没有发行方收入验证；近期发行停滞（45 天无新币，自述）；且 hook 整体采用率低（约 87% 的 v4 成交量仍走无 hook 池子）	0908-Hookr-三种发池方式+五种插件+门槛数字-详细拆解.md ； 正式文档/1011-Hookr代码能不能用-三个问题的答案.md ； others.md §1.1、§4.5、§4.6
pools.trade (Uniswap Labs 官方)	发币免费、LP 费 0.25% 回流池子、流动性永久锁定；Instant（曲线）+ Crowd Launch（4h TWAP，达 \$10K FDV 否则全退）； 自动复投 0.2% 规则由 Hayden 设计	官方免责声明明确「只允许发 meme 币，非 meme 资产请走 CCA」——正规项目被它自己排除；不做收入验证	调研-1006-竞品最新/pools.md §一/§三； 0908-四种发行机制对比...md §八
PONS (RH Chain 体量最大)	1% hook 费，70% 创作者 / 30% 协议，协议部分约 80% 回购销毁；曲线毕业（文档口径约 4.2 ETH；官方只写 graduationThreshold 参数，确切值未从官方文档确认）；30d 费用 \$137M / 收入 \$23M （项目自述；第三方口径 \$97.1M/\$17.9M，冲突记录在案）	体量最大但只证明「交易热度」，不证明「项目有真实收入」；曲线未达标不退款	others.md §1.1、§4.3、§5； 0908-Robinhood-Chain-Launchpad-调研报告-给领导.md 第一类； 0908-四种发行机制对比...md §八

项目 / 阵营	做成了什么（可引事实）	留下的空位	来源
Long (long.xyz)	用代币化股票 (NVDA/AAPL 等 200+) 做计价资产发币；LongX 把 3 倍杠杆仓做成 ERC- 20；股票流动性约 \$12M	「股票叙事」替代不 了「经营证据」；本 质仍是 meme 玩 法，且代币化股票≠ 真股票、无股东权利	0908- Robinhood- Chain- Launchpad-调 研报告-给领 导.md 第三/ 四部分； others.md §1.1
Hookdaq (hookdaq.fun)	自称「股票市场的 launchpad」：对着 \$SPY/\$NVDA/\$AAPL 发 币、创作者费按计价资产 结算、规则第一笔交易前 锁死、零种子、固定美元 开盘估值；公开做 Hookr 对比页	域名 10/06 起解析 失败 (ENOTFOUND), 真实产品状态/合约/ 发行量全部未找到； 只能算「营销占位」	others.md §2.1、§6
Arcus (dYdX 系)	累计交易约 \$20 亿（自 述）；把永续账户打包成 pToken (pBTC/pHOOD3x)，结 构等同杠杆 ETF	是 DEX/衍生品，不 是发行台；不做发行 方收入验证； pToken 只是「省去 维护」不是「消除风 险」	0908- Robinhood- Chain- Launchpad-调 研报告-给领 导.md 第七部 分及风险提示
Solana hook 集群 (Hooked/Ember/SPEC/Hookit 等)	37 条 transfer-hook 规 则、646 次发行 (Hooked 自述)； Ember 7 日曲线成交 \$53.1M (自述)；SPEC 71 个扩展；Hookit 称最 多 384 种组合 + 2 个 MCP	全部围绕「规则、费 用、防捆绑」，没有 一家回答「发行方收 入是否真实」	others.md §1.1、§3.4
最接近的「证据门槛」派 (EDMA / Prism)	EDMA：上架前把身份/资 产/营运证据/里程碑做成 规范 JSON 上链，季度重 认证；Prism：19 项链上 自动检查 + 协议哈希锚定	不是密码学证明： EDMA 靠 KYC + Attestor Registry 人 工签字，无独立第三 方证据证明有真实发 行方；Prism 自认 demo (0	others.md §3.2 ①②、 §6

项目 / 阵营	做成了什么（可引事实）	留下的空位	来源
		businesses / 0 raising / 0 holders)	

B.3 结论：空位在「缝合处」，不在「再做一个台子」

把「验证」和「发行」两端拆开看：验证端有 Dokimo（可验证收入，不发币）、Reclaim（"proof of revenue" 只是 RFP 用例）、zkPass/Primus/DIA（零件供应商）、Zolvency（zkTLS 收入证明，用于借贷）；发行端有 Hookr/Pons/EDMA。**没有一家把「链下收入证明」当作发币的前置条件、定价输入与持续披露义务。**这是我们要占的位置，也是唯一值得押注的护城河（[others.md](#) §3.3）。同时必须承认：空位不等于安全——两端都可能往中间走一步，所以窗口是「时间 + 缝合精度」，不是「独家专利」。

C. 机制选择证据

C.1 四种发行机制对比（为什么 CCA 主力、曲线二期）

机制	价格由谁定	达标后	未达标	适合	我们的用法
Bonding Curve	写死的数学曲线	曲线卖空即毕业进 v4 池	币挂曲线、不自动退款	meme/社区、要公平起步	二期：首期不开放购买，只做「Curve · Beta 预告」灰卡（《基线 v2》§5.3）
CCA（连续清算拍卖）	拍卖撮合，同批同价	达毕业线→按清算价建 v4 池	全额退款 + 未售销毁 + 不开池	正经项目、要保底与市场定价	一期主力：72h / 3 批 × 24h / 40%-35%-25%；毕业线 \$200,000（《基线 v2》§5.2）
时间驱动 (LONG/Airlock)	不定价，时间到即完成	到点标记完成	无保底	不关心募资的发行	不采用
TWAP 众筹 (pools Crowd)	时间加权均价	达 \$10K FDV 毕业	全额退款	短窗口众筹	不采用（与 CCA 重叠，且门槛过低）

结论（三理由）：① CCA 有毕业线 + 自动退款，最符合「验证是闸门」的风险叙事——验证不过就不该开拍卖，拍卖不达标就应原路退回；② 同批同价，消除曲线「先买便宜、后来贵」的抢跑结构，对首次买家更公平；③ 价格由市场发现，才能和「FDV 上限 = 10 × 已验证 ARR」的估值纪律对上。曲线的二期理由也清楚：长尾/未验证项目需要更低门槛、更短路径（pools Instant、District 即时发币只有 5 个字段），但「不退款 + 女巫」是硬伤，所以首期只留入口与灰标，不画成已可用。

C.2 Hookr MIT ≠ 我们可以随便抄：BUSL 到 2027-06-15

代码	许可证	我们能不能用	依据
Hookr 自己写的 hook 代码	MIT	能，随便改、可商用、可闭源（保留版权声明）	正式文档/1011-Hookr 代码能不能用-三个问题的答案.md §一/§三
它依赖的 Uniswap/v4-core	BUSL-1.1	复制/修改源码 → 商用受限到 2027-06-15；在此之前商用需向 Uniswap 买商业许可或不用	同上 §3.2（原文 "Change Date: The earlier of 2027-06-15..."）
Uniswap/v4-hooks-public、OpenZeppelin/uniswap-hooks	MIT	可以，官方/社区脚手架	同上 §3.4

关键法律区分：把 v4-core 源码抄过来改 PoolManager = 受限；只写一个 hook 挂到「已部署在链上的」PoolManager = 大概率不受限。但 hook 源码 import v4-core 的类型/接口不算「使用受 BUSL 保护的源码」，**必须法务确认**（该文档列了三个待法务问题）。**我们的取舍：**不抄 Hookr 整套（35 个合约、明确未审计、自己运维风险更大），只写一个「收入验证门控」极简 hook，用 OpenZeppelin 的 MIT BaseHook 起步，避开 BUSL 争议；2027-06-15 后 v4-core 自动转 MIT，与主网上线节奏天然对齐（正式文档/1011-Hookr代码能不能用-三个问题的答案.md §六/§七/§八）。

C.3 pools「0.2% 复投」：借机制，不借实现

项	内容	对我们的意义
机制原文	任何人可领走某 LP 仓位全部未领取手续费， 前提是把该仓位规模增加 0.2% ；手续费累积到超过 0.2% 时，套利者自然有激励来加仓并领费（Hayden 原推，2026-08-06）	不需要中心化 keeper，把「复投」外包给逐利市场——适合我们毕业后的锁死 LP 池与 VFY 配对池深度维护
可借鉴点	无 keeper、规则极简、复用 Uniswap token jar 原语、与「LP 永久销毁」不冲突（加的是仓位不是提走本金）	二期可做成「毕业池深度自动增厚」的可选模块，降低「池子越交易越薄」的风险
风险 / 待核	调研时没找到 0.2% 复投规则的合约地址或链上文档 ，只有 Hayden 文字描述与社区观察；官方文档口径仅博客 + 两条推文	不写进一期合约；先做监控（池深/手续费累积），等合约实现可核对再评估

结论： pools 这个设计证明「流动性维护可以不用人」；但它不是我们的差异化，也不该在首期占用工程资源。列入二期候选，前提是拿到可核对的合约实现（[调研-1006-竞品最新/pools.md](#) §三、§7.2）。

D. 技术可行性与现状

D.1 事实 / 证据 / 差距（技术状态，不吹）

事实（含模块）	证据（今天核实）	差距
zkTLS 方案：TLSNotary 做证明层 + 自研 Node 数据源框架 + Vela TEE 做验证/聚合 + 设计上 zkVerify 上链；仓库 11 个源码文件、15 个 provider 配置	仓库 ~/projects/launchpad/zktls/ (commit 419e73c, 2026-10-11)；方案见 正式文档/0918-zkTLS-最终方案.md §二/§三/§四	zkVerify 上链 zktls/ 与 v zkVerify 集成作 需求/方案文档 服务生产需求文档 真实商业证明、 生产服务（HA 做
104 项测试：2026-10-19 复跑 4 套测试 104 通过 / 0 失败（test/run.js 25、nsm-test.js 26、registry-test.js 13、vela-verify-test.js 40），含大量「反向用例」（假证明/篡改/空披露必须被拒）	本机 node test/*.js 实跑输出；docs/12-接通Vela并完成聚合.md 记录 27+32 项实测	测试证明的是 辑」，不等于「 用」；5 套测试 v1.sh 未复跑
Vela TEE 定位：Vela 做不了 zkTLS（WASM guest 无 net、禁止随机数/时间，Nitro enclave 无出口）→ 回到 L3：验证证明、跑业务聚合、出链上结论；TEE 可做 notary 加固（论文实测开销约 1.12 倍）	正式文档/0918-zkTLS-推导过程与批判收敛.md 假设 A、判断 G、判断 H；Vela 仓库 commit 01b105b (feat(aggregate): verifiable revenue aggregation inside the Vela TEE)	独立 notary 的 公共 notary notary.pse.c 2026-03-18 另 TLSNotary 自 notary-serve notary 集群/密
对 heliosgen 站的实测：未完成	0924-zkTLS-网站交互-demo 记录.md 的端到端 demo 用的是 api.open-meteo.com（公开天气 API），文末 §九把「对 heliosgen 本地站实测」列为下一步；全文件夹认知地图-2026-10-14.md 明确「对 heliosgen 站的实测从未完成」	测试站（helios zkTLS 的完整 项目演示前必须
合约：contracts-dev 5 个合约 + 17 项测试已提交（a138453, forge test 17/17 通过）；开发副本完成 OpenZeppelin v5.7.0 迁移，新增 29 项测试（含 fuzz，每项 1000 轮），2026-10-19 复跑 46 项全过（forge 1.5.1）	本机 forge test：2 个 suite, 46 tests passed, 0 failed；launchpad-contracts/OZ-MIGRATION-NOTES.md	OZ 迁移未提交 status：4 个 模块 AM、fuz 踪）；无审计（ 「尚未审计，勿 测试网部署（ 目录）；现有合 Curve + 5% 老 结构，与《基 力、无 vesting 存在结构性冲突 线

事实（含模块）	证据（今天核实）	差距
前端：Next.js（App Router）+ TypeScript，4 个路由（ <code>/</code> 、 <code>/t/[id]</code> 、 <code>/portfolio</code> 、 <code>/create</code> ）；2026-10-19 <code>npm run build</code> 通过（静态 7/7 页）	<code>launchpad-web</code> 仓库 README + 本机 build 输出	4 处假数据： ① 地址哈希确定性链（目命中 72 个）；② 3 步「出证明」本地模拟；③ 持仓与「我发的币」造；④ 价格走势联 SVG。无钱包（合约未审计前
数据层：Postgres 已真实灌数——launches 663 、trades 2728 、auctions 131 、holders 302 、candles/price_points 各 432 、auction_bids 521 、tokens 840 ；2026-10-19 复跑 19 项测试全过	本机 <code>psql</code> 查询； <code>launchpad-data</code> README； <code>npm test</code> 19 pass / 0 fail	索引器空转： <code>indexer_check</code> 行（chain_id 4 <code>contract_address</code> <code>last_block=0</code> <code>last_scanned</code> RPC 与合约地址 API 当前未运行 （127.0.0.1:87 来自克隆站，挂 开发
演示站： https://zklaunch-demo.pages.dev 可打开（2026-10-19 12:18 实测 HTTP 200，1.6s），但仍在用旧样例数据	线上抓取： <code>/assets/data.js</code> 与本地 <code>演示站/assets/data.js</code> sha1 完全一致 （ <code>c7cb180e...</code> ）；线上 24 条 launches / 10 条 graduated，6 个拍卖对象 <code>targetUsd=350000</code> ；本地 <code>app.js</code> 仍有 <code>\$100,000</code> 输入、 <code>\$10,000</code> 押金、团队 15% + 12 个月 vesting、6 步向导	数字口径与《基线 v2》 （\$350K/\$100K 押金、团队 15% 均已废弃），且旧站同源数据 <code>pools.trade</code> 等 2026-09-08 16:00《基线 v2》§8 Helios/Nebula 今晚须替换并匹

D.2 状态表：已可用 / 部分可用 / 未开始

已可用（可演示/可复核）	部分可用（能跑但不完整）	未开始
zkTLS 框架 + 验证器（104 测试复跑通过；真实 API 证明、白名单披露、凭证抹除、反滥用断言）	合约套件（46 测试通过，但机制是旧曲线/旧费率，OZ 迁移未提交，未审计、未部署）	CCA 拍卖合约、Uniswap v4 建池 + LP 销毁、门控 hook
Vela TEE 可验证加总（提交 01b105b；40 项独立复核测试通过）	前端（4 页可 build；4 处假数据、无钱包/真买卖）	外部审计、审计就绪包 16 项交付
数据层（Postgres 8 张表真实灌数 663/2728；19 测试通过）	演示站（可打开；口径旧、数据集旧，今晚修）	索引器接真链、查询 API 常驻、真链数据
合约（5 个合约 + 46 测试在本机全绿）	zkTLS 生产服务（notary 集群、zkVerify 上链、监控/部署/密钥）	测试网/主网部署、运营后台 O1、多签/时间锁/暂停守护者落地
工程纪律（Acta 预防清单 10 条对照 + 7 条特有风险；提交/测试习惯已建立）	权限与托管方案（1018 已完成文档，Stage 0 未落地）	KYC/地区屏蔽、法务意见（证券属性/BUSL）、真实项目方访谈

一句话：技术底座是真的，产品是半成品，发行/审计/合规是空白。今晚交付的是「可信的设计 + 可验证的技术证据」，不是「可上线产品」。

E. 设计依据：AF4 三大痛点 → 8 处改动（证据 → 改法 → 落屏）

AF4 诊断对象是旧版 App-IPO 界面，结论是：方向对，但界面还在讲别人的品类语言；最值钱的差异化只是一个徽章，不是一条能走完的信任链（[AboutFace4 整理/html/parts/project.html](#)「结论先行」）。三大痛点是：① 差异化不在第一屏；② 数字自己的账对不上；③ 核心动作的摩擦被当成「以后再说」。

10 个人物模型中，v6 直接服务 6 个：阿杰（首次买家，主人物模型）、老 K（degen）、林哲（项目方）、何嘉（审计）、唐蕊（运营）、刷子（负面，用规则而非文案对抗）；其余 4 个通过界面兜住：小鹿（可分享结论卡）/ 周姐（图表轴/单位/来源 + CSV/API）/ 阿浩（375px 移动端 + 底部抽屉）/ 王叔（中英双语 + 术语表 + 首屏人话版风险）。人物模型原文见 [AboutFace4 整理/html/parts/project.html](#)「用户模型 · 10 个人」。

产物状态（12:35 核对）：线框 v6 7 屏 + 总览已交付（[03-线框图/v6/*.html](#)、[03-线框图/线稿总览-v6.html](#)；自检：8 页 console error 0 / 横向溢出 0，见 [03-线框图/自检报告.md](#)）；高保真 5 屏已交付（[04-高保真设计/screens/*.html](#)；自检：5 屏 0 error / 0 横滚）。下表逐条

核对实际落屏文件与模块；未画到的条目已标「未落屏，今晚补」。v6 总览明示砍掉 D2/D7/D8/MB1/MB3/O1 六屏（D7 列「今晚补」）。

#	证据（旧界面）	改法（v6 / 高保真）	落屏（v6 实际文件/模块 → 高保真实际文件/区块；状态）
1	首屏=两张满图 banner + Trending + 已验证榜，没有一句「每个币背后是一个真实 app」；差异化被推到可选落地页（AF4 痛点①）	一句话价值主张 + 三入口（发项目/买项目/验证证明）+ 三证据（已验证项目 23 / 累计验证收入 \$4.82M / 最近链上证明 2 分钟前，可点）；banner 降第二屏	v6 V6-D1-首页.html · H1-M1 故事条 + H1-M2 实时证据流；高保真 01-home.html 首屏（三入口 + 三证据；另加 Verified leaderboard）。已落屏
2	项目卡=图+名字+涨幅+一堆标签，看不出 app 与 token 的关系（AF4 视觉改法表）	卡片拆「App 段（logo/一句话/品类/连接点）+ Token 段（价格/进度/倒计时/持有人）+ 验证条（◆收入已验证·来源·覆盖 12 月·更新时间）」	v6 V6-D1-首页.html · H1-M4 双段卡 6 张；高保真 01-home.html 卡网格（Helios 拍卖 / Nebula 已上线 / Lumen 曲线 Beta / Kite 即将开拍，金色验证条）。已落屏
3	v5 三栏骨架在，但 K 线/买卖/成交压在右栏，收入证据埋在中栏深处；v5 还把验证通栏取消了（AF4 ch9/ch17）	中栏顺序固定「证据条 → App 业务指标 → 走势图 → 里程碑 → 季度报告 → 代币用途 → 团队 → 持有人」；左锚点 5 条；右栏价格+动作 sticky；顶部拍卖状态条	v6 V6-D3-项目页-已上线.html （19 模块，C1→T1→F1→C3...C10）与 V6-D4-项目页-拍卖中.html （21 模块，A1+B1），两态均已落屏；高保真 02-project.html 为拍卖态（D4）：三栏 + 可分享结论卡 + T1 + F1 + 中栏同序。部分落屏：高保真未出 D3 已上线态（不阻塞今晚，如需双态高保真列今晚后补）
4	徽章 ◆/◇ 只是一个 tag，串不起「来源 → 覆盖期 → 检查项 → Proof → 复核」（AF4 ch11）	新增 Trust Chain 六节点：结论 → 来源 → 覆盖期 → 4 项检查 → 链上 Proof ID → 本地复核；徽章只做入口，项目页/验证页/持仓页三处复用	v6 V6-D3 T1 + V6-D4 T1 + V6-D5-验证页.html V-M1/M2；高保真 02-project.html 六节点 + 03-verify.html 六节点（两处复用）。部分落屏：D7 持仓页未落屏，今晚补（v6 总览 CUT 表已列）；三页复用只落了 2/3
5	出价面板出现「Est receive 0% / 0 TOKEN」；最坏结果埋在进度条下小字；未连钱包行为未定义（AF4 痛点③）	五行「最多花多少 → 最高单价 → 最坏到账 → 费用 → 退款条件」；未连钱包先解释再禁用；不公开个体 Max 上限	v6 V6-D4 B1 五段式 + B1-未连钱包变体 + V6-MB2-移动-项目页.html 出价底部抽屉；高保真 02-project.html 右栏 B1（Max spend / Max price / worst fill / fees / full refund）。已落屏（移动端仅 v6，无移动高保真）
6	验证页以「拖文件复核」为主视觉，普通投资人像在打开开发者工具（AF4 ch9/ch16）	改「审计底稿」：结论卡置顶（可引用/可导出 PDF/JSON/分享 URL）→ 4 项检查快照 → 本地复核降	v6 V6-D5-验证页.html V-M0-V-M5；高保真 03-verify.html （结论 hero 中性底金边、4/4 检查、导出 PDF/JSON/分享、二级复核、开放范围）。已落屏（高

#	证据（旧界面）	改法（v6 / 高保真）	落屏（v6 实际文件/模块 → 高保真实际文件/区块；状态）
		二级抽屉；失败写清缺哪个月	保真另加 Trust Chain 六节点 + 证明过程 4 步)
7	发币向导 7 步单页长表单，押金/里程碑到第 7 步才出现；「验证可跳过」不写代价；团队/vesting 字段残留（AF4 ch10/ch12）	界面压 4 段（字段仍按 7 步完整定义）：①项目与代币 ②连接数据源+出证 ③发售与资金（12 个月现金流预览、押金 5%）④核对与签名；入口写「约 10 分钟 / 费用明细 / 哪步可跳过」；删团队/vesting	v6 V6-D6-发币向导.html · W-M1 入口承诺 + W-M2 步骤条 + W-M2b 4 段↔7 步映射 + W-S1-S4， 4 段已落屏 ；高保真 04-launch.html 仅 Step 2-3 （Step 1/4 按 stepbar 示意，产品线已允许）。 部分落屏：高保真 2/4 段
8	没有「钱在哪」模块；拍卖/放款/押金/退款状态散落；只有成功路径，无空/错态（AF4 场景 3/4、ch15）	新增 资金状态机 四格（已募/托管余额/下一笔触发条件/失败退款）+ 统一状态词 + 8 个标准空/错模板（无钱包/无数据/验证失败/拍卖失败退款/网络错误/退款中/已结束/无权限）	v6 V6-D3 F1 + V6-D4 F1 + V6-S1-状态板.html 8 模板；高保真 02-project.html F1 四格 + 05-design-system.html 7 个状态词。 部分落屏：D7 未落屏，今晚补；8 模板仅 v6，无高保真

E.1 为什么不直接抄竞品

我们研究了 District、MetaDAO、Nemesis、WorkAgnt、First Dollar 五个参照产品（[参照产品调研-2026-10-18/report/index.html](#)），结论是：它们没有一个是「更好的 launchpad」，而是五个不同问题的解法——District 解决「定位要短」（三入口 + 累计收益），MetaDAO 解决「机制要可见」（钱在托管、下一笔条件、失败退款），Nemesis 解决「复杂交易要做简单」（最坏结果前置），WorkAgnt 解决「使用要实时」（实时证据流 + 4 步上手），First Dollar 解决「工作要可结算」（状态流水线 + 状态词）。我们抄的是这五个**模式**，不抄它们的**内容**：

- **不抄倍数当主指标**：District 用 ATH 倍数讲结果，会吸引投机用户，与「proof」定位冲突；
- **不抄功能堆首页**：WorkAgnt 首页 10+ 段、First Dollar 三个市场并列，都会稀释主任务；
- **不抄「计划中混成已上线」**：它们至少标了 testnet / Planned；我们更要把「演示数据 / 未验证 / 待接入」标清楚。

最反面的证据来自 District 与 First Dollar 自己：**District** 项目页只有项目卡 + 交易 + Open App 外链，App 指标/收入/里程碑都不在页面里；**First Dollar** 的「Get Verified」点进去回首页，根本没有验证页。这正是我们的空位——「验证做成独立页、项目页放 app 证据」别人

没做，只能自己长出来。所以 v6 的差异化不靠「更像谁」，靠「一条能走完、能看懂、能复核的信任链」。

F. 风险登记册（15 条）

概率/影响为主观判断（高/中/低），用于排序，不作为量化承诺；「触发条件」是预先写死的检查点。

#	风险	概率	影响	缓解动作	负责人角色	触发条件
14	第三方数据源 / TLS 1.2 约束：某数据源弃用 TLS 1.2 或 P-256/AES-128-GCM	中	中	定期探测（复刻精确 offer 列表）；不通切 proxy 模式；多数据源冗余	技术负责人	探测失败或数据源 API 变更
15	BUSL / 克隆数据 / 其他法务与合规：v4-core 商用受限到 2027-06-15；演示站含第三方克隆数据	中高	中高	不抄 v4-core，用 MIT 脚手架；法务确认三个问题；今晚替换演示站数据、生产环境禁克隆数据	技术 / 法务	引入 v4 依赖前、每次部署前

G. 路线图：今晚 → 本周 → 4 周 → 主网前

与《基线 v2》§12 的 5 项未定项保持一致：未定项在路线图中是「门槛」，不是「假设」——不拍板就不进入下一步。

阶段	交付物	门槛（做完怎么算过）	与未定项的关系
今晚 (10/19 20:00)	产品方案 v2 (16:00)、线框 v6 (6 屏+总览+状态板, 18:00)、高保真 4 屏+设计系统板 (19:40)、一页纸、证据附录；演示站替换为《基线 v2》§8.2 数据集	旧口径 grep 零命中；数字自洽脚本通过；1440/375 截图；无 console error、无横向溢出；页脚「口径：产品基线 v2 · 2026-10-19」	押金 80% 界面标「待拍板」；曲线全程标 Beta · 即将开放
本周 (10/20– 10/25)	① 口径冻结 (§7 裁决 + §12 未定项登记) ② CCA 规格与参数表 (72h / 3 批 × 24h / 40%-35%·25% / \$200K / 2% / 10×ARR) ③ 合约：OZ 迁移合并提交、门控 hook 最小版 (OZ uniswap-hooks MIT)、CCA 合约骨架 ④ zkTLS：Stripe 受限密钥真实证明、Vela 聚合接生产、zkVerify 提交接口定义 ⑤ 前端接真 API (数据层 19 测试) + 钱包占位 ⑥ 权限 Stage 0：Den Safe 2-of-3、24h 时间锁、ACCESS-CONTROL-MATRIX、凭证台账 ⑦ 测试网 (Horizen Chain ID 2651420) 部署 5 合约 + 源码验证	46 + 104 + 19 项测试全绿；测试网地址可在浏览器查到源码；1018 §6.1 八项 Stage 0 验收；zkTLS 真实商业证明产物落盘	押金 80% 必须在押金模块开工前拍板 (10/21)
4 周 (10/26– 11/16)	① CCA 拍卖 + v4 建池 + LP 销毁 E2E ② 外部审计启动 (审计就绪包 16 项齐备) ③ 运营后台 O1 (待审/复核/资金动作/留痕) ④ zkTLS 生产服务 (notary ≥2、HA、监控、部署手册) ⑤ 前端四页全部换真数据、假数据清零 ⑥ 法务三件：证券属性、KYC/地区、BUSL ⑦ 拍卖失败/退款/罚没演练	测试网 E2E 跑通一轮 (发币→验证→拍卖→放款)；审计 kickoff；假数据清零；演练记录留档	曲线是否开放购买在此阶段拍板 (10/23 前)；若不上，首页继续灰标
主网前 (审计通 过后)	① 外部审计通过、高危清零 ② 金库 4-of-7 + 7 天时间锁 + 暂停守护者 2-of-3 + 证明签名密钥分离/门限评估 ③ 主网部署 + 源码验证 + 公开地址页 ④ 合规：条款/风险/退款页、KYC 决策落地、地区屏蔽 ⑤ 季度演练 + 备份恢复 + 事故响应演练	1018 §10 验收标准全绿；「无审计不上主网」红线；验证门控 (无验证不上 CCA) 与 FDV 上限链上强制生效	KYC/地区屏蔽 最晚 10/30 拍板；汇率取价按「USDC 收、不引预言机」执行

《基线 v2》§12 第 5 项（曲线虚拟储备定价公式）随曲线二期冻结：一期页面不显示内部公式，只保留「起售价 + 5 ETH 毕业线」；二期定公式前不得在对外材料中出现具体参数。

H. 决策记录与待拍板

H.1 已裁决（引《基线 v2》§ 7，5 条）

#	事项	裁决	废弃的旧口径
1	CCA 毕业线	\$200,000 （失败全额退款 + 未销毁 + 不开池）	\$100K / \$350K 演示数字已废弃
2	上市押金	募资额 5% （现金 2.5% + 等值 VFY 2.5% ），非收入，按季度达标分 4 批释放	押金固定额方案（含 \$18,000 旧例）已废弃； \$10,000 是 \$200K 募资按 5% 的示例值，不是旧口径
3	平台币	VFY 一币双角色 （交易对基准 + 回购标的），不另发平台币	0928 双代币方案已废弃
4	代币分配	只有两处：发售量 + 建池预留；无团队份额、无社区/生态/金库预留、 无 vesting	旧 10/20/25/30/15 + vesting 模板已废弃
5	验证口径	指定验证方出证 · 任何人可复核	「任何人可验证 / 零信任 / 数学保证一切」已废弃

另两条同日裁决（同源）：里程碑放款 **30%/30%/40%**；交易费 **0.3%**（0.1 回购销毁 + 0.1 买 VFY + 0.1 平台金库）。旧 5% 交易费「已废弃」。

H.2 待拍板（3 条）

事项	建议	影响	最晚决策时间
押金达标线 80% (《基线 v2》§12.1, 界面已按 80% 展示并标「待拍板」)	按 80% 冻结: 季度实际收入 $\geq$ 申报目标 80% 视为达标, 连续 2 次失败冻结并降级	押金合约参数、季度释放 25%、持仓页进度、条款与罚没争议	2026-10-21 (押金模块开工前)
曲线是否/何时开放购买 (§12.2, 页面现标 Beta)	一期不开放购买, 只保留「Curve · 即将开放」灰卡与筛选; 二期窗口放在主网上线后 4-8 周, 前提是退款/女巫/限额规则齐备	首页/项目页卡片、合约排期、长尾供给节奏、审计范围	2026-10-23 (一期前端开发前)
KYC / 地区屏蔽 (§12.3, 一期产品页不承诺)	一期不做 KYC、做地区屏蔽 + 条款 + 不作 KYC 承诺; 主网前根据法务意见决定是否引入供应商	合规风险、转化率、运营人手、上市节奏	2026-10-30 (主网上线前合规评审)

I. 附录

I.1 关键来源清单 (24 条)

A. 内部事实源与产品基线

- 交付-2026-10-19/_工作/10-产品/00-产品基线-v2.md (唯一事实源)
- 交付-2026-10-19/_工作/00-审计/01-产品现状与v2提纲.md
- 交付-2026-10-19/_工作/00-审计/02-线框现状与v6方案.md
- 交付-2026-10-19/_工作/00-审计/03-设计现状与高保真方案.md

B. 竞品与机制调研 (二手调研)

5. 调研-1006-竞品最新/others.md (25+ hook launchpad 排查 + 可验证收入专项) 6. 调研-1006-竞品最新/pools.md (0.2% 复投、\$10K FDV、meme-only 限制) 7. 调研-1006-竞品最新/hookr.md、pons.md、uniswap.md (同日调研全量材料) 8. 0908-四种发行机制对比-Bonding-Curve-CCA-时间-TWAP-与设计取舍.md 9. 0908-Hookr-三种发池方式+五种插件+门槛数字-详细拆解.md 10. 正式文档/1011-Hookr代码能不能用-三个问题的答案.md (MIT / BUSL-1.1 / 2027-06-15) 11. 0908-Robinhood-Chain-Launchpad-调研报告-给领导.md (生态全貌与风险提示) 12. 0902-Launchpad-产品设计-三问详解.md (合规红线: Howey、Pump.fun 诉讼; 旧机制参数已废弃)

C. zkTLS 技术 (一手实测 + 方案)

13. 正式文档/0918-zkTLS-推导过程与批判收敛.md (10 条判断推翻 6 条) 14. 正式文档/0918-zkTLS-最终方案.md 15. 0916-zkTLS服务生产需求文档.md

16. `~/projects/launchpad/zktls/` (commit `419e73c` ; `docs/06`、`docs/10`、`docs/12` ; `test/` 四套测试) 17. `~/projects/launchpad/vela/` (commit `01b105b` ; TEE 内可验证聚合) 18. `0924-zkTLS-网站交互-demo记录.md` (open-meteo 闭环; heliosgen 未做)

D. 设计、参照产品与工程状态 19. `AboutFace4整理/html/parts/project.html` (AF4 项目诊断: 三大痛点/10 人物/5 参照/逐章判决) 20. `参照产品调研-2026-10-18/report/index.html` 与 `notes/{district,nemesis,workagnt,firstdollar}.md` 21. `1018-Launchpad-权限托管与韧性方案-v1.0.md` (多签/时间锁/非托管/审计就绪包) 22. `1011-看板-Launchpad开发总盘.md`、`1011-Acta教训-我们的预防清单.md` 23. `全文件夹认知地图-2026-10-14.md` (heliosgen 未实测、资产地图) 24. 工程实况 (2026-10-19 本机核实): `launchpad/contracts-dev/`、`/Users/jethalo/.dsh/bot/workspace/{launchpad-contracts,launchpad-web,launchpad-data}`、`演示站/assets/data.js`、<https://zklaunch-demo.pages.dev>

I.2 术语表 (20 词, 中英)

#	中文	English	一句话解释
1	zkTLS	zero-knowledge TLS	证明「某时刻某请求返回了某段真实数据」而不暴露凭证的技术总称
2	指定验证方	designated verifier / notary	对证明签字的信任锚；zkTLS 的第三方验证只验它的签名
3	TLSNotary	TLSNotary	我们采用的 zkTLS 实现（Rust, MPC 模式, pin alpha.15）
4	zkVerify	zkVerify	证明验证链，用于把证明哈希/摘要锚定上链（ 本期未接 ）
5	可信执行环境	TEE	硬件隔离的执行环境；Vela（Nitro）用于验证与聚合，不做 TLS
6	连续清算拍卖	CCA（Continuous Clearing Auction）	分批撮合、同批同价、按清算价成交的一期主力发行机制
7	联合曲线	Bonding Curve	价格由数学公式决定的单边发售机制（二期）
8	毕业	Graduation	达标后建 Uniswap v4 池并销毁锁定 LP 的动作
9	完全稀释估值	FDV（Fully Diluted Valuation）	单价 × 10 亿；本项目上限 = 10 × 已验证 ARR
10	年化经常性收入	ARR（Annual Recurring Revenue）	已验证收入年化值，是 FDV 上限的输入
11	上市押金	Deposit	募资额 5%，现金 + 等值 VFY 各半，非收入，按季释放
12	里程碑放款	Milestone Disbursement	非托管金库按 30%/30%/40% 三批、按验证结果放款
13	非托管	Non-custodial	平台无任意提取权限，资金只按规则放款或由用户 claim
14	多签	Multisig	N-of-M 签名钱包（Safe/Den），消除单人权限
15	时间锁	Timelock	变更排队 ≥24h（主网 7 天），给其他人取消窗口
16	回购销毁	Buyback & Burn	已验证净收入 20% 回购（一半销毁项目币、一半买 VFY 质押）；对外只写「回购」
17	v4 钩子	Uniswap v4 hook	挂在池子交易/建池等生命周期上的自定义合约；我们只做「收入验证门控」一个

#	中文	English	一句话解释
18	商业源代码许可	BUSL-1.1	Uniswap v4-core 的许可证，商用受限至 2027-06-15
19	女巫	Sybil	批量账号套利；用证据链 + 限额 + 冷却对抗
20	三层验证	L1/L2/L3	L1 归属（GitHub OAuth）、L2 经营数据（收入/流量）、L3 季度复验

J. 演示站旧口径替换清单（今晚代码唯一依据）

目标文件：`演示站-en/assets/app.js` (133,830B, sha1 `6cab8535...`，与线上 <https://zklaunch-demo.pages.dev/assets/app.js> 完全一致) + `演示站-en/assets/data.js` (100,974B, sha1 `c7cb180e...`，与 `演示站/assets/data.js` 同源)。行号以 `演示站-en` 为准；中文变体 `演示站/assets/app.js` (sha1 `fc1817a4...`) 需同步改，行号在表内单列。线上站点就是 `演示站-en`，改完以线上为准。更新 (2026-10-19 13:22)：演示站已按本清单与《基线 v2.1》完成改造并重新部署 (<https://zklaunch-demo.pages.dev>)：6 条 canonical 数据、毕业线 \$200,000、押金 5%、30/30/40、覆盖 12 个月、4 段向导、无团队/vesting；旧口径 grep 零命中。J.3 验收：静态 10/10 PASS、运行时 16 PASS / 0 FAIL。本附录 D/J 节保留交付时 (12:24) 快照作对照。文件分工：数值/价格/拍卖对象在 `data.js`；覆盖期、MAU、\$777,777、押金、向导、团队/vesting 等展示文案全在 `app.js` 硬编码。下表行号按实际所在文件给出。执行原则：先整包替换 `data.js` 为《基线 v2》§8.2 数据集，再改 `app.js` 里所有硬编码字符串。只换 `data.js` 不改 `app.js`，页面照样出现 \$777,777、6 步、团队 15%、\$10,000 押金；只改 `app.js` 不换 `data.js`，24 条克隆数据与 \$350,000 目标仍在。所有新值只从《基线 v2》§5/§6/§8 取。今晚基准 (Helios 拍卖态)：已验证 ARR \$284,000 (覆盖 12 个月 2025-10→2026-09，缺 0 月；Stripe 68% / App Store 32%，GA4 ☉)；第 2/3 批，剩 31h，已承诺 \$168,200 (毕业线 \$200,000 的 84%)，指示清算价 \$0.00205，参与 1,264，单地址上限 2,000,000 HELI；FDV 申报 \$2.40M (锚定价 \$0.0024)，FDV 上限 \$2.84M (=10×ARR)；押金 5% (示例 \$10,000 = 现金 \$5,000 + VFY \$5,000)；里程碑 30/30/40。

J.1 旧值 → 新值 → 出现位置 (15 行)

#	旧值（现状）	《基线 v2》 新值	出现位置（文件:行号 / 字段）	改法 / 陷阱
1	毕业线 \$350,000 （拍卖 <code>targetUsd</code> ）	\$200,000 （毕业门槛，不是募资目标）	演示站— <code>en/assets/data.js</code> L1214 / L1332 / L1450 / L1568 / L1686 / L1804 （6 个 auction 对象 <code>targetUsd</code> ）； <code>app.js</code> L530 兜底 <code>{raisedUsd:205000, targetUsd:350000}</code> ；中文站 <code>app.js</code> L465 （ <code>data.js</code> 同行号）	首选整包换 §8.2（Helios 毕业线 \$200,000）；若包底改 <code>targetUsd:200000</code> <code>raisedUsd:168200</code> 陷阱：不要动 <code>FDV</code> <code>10K/50K/100K/150K</code> （ <code>app.js</code> L1435/L1439/L1440 ）——那是市值档位 毕业线
2	毕业线文案 \$100K	\$200,000 graduation floor	演示站— <code>en/assets/app.js</code> L803 <code>"Auction · \$100K graduation"</code> ；中文站 <code>app.js</code> L735 <code>"Auction · 毕业线 \$100K"</code>	改 <code>"Auction · \$200,000 graduation floor"</code> ； <code>Targeted Graduation floor</code> 部改 <code>Graduation floor</code> （ <code>en</code> L547/L549 、中文站 L482/L484 ）
3	向导募资目标 \$100,000 （readonly 输入）	\$200,000	演示站— <code>en/assets/app.js</code> L710 <code>Raise target</code> <code><input value="\$100,000"></code> ；中文站 <code>app.js</code> L642 募资目标 同值	改 <code>\$200,000</code> ， <code>Graduation floor</code> 毕业线（不是募资目标）
4	押金写死 \$10,000 （无百分比）+ 曲线也写 0.5 ETH（AF4 旧截图另见押金 \$18,000 ，当前代码无命中，不要补）	募资额 5% （现金 2.5% + 等值 VFY 2.5%）；Helios 示例 \$10,000 ；曲线无押金，只有建池费 0.0005 ETH	演示站— <code>en/assets/app.js</code> L708 （ <code>\$10,000 / 0.5 ETH</code> ）、 L816 显示、 L923 / L950 （Deposit \$10,000）；中文站 <code>app.js</code> L640 / L748 / L855 / L882	固定金额改成「5% raise · example \$10,000 (\$5,000 + \$5,000 VFY)」； <code>curve</code> 显示「建池 0.0005 ETH」。附注： \$10,000 不是要改成 5% 的，是
5	押金退还 35% / 0%	每季释放 25% ，4 批；达标线季度收入 $\geq$	演示站— <code>en/assets/app.js</code> L923–924 （35% + tube 35%）、 L950 （0%）；中文站 <code>app.js</code> L855–856 / L882	改「Released 25% per quarter · 4 batch」 <code>target ≥80% of reported revenue</code>

#	旧值（现状）	《基线 v2》 新值	出现位置（文件:行号 / 字段）	改法 / 陷阱
		申报目标 80%；连续 2 次失败冻 结并降级		tube 只允许 25/50/75/100； 「35%」
6	团队 15% + vesting 12 个月线性	无团队份 额、无 vesting （只有发售 量 + 建池预 留）	演示站-en/assets/app.js L687（步骤名 "Team & Revenue"）、L774-775（Team allocation 15% / Vesting 12-month linear）、L1587（设 计系统 stepbar）；中文站 app.js L619（steps 数组）、 L704-707	删两个输入框与 placeholder="" 步骤名改 "Rever terms / 收入与条 可保留否定声明 team allocation vesting」。AF4 记 「45%」当前代 命中，不要补
7	6 步向导	4 段呈现 （字段仍按 7 步：①=旧 ①，②=旧 ②⑥，③=旧 ③④⑤，④= 旧⑦）	演示站-en/assets/app.js L687 steps 数组（①Token ②Claim Project ③Sale Method ④Team & Revenue ⑤Revenue Verification ⑥Review & Deposit）、L797 / L1589；中文 站 app.js L619 / L649 / L704-L729	steps 数组改 4 段 Project & token Prove revenue Sale & funds / Review & sign * 卡合并为 4； 4 节点。陷阱：不 6 卡删成 4 卡了 段映射要按基线 保留
8	覆盖期 "12 months covered" 与 "6 months" 并存（另有 GA4 "9 months"）	Helios: 12 个月 （2025- 10→2026- 09）、0 缺 月；GA4 未 连接（不显 示流量覆 盖）	演示站-en/assets/app.js L469 / L702（12 months）、 L1002（"6 months claimed"）、L1011（"6 months · 100% complete"）、L480 （GA4 9 months）；中文站 app.js L407 / L634（12 个 月）、L934 / L943（6 个月）、 L418（GA4 9 个月）	统一为「Covera months · 0 miss 2025-10→2026 验证失败模板保留 缺月，改「11 of months · missing 2026-07」；删 C 盖行
9	\$777,777 fixture 复用	\$284,000 （Helios 已 验证 ARR）；来 源拆分： Stripe \$193,120	演示站-en/assets/app.js L461 / L701 / L1008 / L1228 （4 处）；中文站 app.js L399 / L633 / L940（3 处）；假收入 序列 revY EN L435 / 中文 L373（402/518/661/778）	全部换 \$284,000 （TTM）标签改 收入图按 Stripe/ Store 两源拆分， 402/518/661/77 列

#	旧值（现状）	《基线 v2》 新值	出现位置（文件:行号 / 字段）	改法 / 陷阱
		(68%) + App Store \$90,880 (32%)		
10	MAU 84,210 + 14.7% 粘性 + MAU 增长图	不显示 (Helios 的 GA4 = 0 未 连接; 「Null is not zero」, 不 是 0)	演示站-en/assets/app.js L473 / L475-476 / L479 、 MAU 数组 L437-438 ; 中文站 app.js L411 / L413-414 / L417 ; traffic 工具提示 EN L63/L254/L358/L451/L1418 、 中文 L194	删 MAU 三卡与图 示 "Traffic · GA4 connected — No shown"; 12K M 具提示改「Traffic connected」。AF 的 45,800 当前 命中, 不要补
11	对外表述 " Anyone — fully permissionless "	指定验证方 出证 · 任何 人可复核	演示站-en/assets/app.js L1057 ; 中文站 app.js L989 ("任何人都可以, 不需要许可")	改 Designated verifiers issu proofs · anyone recheck / 指定 证 · 任何人可复核
12	FDV \$18K vs 已募 \$284K (数字自相矛盾)	FDV 必须 = 单价 × 10 亿; 已募 ≤ FDV × 发售 比例; Helios 示 例: FDV \$2.40M / 已承诺 \$168,200	演示站-en/assets/data.js L1115 (ABE fdvUsd 37,509) vs L1213 (同一 ABE 对象 raisedUsd 283,500, 已募 > FDV); L1933 (UNISOCKS fdvUsd 18,872 ≈ \$18K 卡); AF4 旧截图记录 \$18K/\$284K	整包换 \$8.2 数据 保留旧样例, 加 raisedUsd <= * salePct 且 t ≈ priceUsd × 1 ABE/UNISOCKS 现在新演示集中
13	时间戳过期: 数据 2026- 08/09 、验证 2026-10- 08	演示时间 2026-10- 19 ; Helios 最近验证 2026-10- 19 10:12 、 拍卖剩 31h (第 2/3 批)、覆盖 2025- 10→2026- 09	演示站-en/assets/data.js 24 条 createdAt (如 L13)、ABE endsAt L1217 (2026-09- 10)、poolPriceSeries 2026- 09-08; app.js L469 / L702 "Last verified 2026-10-08"; 中 文站 app.js L407 / L634	全部 K 线/时间轴 2026-10; ends 当前时间 + 31h 批剩余); 验证时 2026-10-19 10: Next review 改 2027-01

#	旧值（现状）	《基线 v2》 新值	出现位置（文件:行号 / 字段）	改法 / 陷阱
14	24 条克隆数据 / 10 graduated （含 Hookr.fun、pools.trade 等第三方真实代币）	《基线 v2》 §8.2 四项 目：Helios （拍卖）/ Nebula（已 上线）/ Lumen（曲 线 Beta）/ Kite（即将 开拍）+ 首 页证据数字 （23 / \$4.82M / 2 分钟前 / \$1.36M）	演示站-en/assets/data.js L1-L4140 全文件（24 条 launches）；中文站 data.js 同源。红线： cloned 数据只许本地开发，不许上线	整包替换；若时间够，至少落 Helic Nebula 两条 + 首 据 + 四种状态各 （数据必须来自 不得再用第三方真 币名）
15	其他写死文案："21% above floor"、"Target"、"Full refund if the target is not met"、"Verified annual revenue (TTM)"	指示溢价动 态算或删； 统一「毕业 线 / graduation floor」；退 款条件按基 线 \$5.2 (< \$200,000 全额退款 + 销毁 + 不开 池 + 不收发 行费)	演示站-en/assets/app.js L542 (21% above floor)、 L547/L549 (Target/Pool created at)、 L550 (target is not met)、 L461 (TTM)；中文 站 app.js L477 / L482 / L484 / L485 / L399	删写死 21%； Target→Graduation floor；退款句改 refund + unsold burned + no pool issuance fee if r \$200,000 at 72h TTM→ARR

J.2 今晚执行顺序（4 步）

1. 备份：cp -r 演示站-en/assets 演示站-en/assets.bak-20261019 （只备份，不改旧文件内容）。
2. 换数据：按 §8.2 重写 演示站-en/assets/data.js （4 项目 + 首页证据数字 + 拍卖/已上线/曲线/即将开拍四态）；同步 演示站/assets/data.js （两文件同源）。
3. 改 app.js：按 J.1 的 15 行逐条改；先全文 grep 旧值清单，再改，再 grep 一遍。
4. 跑验收断言（J.3）+ 1440/375 截图 + 线上部署到 zklaunch-demo 项目。

J.3 验收断言（改完逐条跑，全部通过才算完）

#	断言	检查方式
1	旧毕业线零命中	<code>grep -n "\\$350K \\$350,000 350000 \\$100K \\$100,000 100000"</code> 演示站-en/assets/app.js 演示站-en/assets/data.js → 0（FDV tiers 100K 无\$前缀，不算旧口径）
2	押金只为 5%	<code>grep -n "18,000"</code> → 0；所有 <code>\$10,000</code> 上下文含 <code>5%</code> 或 <code>example</code> ； <code>grep -n "35% refunded refunded.*35%"</code> → 0；退款百分比仅 25/50/75/100
3	团队/vesting 字段清零	<code>grep -n "Team allocation Vesting 团队持有比例 placeholder=\"15%\""</code> → 0； <code>grep -n "Team & Revenue 团队与收入"</code> → 0
4	向导 4 段	<code>steps</code> 数组 length = 4； <code>grep -c "class=\"stp"</code> = 4；⑥ 不再作为步骤号出现；4 段 ↔ 7 步映射表在页面可见（基线 §6 D6）
5	覆盖期统一 12 个月	<code>grep -n "6 months 6 个月 9 months 9 个月"</code> → 0； <code>grep -n "12 months covered 覆盖 12 个月"</code> ≥ 1；失败模板保留 <code>missing 2026-07</code> 且为 11/12
6	\$777,777 清零、\$284,000 就位	<code>grep -n "777,777 777777"</code> → 0； <code>grep -c "284,000"</code> ≥ 3（项目页/验证页/发币页）； <code>TTM</code> 标签 → 0
7	MAU 清零、GA4 空态可见	<code>grep -n "84,210 45,800 MAU 月活"</code> → 0（项目页范围）； <code>GA4 not connected GA4 未连接</code> 存在； <code>Null is not zero</code> 文案存在
8	FDV/募资自治	脚本遍历 <code>launches</code> ： <code>fdvUsd ≈ priceUsd × 1e9</code> (±1%)；有 <code>auction</code> 的项 <code>raisedUsd ≤ fdvUsd × 发售比例</code> ；ABE / UNISOCKS 不在数据集中
9	对外表述	<code>grep -n "permissionless 任何人可以 无需许可"</code> → 0； <code>designated verifier 指定验证方</code> ≥ 1
10	时间戳	<code>grep -n "2026-09-10 2026-10-08"</code> → 0；Helios 验证时间 = <code>2026-10-19 10:12</code> ；所有 K 线/时间轴日期 ≥ 2026-10-01
11	页面自检	复用 <code>03-线框图/_build/check.js</code> 思路：1440 与 375 各页 console error = 0、 <code>scrollWidth == innerWidth</code> 、无横向溢出；首页三证据 = 23 / \$4.82M / 2 分钟前 / \$1.36M

本附录的边界

一手实测 (2026-10-19, 本机/线上, 可复现): `forge test` 46 项通过 / 0 失败 (forge 1.5.1, `launchpad-contracts` 工作副本); zkTLS 4 套测试 25+26+13+40 = **104 项通过 / 0 失败** (`~/projects/launchpad/zktls`); 数据层 `npm test` 19 项通过、`psql` 实查 8 张表行数 (663/2728/131/302/432/432/521/840)、索引器 checkpoint 为空转状态; 前端 `npm run build` 通过 (4 路由); 演示站 HTTP 200、线上 `data.js` 与本地 sha1 一致、旧数字与 6 步/团队/vesting 残留实见; 合约仓库 `git status` 未提交状态。

二手调研 (转述官方文档/推文/第三方数据, 未独立复算): 25+ hook launchpad 的机制与数字 (Hookr/Pons/Long/Hookdaq / Solana 集群); Pons 30d 费用 \$137M 与第三方 \$97.1M 的冲突未解决; Hookr 116 发行 vs 51 发行/12 毕业 vs 「45 天无新币」的口径矛盾未调和; Robinhood Chain 收入量级相差 100 倍的矛盾; EDMA/Prism 的「有真实发行方」无法独立证实 (Prism 自认 demo); Dokimo/Reclaim/zkPass/Primus/DIA/Zolvency 的机制为官方自述; Hookdaq 域名 10/06 解析失败。

未验证 (不能当事实用): 真实项目方与买家的付费意愿 (没有一手用户访谈, AF4 已指出「零一手研究」); Stripe 真实商业密钥的出证、Apple ASC 的 gzip 行为 (无开发者账号)、heliosgen 站的 zkTLS 端到端、独立 notary 的商业安排、聚合可验证的生产落地、zkVerify 上链; 证券属性与 BUSL 的法律结论 (需律师); 演示站之外的真实用户/交易数据。

方法与口径边界: J 节的行号基于 2026-10-19 12:30 的演示站文件, 改完以后以 J.3 的 grep 断言为准; 竞品排查「未找到 ≠ 不存在」(仅覆盖 205 条推文 + 公开网络; 第 206–223 行未读); 本平台所有数字只认《基线 v2》§8, 旧口径 (\$100K/\$350K、5%/10% 押金、团队份额/vesting、平台币、5% 交易费) 一律**已废弃**, 本文若出现仅为标注冲突; 对外表述统一为「指定验证方出证 · 任何人可复核」, 不用「任何人可验证 / 零信任 / 数学保证一切」。

本附录的用途是让决策者相信三件事: 方向有证据、技术有实测、风险有清单。它不替代尽职调查, 也不把「未验证」包装成「已验证」。