研究报告 · 2026 年 11 月

算力即共识

AI × Crypto × 芯片全景研究（2026），从 Pearl 谈起

Pearl · 有用工作量 · DePIN 与智能体 · ASIC 经济学 · 工艺节点 · 分阶段预算

谭帅

tanshuai.com · i@tanshuai.com



定理成立，激励未成立

01 Pearl 在工程上可行，但工作尚未“有用”

约 90 EH/s 的整数矩阵乘法保护着这条链，但只有约 1% 的区块承载真实 AI 工作。

02 付费需求在推理、数据与隐私

Bittensor 可验证收入年化约 7,000 万美元，Grass 2026 年上半年 1,700 万美元，TEE 已投产；Agent 支付每月约 5,000–11,000 美元。

03 ASIC 只在盘子大、规则稳、有第二市场时才值得做

其利润上限为 R × (1 − 1/k)。今天没有任何网络三者兼具 笔者分析 。

≈90 EH/s

2026 年 11 月 13 日的 Pearl：约合 12.2 万张 H100 的整数算力

≈1%

的 Pearl 区块承载真实 AI 工作（Blockworks）

4–11×

Bittensor 排放相对其可验证收入的倍数

AI × Crypto 六条赛道：付费需求真实在哪里

有用工作量类链 01

真实但小

≈7,000 万美元/年

Bittensor 可验证外部收入

信号： 排放为收入 4–11×；Pearl ≈1% AI 区块

机制可行；“有用”需要付费方

去中心化算力 02

真实但小

235 万美元/年

Render 链上费用，可验证者中最大

信号： 市值 ≈ 费用的 360×

以商品化推理转售为主

训练与推理 03

利润归股权

1 亿美元+/年

Prime Intellect，用中心化 GPU 的股权公司

信号： Gensyn 训练主网未上线

进步真实；利润归股权

可验证 AI 04

尚早

398

Phala TEE 云的付费用户，2025 年底

信号： zkML 未披露付费使用

TEE 已投产；zkML 尚早

Agent 支付 05

需求未至

0.5–1.1 万美元/月

真正由智能体发起的 x402 支付

信号： ≈2 亿笔交易，多为信号

通道先行，需求未至

数据网络 06

有真实买家

1,700 万美元

Grass 数据收入，2026 年上半年（自报）

信号： 市值 ≈ 年化收入的 10×

少数有真实买家的赛道之一

> 补贴是冷启动的燃料，不是商业模式。加密负责分发与结算，股权收走利润，至少在 2026 年如此。

一次乘加就是一个哈希

从定理到主网

Komargodski 与 Weinstein（2025 年 4 月）：为任意矩阵乘积构造有用工作量证明，开销 1 + o(1)。Pearl 主网于 2026 年 4 月 27 日启动。

工作原理

矿工计算带噪矩阵乘法，把每个分块的累加器哈希成彩票，并用 60 KB 以内的 Plonky2 证明打开中奖分块。

计量单位

1 H 即一次被记账的 INT7 × INT7 → INT32 乘加：区块链的安全预算以张量吞吐计价。

2026 年 11 月 13 日的 Pearl

89.77 EH/s

全网算力（独立全节点）

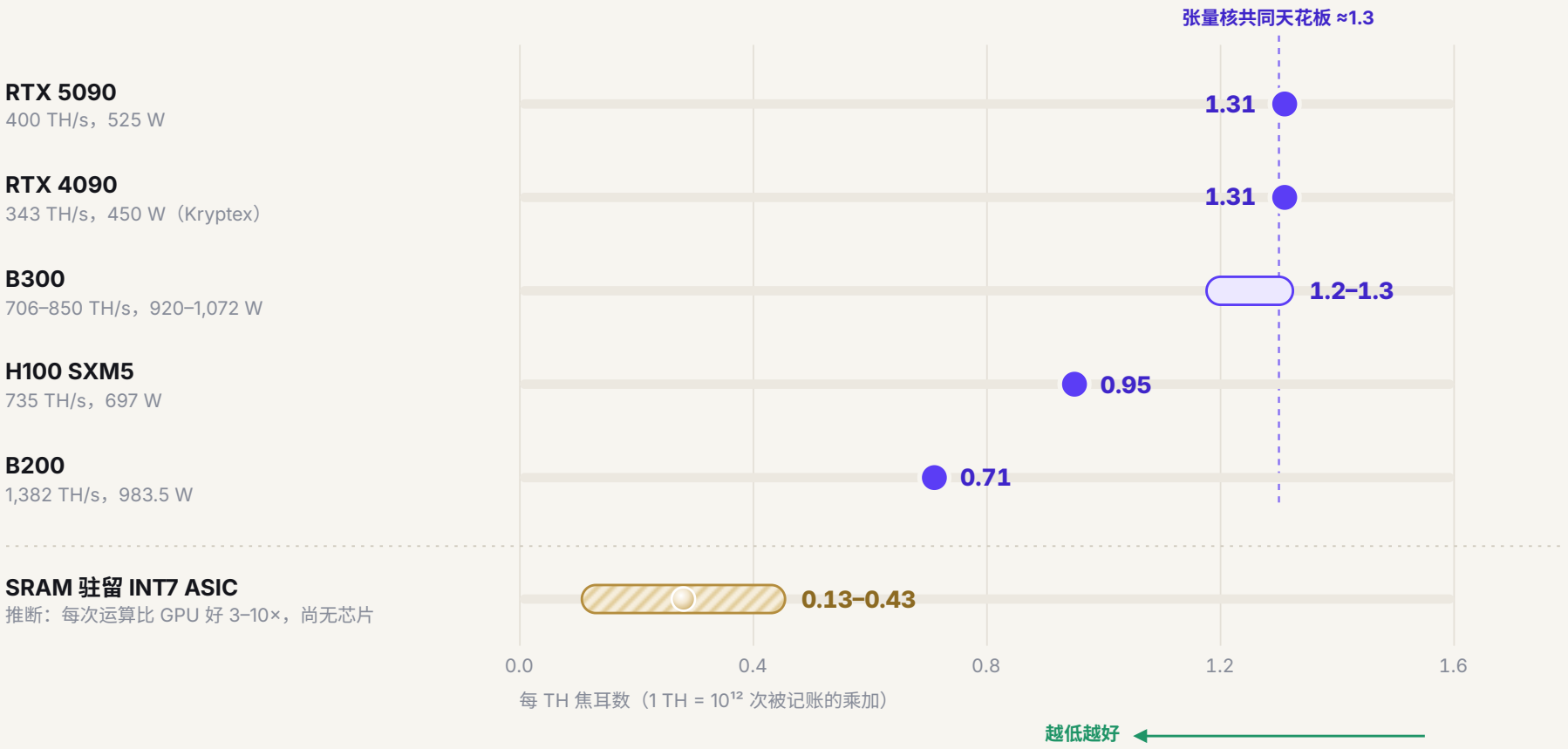
≈5 亿美元

市值；完全稀释估值约 28 亿美元

+78%

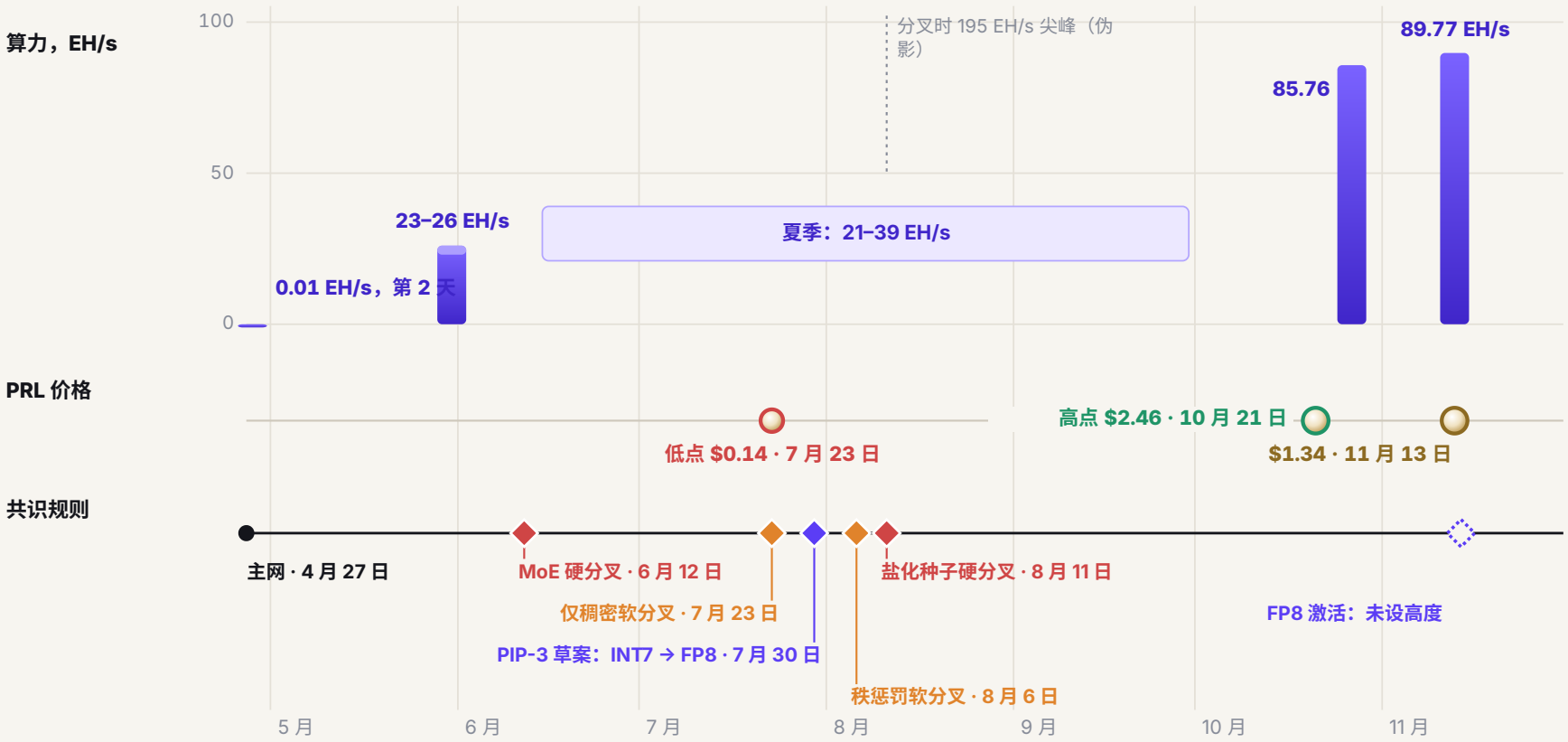
未来 12 个月的新增供应

在 Pearl 的整数工作上，GPU 共享一道能效天花板



游戏卡与 B300 都在约 1.3 J/TH，即便 B200 也只有 0.71。一颗只从 SRAM 读取 7 位整数做乘法的芯片，原理上或可好 3–10 倍 笔者分析。

算力追随币价，规则不断变化



前六天挖出约 1.2 亿枚，占今日供应的 32%。一张 RTX 5090 现在每天约赚 5–6 美元；纯为挖矿租卡会亏钱。

定理成立，激励未成立

有用工作的成本

推理侧：开销很小

Pearl 自报 4 张 H200 运行 Llama 70B 时间增加 5.08%；独立测试在单张 Hopper GPU 上测得吞吐下降 9.2%。

有用工作的收益

挖矿侧：算力太少

在线推理的卡，预填充时约为专用矿卡的 27%，对话负载下 5.4%，解码主导时约 1%。

所以理性矿工去算随机矩阵。“有用”是一个链下的商业问题：必须有人为推理付费。

两个月四次分叉，下一步是 FP8

6 月 12 日
混合专家硬分叉（区块 71,935）

7 月 23 日
仅稠密软分叉（区块 91,630）

8 月 6 日
秩惩罚软分叉：部分配置损失 50–87.5% 的有效算力

8 月 11 日
盐化种子硬分叉：旧矿工只能产出无效份额

未定
PIP-3：INT7 改为 FP8，只准入 Hopper 与 Blackwell

三取二

对 AI 有用、逐位可验证、硬件中立：数值格式最多得其二

13 位

Hopper FP8 累加保留的小数位，且截断：跨代不可复现

≈82%

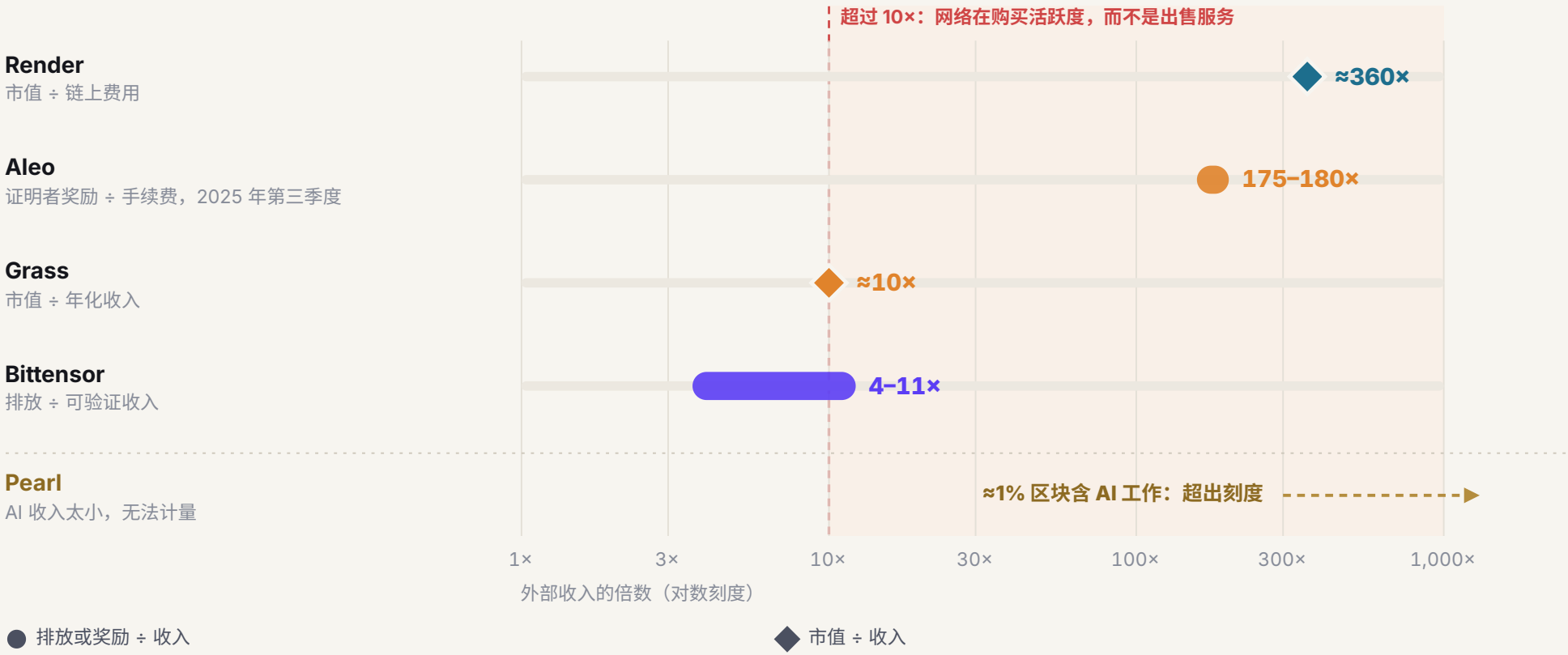
的算力来自 PIP-3 不准入的消费级显卡（低置信度模型）

谁控制工作函数，谁就控制硬件投资者的命运 笔者分析。

矩阵与零知识都挡不住 ASIC

网络	发生了什么	启示
Kaspa	哈希之间夹 64 × 64 矩阵乘积；16 个月后出 ASIC，能效约为 GPU 的 1,000×；最好的机器如今每天赚 0.86 美元	矩阵既不等于有用，也不等于抗 ASIC
Aleo	合成 SNARK 谜题；五个月后出专用机；证明者奖励为手续费的 175–180×	合成工作靠补贴运转
Qubic	宣称训练 AI；其算力挖过门罗币（宣称 51%），如今挖狗狗币	通用 PoW 可被外部收编
Bittensor	质押加权打分；可验证收入年化约 7,000 万美元，排放逾 3 亿美元	唯一有规模外部收入者
门罗币、Sia、以太坊	分叉让 ASIC 变砖；合并后不到 20% 的矿工找到新工作	有第二市场的硬件才能活下来

补贴倍数是最诚实的体检指标



超过外部收入约 10 倍，网络就是在购买活跃度，而不是出售服务。Pearl 的 AI 收入太小，无法放上刻度。

需求真实但很小，价值流向股权

- **算力市场**

  Render 链上费用每年约 235 万美元；Akash 的 H100 每小时 2.73 美元，比 AWS 和 Google 便宜，但不及 Vast.ai 或 RunPod。

- **训练**

  互联网上已训练 80–400 亿参数模型；INTELLECT-3 回到了 InfiniBand 互连的 512 张 H200。

- **可验证 AI**

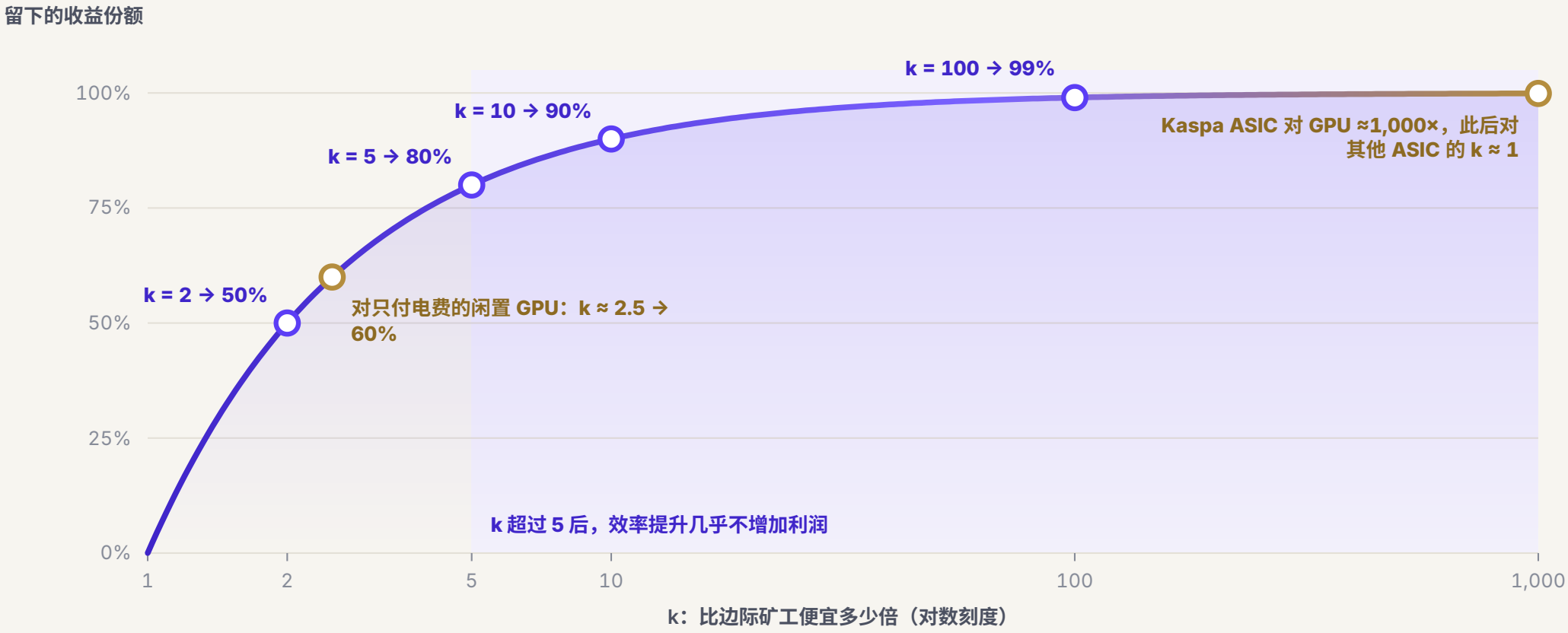
  TEE 开销低于 7%，已投产；TEE.fail 用 1,000 美元的插入器攻破证明；zkML 证明 GPT-2 每分钟 174 个 token。

- **智能体与数据**

  x402 中智能体发起的流量每月约 5,000–11,000 美元；Grass 2026 年上半年数据收入 1,700 万美元。

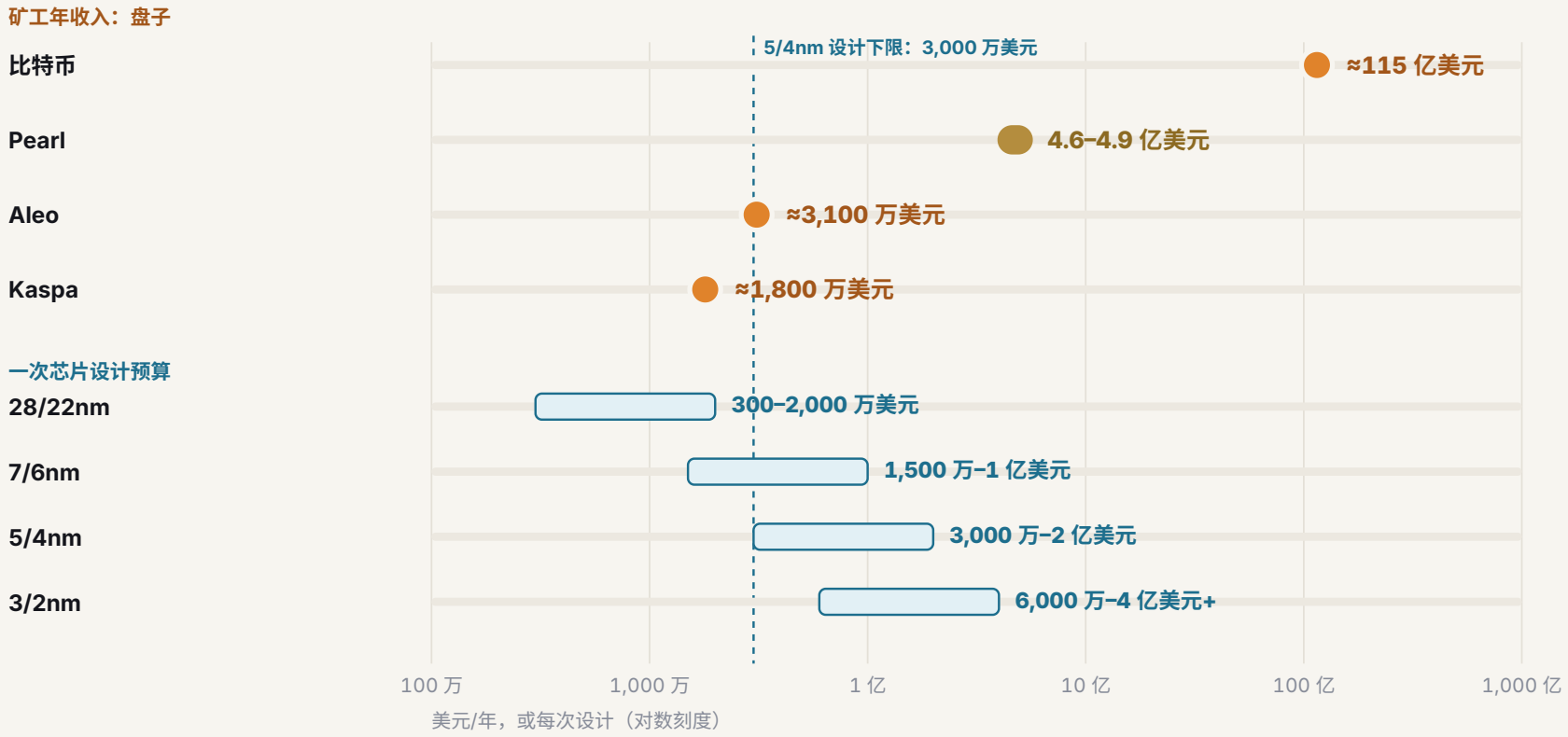
> **四家用中心化基础设施的股权公司估值约 85 亿美元，大致相当于协议层与应用层 AI 代币的总和。**

为什么 k 超过 5 之后效率不再值钱



利润上限 ≈ R × (1 − 1/k)。一旦 ASIC 成为边际矿工，k 就要相对其他 ASIC 重新计算；对只付电费的闲置 GPU，k 约为 2.5 笔者测算 。

多数盘子比一次芯片设计预算还小



回本算力 h* = NRE ÷ [R × (1 − 1/k) × T × p]。Pearl 按 NRE 2,000 万美元、k = 5 计：规则不变时需全年约 4.9 EH/s，规则维持概率五五开时需 9.8 EH/s 笔者测算。

五类芯片，五个答案



Pearl 类 PoUW 矿机芯片

暂不做

k： 无 HBM、无通用单元：每次运算 3–10×（推断）

第二市场： AI 推理（若做通用 INT8/FP8 GEMM）

押注推理优先、可挖矿的芯片，而非专用 INT7



比特币 SHA-256 矿机芯片

不进入

k： 相对在位者 ≤1

第二市场： 几乎没有

只做自带电力、细分形态或 IP



AI 训练芯片

做 IP，不做芯片

k： 同精度下 1.1–1.8×

第二市场： —

封装与 HBM 决定成败；做 IP、chiplet、服务



AI 推理芯片

值得做

k： 放弃通用性：宣称 10–20×

第二市场： 自身即主市场

先签客户，再选锁定程度



ZK 证明加速器

观望对冲

k： 宣称为 GPU 的 10–100×

第二市场： ZK 之外有限

可编程 MSM 与 NTT 引擎；先 FPGA



FHE 加速器

早布局

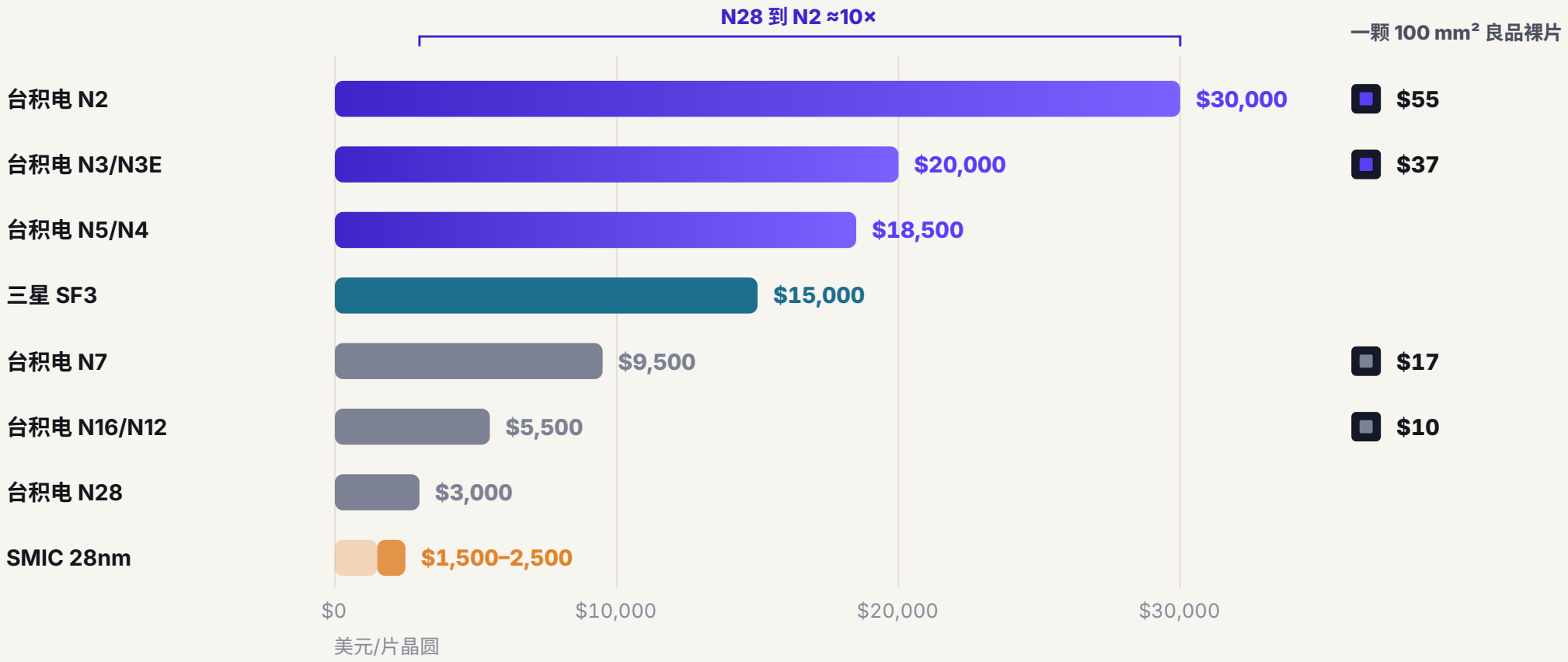
k： 对至强 1,074–5,547×（Heracles）

第二市场： 加密计算、隐私 AI

2027–2029 窗口；轻资产验证

今天没有任何网络同时具备大盘子、稳规则和大于 1 的 k：比特币的 k 归在位者，Pearl 的规则最不稳，Kaspa 与 Aleo 的盘子太小。

领先节点晶圆的价格是成熟节点的十倍



让终生成本最大项来选：全天候算力芯片看能耗，训练芯片看封装与 HBM（占 H100 成本的 63%），推理芯片看 SRAM 还是 HBM。

每类芯片、每种团队各有其节点

芯片	小团队	规模化公司	中国内地路径
PoUW 矿机芯片	28nm 或 16/12nm MPW；首批量产 N7/N6	N3/N3E 或三星 SF3	SMIC N+1/N+2 可行，每颗裸片成本约高 40–50%
SHA-256 矿机芯片	不追前沿	3nm 级	能效难以对标领先节点
AI 训练芯片	IP、chiplet、设计服务	N3P 再到 N2/A16，配 CoWoS 与 HBM	SMIC N+2/N+3 配国产 HBM
AI 推理芯片	SRAM 为中心，N6/N7 或 N4/N5/SF4	N3/N2 配 HBM，或 SRAM chiplet	SMIC N+2 配 LPDDR 或 GDDR
ZK 与 FHE 加速器	先 FPGA 或 16/12nm MPW	N5/N3；FHE 配 HBM	ZK 可行；FHE 受限于 HBM

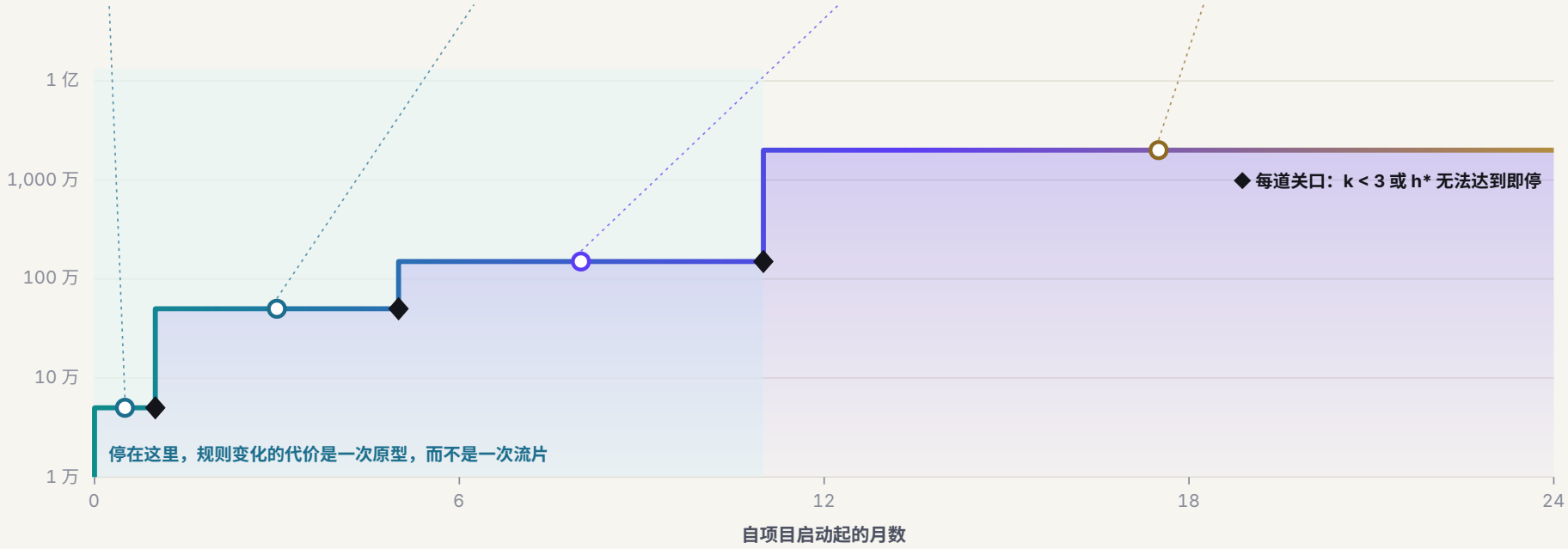
先买证据，再买掩模

关口 0 · 模型
≈5 万美元 · 数周
依据算术单元、SRAM 与 I/O 估算 J/op 与 $/op

关口 1 · FPGA
≈50 万美元 · 数月
端到端运行真实负载：份额或 token

关口 2 · MPW
≈150 万美元 · 第 11 个月
实测硅片取代模型

关口 3 · 掩模与首批量产
≈2,000 万美元 · 第 24 个月
N7 掩模 ≈350 万美元，处在 1,500 万–1 亿美元的设计预算内



模型、FPGA 与 MPW 约 150 万美元、十一个月即可拿到实测硅片；掩模组与首批量产的花费是其十倍以上。在买家或协议版本确定之前，停在掩模之前。

以 Crypto 为第一个客户，以 AI 为第二市场

定制芯片

- 需求压倒性来自 AI：博通 2026 财年 AI 半导体收入约 580 亿美元
- 矿机芯片能力可迁移：低压阵列、千瓦级供电、快速流片
- 靠独立的市场进入路径取胜，而非挖矿渠道

AI 开发

- 工时已商品化：Clutch 上每小时 25–49 美元
- 价值在结合部：为定制芯片写算子，把挖矿嵌进推理服务
- 可验证推理：TEE 加 ZK 抽检

AI × Crypto 系统

- 分层验证：TEE 或抽样，再加争议博弈或 ZK 抽检
- 门槛是分发与流动性，而不是成本
- 先签算力买家，再发币

三条路，各有一个小的第一步

路径	第一步
A. 推理优先、可挖矿的加速器	用四周对比 SRAM 驻留 INT8/FP8 阵列与 RTX 5090、H100 的 J/op 与 $/op，再做 FPGA 或成熟节点 MPW
B. 定制芯片服务：Crypto 优先，AI 其次	把本报告的 NRE 与盈亏平衡模型做成付费可行性研究，按里程碑付款、以固定协议版本验收
C. 先有买家、再有代币的 AI 原生网络	与一家具名的推理买家共同撰写设计说明，涵盖分层验证与厂商中立的规范算术

> **最多三条路，每条都在投入资金之前先行检验** 笔者分析 。

值得关注的信号，与该问的问题

观察信号	
随时	Pearl 的 FP8 激活高度，以及链是否分裂
每月	Pearl 承载 AI 工作的区块占比
每季度	Bittensor 可验证收入相对排放；x402 中智能体发起的流量
2027 年 1 月	据报台积电 2nm 与 3nm 涨价 3–6%
2027 年第一季度	Pearl 引入 FP4（据创始人 AMA 的报道）
2028 年 4 月	比特币下一次减半

该问的问题

01 谁控制工作函数？

02 补贴倍数是多少？

03 下一道关口要花多少钱，什么会让你停下？

04 回本算力是多少，p 取多少？

05 芯片的第二市场是什么？

06 第一个付费客户是谁，叫什么名字？

这些是我们可以通过技术交流与技术合作共同探索的方向：定制芯片、AI 研发与 AI × Crypto 系统。

i@tanshuai.com · tanshuai.com