研究筆記 · 2026 年 11 月

算力即共識

2026 年的 AI × 加密貨幣 × 晶片，從 Pearl 談起

Pearl · 有用工作 · DePIN 與 Agent · ASIC 經濟學 · 製程節點 · 分階段預算

譚帥

tanshuai.com · i@tanshuai.com



結論

定理成立，激勵不成立

01 Pearl 在工程上可行，但還不是有用工作

約 90 EH/s 的整數矩陣乘法保護著這條鏈，但只有約 1% 的區塊承載真實 AI 工作。

02 付費需求在推論、資料與隱私

Bittensor 每年約 7,000 萬美元可驗證收入，Grass 2026 年上半年 1,700 萬美元，TEE 已上線生產；Agent 支付每月約 5,000–11,000 美元。

03 ASIC 只在盤子大、規則穩、有第二市場時才划算

其利潤上限為 R × (1 − 1/k)。目前沒有任何網路三者兼具 分析 。

≈90 EH/s

Pearl（2026 年 11 月 13 日）：約相當於 12.2 萬張 H100 的整數吞吐量

≈1%

的 Pearl 區塊承載真實 AI 工作（Blockworks）

4–11×

Bittensor 排放與其可驗證收入之比

AI × 加密貨幣六大領域：哪裡有真實付費需求

有用工作鏈 01

真實但小

≈每年 7,000 萬美元

Bittensor 可驗證的外部收入

訊號： 排放為收入 4–11 倍；Pearl AI 區塊 ≈1%

機制可行；有用性需要付費者

去中心化算力 02

真實但小

每年 235 萬美元

Render 鏈上手續費，可驗證者中最大

訊號： 市值 ≈ 手續費 360 倍

多半是轉售一般推論

訓練與推論 03

利潤歸股權

每年 1 億美元以上

Prime Intellect，股權公司，用中心化 GPU

訊號： Gensyn 訓練主網未上線

進展真實；利潤歸股權

可驗證 AI 04

早期

398

Phala TEE 雲端付費用戶，2025 年底

訊號： 無已披露的付費 zkML

TEE 已上線生產；zkML 尚早

Agent 支付 05

需求未到

每月 5,000–11,000 美元

真正由 Agent 發起的 x402 支付

訊號： ≈2 億筆交易，多為訊號性質

通道先建好了，需求還沒來

資料網路 06

真實買家

1,700 萬美元

Grass 2026 年上半年資料收入（自報）

訊號： 市值 ≈ 年化收入 10 倍

少數有真實買家的領域之一

補貼是冷啟動的燃料，不是商業模式。加密貨幣負責分發與結算；利潤歸股權，至少 2026 年是如此。

一次乘加就是一次雜湊

從定理到主網

Komargodski 與 Weinstein（2025 年 4 月）：任意矩陣乘積的有用工作量證明，額外開銷為 1 + o(1)。Pearl 主網於 2026 年 4 月 27 日上線。

運作方式

礦工對加噪矩陣做乘法，把每個 tile 的累加器雜湊成一張彩券，並以小於 60 KB 的 Plonky2 證明證實中獎的 tile。

單位

1 H 是一次計入的 INT7 × INT7 → INT32 乘加：以張量吞吐量計價的區塊鏈安全預算。

Pearl，2026 年 11 月 13 日

89.77 EH/s

全網算力（獨立全節點）

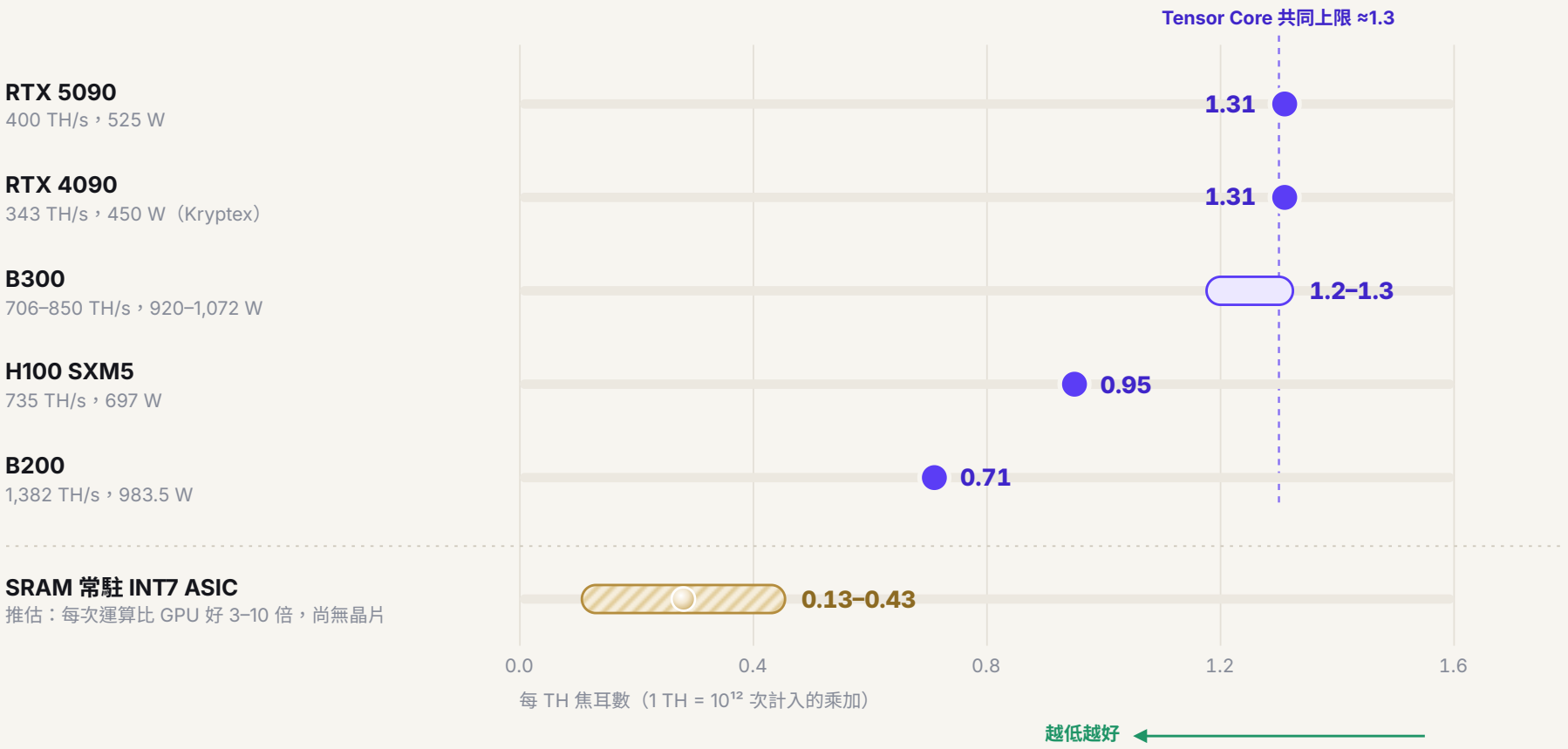
≈5 億美元

市值；完全稀釋約 28 億美元

+78%

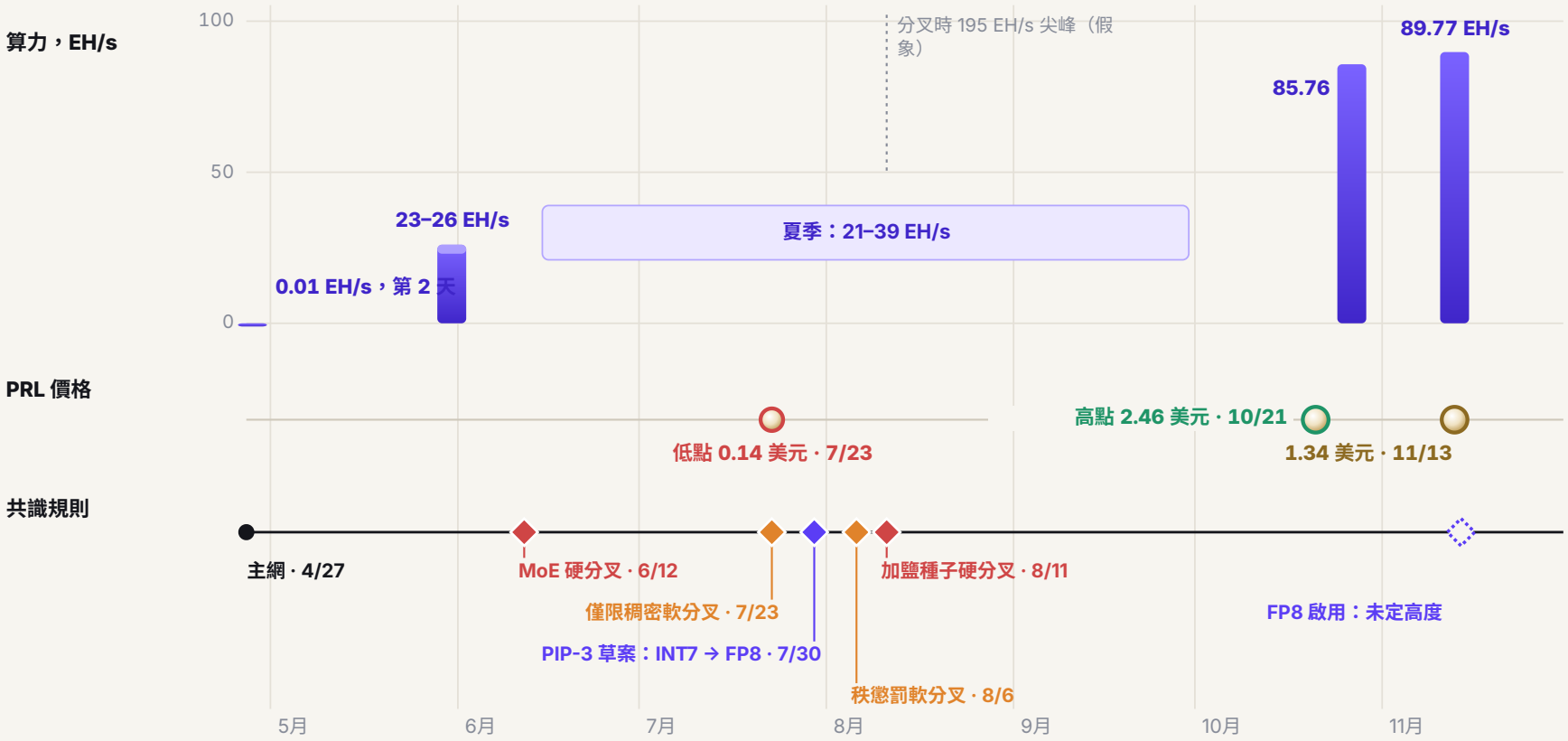
未來 12 個月的新增供給

在 Pearl 的整數工作上，GPU 共享同一能耗上限



遊戲顯示卡與 B300 都落在約 1.3 J/TH；連 B200 也只到 0.71。一顆只從 SRAM 讀取、只做 7 位元整數乘法的晶片，有理由好上 3–10 倍 分析 。

算力跟著價格走，規則一改再改



前六天挖出約 1.2 億枚幣，占目前供給的 32%。一張 RTX 5090 現在每天約賺 5–6 美元；只為挖礦而租卡是虧錢的。

定理成立，激勵不成立

有用工作的成本

推論端：開銷很小

Pearl 公布在四張 H200 上跑 Llama 70B 多花 5.08% 時間；一項獨立測試在單張 Hopper GPU 上測得吞吐量少 9.2%。

有用工作的收益

挖礦端：算力太少

一張提供推論服務的卡，挖礦算力在 prefill 時約為專用礦卡的 27%，聊天時 5.4%，以 decode 為主時約 1%。

所以理性的礦工會去乘隨機矩陣。有用性是鏈下的商業問題：總得有人為推論付錢。

兩個月四次分叉，接下來是 FP8

6 月 12 日
混合專家（MoE）硬分叉（區塊 71,935）

7 月 23 日
僅限稠密軟分叉（區塊 91,630）

8 月 6 日
秩懲罰軟分叉：部分配置損失 50–87.5% 有效算力

8 月 11 日
加鹽種子硬分叉：舊礦機只產生無效 share

未定
PIP-3：INT7 改為 FP8，只接納 Hopper 與 Blackwell

3 取 2

對 AI 有用、逐位元可驗證、硬體中立：一種數字格式最多只能兼顧兩項

13 位元

Hopper 的 FP8 累加所保留的位數，且有截斷：跨世代無法重現

≈82%

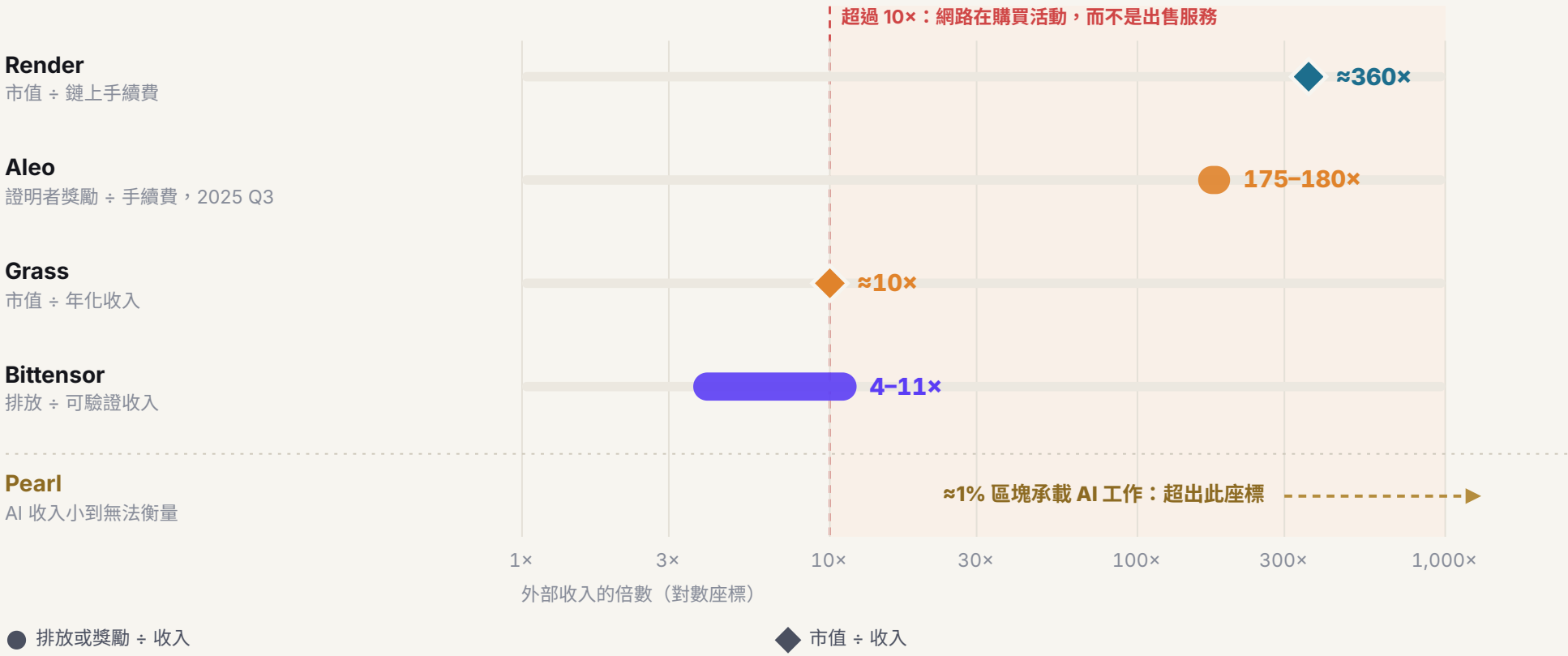
的算力在 PIP-3 不接納的消費級顯示卡上（低信心模型）

誰控制工作函數，誰就掌握硬體投資者的命運 分析 。

矩陣和零知識都擋不住 ASIC

網路	發生了什麼	學到什麼
Kaspa	在雜湊之間做 64 × 64 矩陣乘積；16 個月後出現 ASIC，效率約為 GPU 的 1,000 倍；最好的機型現在每天賺 0.86 美元	矩陣既不有用，也擋不住 ASIC
Aleo	合成的 SNARK 謎題；五個月後出現專用機；證明者獎勵為手續費的 175–180 倍	合成工作靠補貼運轉
Qubic	宣稱做 AI 訓練；其算力挖了 Monero（宣稱 51%），現在挖 Dogecoin	通用 PoW 可能被外部劫持
Bittensor	以質押加權評分；每年約 7,000 萬美元可驗證收入，對比逾 3 億美元排放	唯一有規模化外部收入者
Monero、Sia、Ethereum	分叉讓 ASIC 變磚；合併後不到 20% 的礦工找到新工作	有第二市場的硬體才活得下來

補貼倍數是最誠實的健康檢查



超過外部收入約 10 倍時，網路是在購買活動，而不是出售服務。Pearl 的 AI 收入小到無法放上座標。

真實但不大的需求，價值移向股權

- **算力市場**

  Render 鏈上手續費每年約 235 萬美元；Akash 的 H100 每小時 2.73 美元，比 AWS 和 Google 便宜，但不如 Vast.ai 或 RunPod。

- **訓練**

  透過網際網路訓練了 80–400 億參數的模型；INTELLECT-3 回到 InfiniBand 上的 512 張 H200。

- **可驗證 AI**

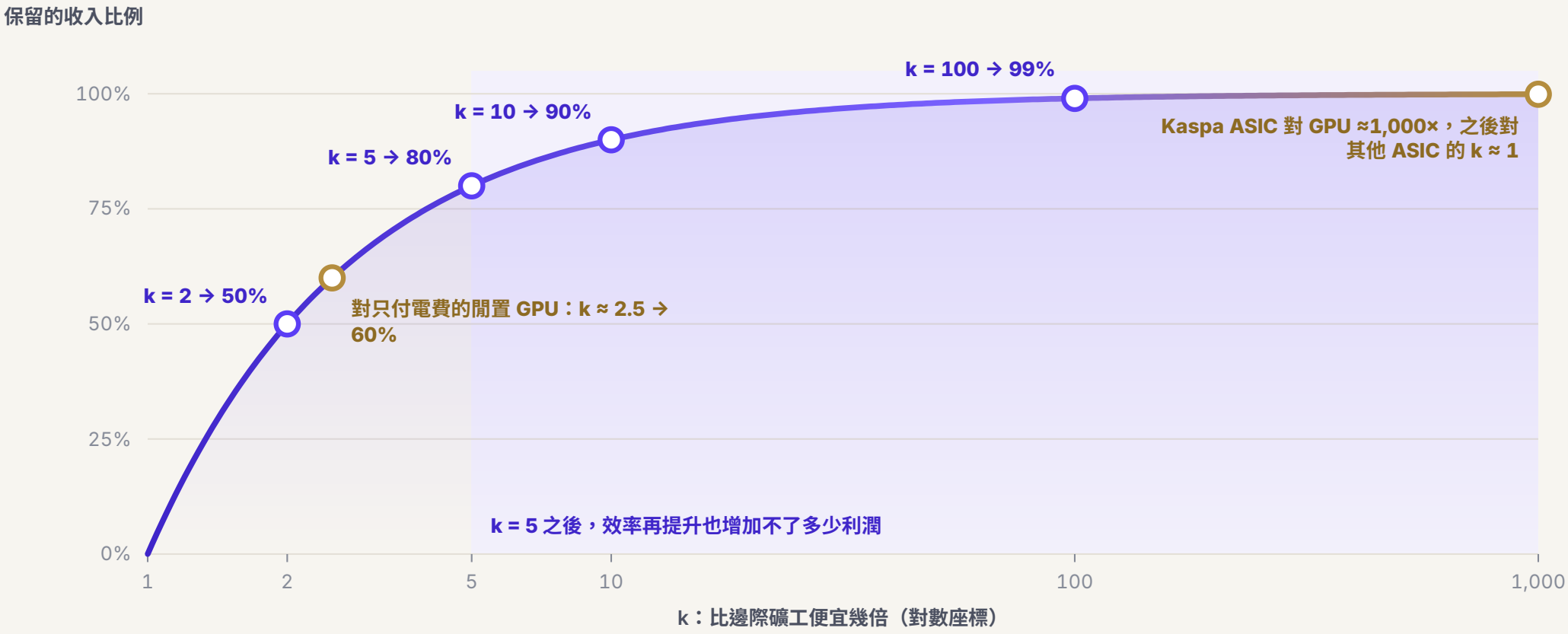
  TEE 開銷低於 7%，已上線生產；TEE.fail 用 1,000 美元的中介器攻破遠端證明；zkML 證明 GPT-2 每分鐘 174 個 token。

- **Agent 與資料**

  x402 由 Agent 發起的流量每月約 5,000–11,000 美元；Grass 2026 年上半年資料收入 1,700 萬美元。

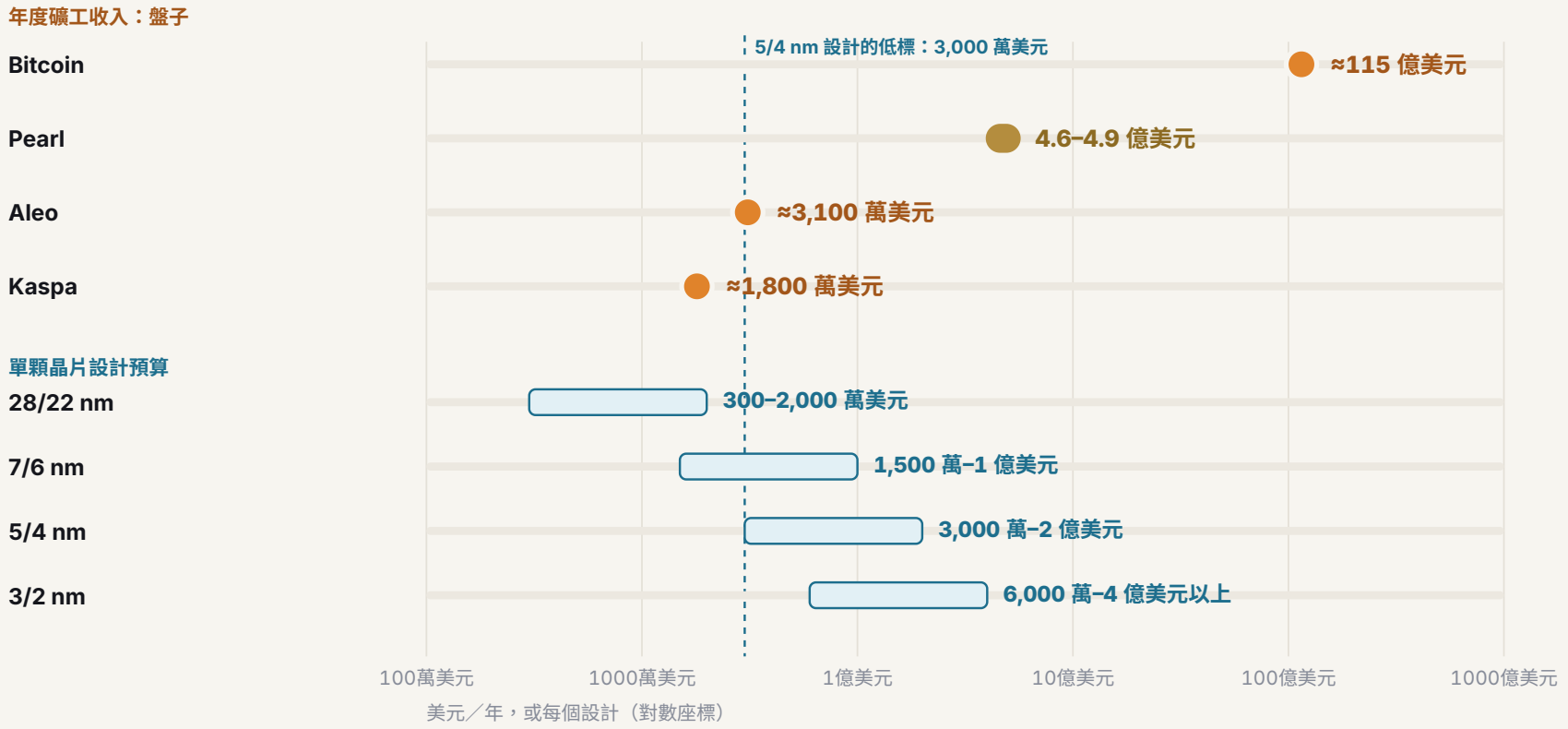
> **四家建在中心化基礎設施上的股權公司價值約 85 億美元，大約等於所有協議層與應用層 AI 代幣的總和。**

為何 k = 5 之後效率就不再帶來利潤



利潤上限 ≈ R × (1 − 1/k)。一旦 ASIC 自己成為邊際礦工，k 就改以其他 ASIC 為基準重算；對只付電費的閒置 GPU，k 約為 2.5 估算。

多數盤子比不上一顆晶片的設計預算



回本算力 h* = NRE ÷ [R × (1 − 1/k) × T × p]。Pearl 在 NRE 2,000 萬美元、k = 5 時：規則維持一年需約 4.9 EH/s，規則維持機率僅五成時需 9.8 EH/s 估算。

逐類看晶片

五類晶片，五種答案



Pearl 類 PoUW 礦機晶片

現在不做

k： 無 HBM、無通用單元：每次運算 3–10×（推估）

第二市場： AI 推論，若為通用 INT8/FP8 GEMM

押注能挖礦的推論優先晶片，而非專用 INT7 晶片



Bitcoin SHA-256 礦機晶片

別進場

k： 對既有業者 ≤1

第二市場： 幾乎沒有

只在自有電力、利基形態或做 IP 時可行



AI 訓練晶片

做 IP，不做晶片

k： 同精度下 1.1–1.8×

第二市場： —

封裝與 HBM 決定成敗；做 IP、chiplet、服務



AI 推論晶片

做

k： 放棄通用性：宣稱 10–20×

第二市場： 它就是主要市場

先簽下客戶，再選擇鎖定



ZK 證明加速器

觀望避險

k： 宣稱為 GPU 的 10–100×

第二市場： ZK 以外有限

可程式化 MSM 與 NTT 引擎；先上 FPGA



FHE 加速器

提早布局

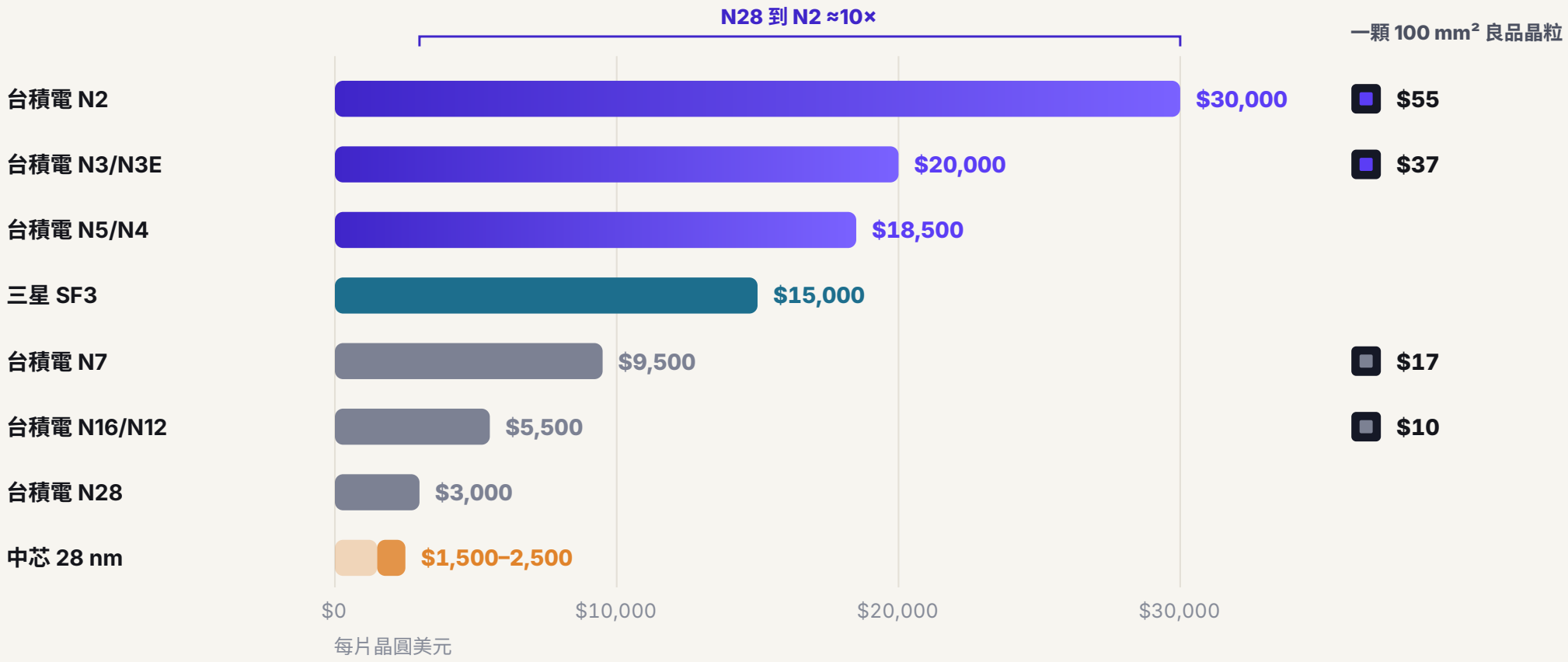
k： Xeon 的 1,074–5,547×（Heracles）

第二市場： 加密運算、隱私 AI

2027–2029 年的窗口；以輕資產驗證

目前沒有網路同時具備大盤子、穩定規則與大於 1 的 k：Bitcoin 的 k 屬於既有業者，Pearl 的規則最不穩定，Kaspa 與 Aleo 的盤子太小。

一片先進製程晶圓的價格是成熟製程的十倍



讓終生成本中最大的一項來做選擇：全天候運算晶片看能耗，訓練晶片看封裝與 HBM（占 H100 成本 63%），推論晶片看 SRAM 還是 HBM。

每類晶片、每種團隊各有其節點

晶片	小團隊	規模化公司	中國大陸路徑
PoUW 礦機晶片	28 或 16/12 nm MPW；首批量產 N7/N6	N3/N3E 或三星 SF3	中芯 N+1/N+2 可行，每顆晶粒貴約 40–50%
SHA-256 礦機晶片	別追最先進製程	3 nm 級	難以匹敵先進節點的效率
AI 訓練晶片	IP、chiplet、設計服務	N3P 再到 N2/A16，搭配 CoWoS 與 HBM	中芯 N+2/N+3 搭配國產 HBM
AI 推論晶片	以 SRAM 為核心，N6/N7 或 N4/N5/SF4	N3/N2 搭配 HBM，或 SRAM chiplet	中芯 N+2 搭配 LPDDR 或 GDDR
ZK 與 FHE 加速器	先 FPGA 或 16/12 nm MPW	N5/N3；FHE 搭配 HBM	ZK 可行；FHE 受限於 HBM

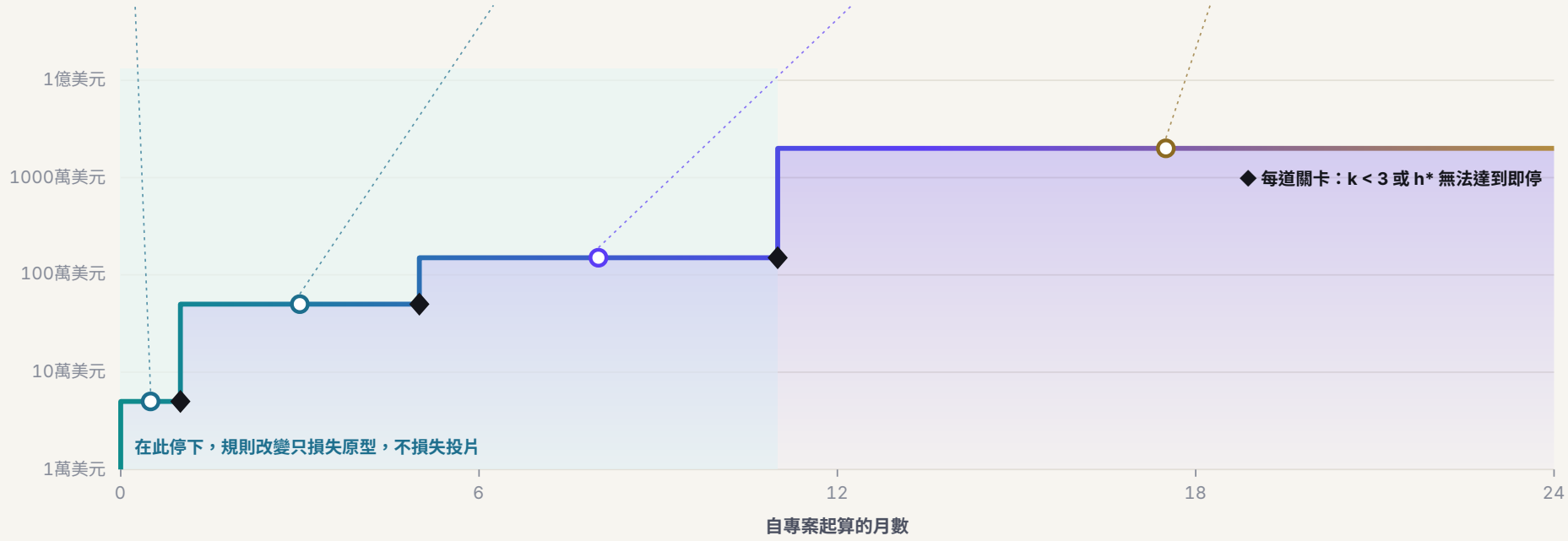
先買證據，再買光罩

關卡 0 · 模型
≈5 萬美元 · 數週
依算術、SRAM 與 I/O 估算 J/op 與 $/op

關卡 1 · FPGA
≈50 萬美元 · 數月
端到端跑真實工作負載：share 或 token

關卡 2 · MPW
≈150 萬美元 · 第 11 個月
實測的矽取代模型

關卡 3 · 光罩與首批量產
≈2,000 萬美元 · 第 24 個月
N7 光罩 ≈350 萬美元，設計預算 1,500 萬–1 億美元



模型、FPGA 與 MPW 約 150 萬美元、十一個月就能拿到實測的矽；光罩組與首批量產的花費是其十倍以上。在買家或協議版本確定之前，先別買光罩。

加密貨幣是第一個客戶，AI 是第二市場

客製化晶片

- 需求壓倒性來自 AI：博通 2026 財年 AI 半導體約 580 億美元
- 礦機晶片能力可移轉：低壓陣列、千瓦級供電、快速投片
- 靠獨立的市場通路取勝，而非挖礦通路

AI 開發

- 工時是大宗商品：Clutch 上每小時 25–49 美元
- 價值在接縫處：客製化晶片的 kernel、在推論服務中挖礦
- 可驗證推論：TEE 加 ZK 抽查

AI × 加密貨幣系統

- 分層驗證：TEE 或抽樣，再加爭議機制或 ZK 抽查
- 門檻是分發與流動性，不是成本
- 先簽下算力買家，再發代幣

三條路徑，各有一小步起點

路徑	第一步
A. 推論優先、也能挖礦的加速器	用四週研究 SRAM 常駐 INT8/FP8 陣列對比 RTX 5090 與 H100 的 J/op 與 $/op，再上 FPGA 或成熟節點 MPW
B. 客製化晶片服務：先加密貨幣，後 AI	把本報告的 NRE 與損益平衡模型，變成有里程碑、鎖定協議版本的付費可行性研究
C. 先有買家、後有代幣的 AI 原生網路	與一位具名的推論買家共同撰寫一份設計說明，內容為分層驗證與廠商中立的標準算術

> **最多三條路徑，每條都在投入資金前先驗證** 分析 。

觀察重點與該問的問題

觀察指標

隨時	Pearl 的 FP8 啟用高度，以及鏈是否分裂
每月	Pearl 承載 AI 工作的區塊比例
每季	Bittensor 可驗證收入對比排放；由 Agent 發起的 x402 流量
2027 年 1 月	據報台積電 2 nm 與 3 nm 漲價 3–6%
2027 Q1	Pearl 導入 FP4（據創辦人 AMA 報導）
2028 年 4 月	Bitcoin 的下一次減半

該問的問題

01 誰控制工作函數？

02 補貼倍數是多少？

03 下一道關卡要花多少？什麼會讓你停下？

04 回本算力是多少，p 是多少？

05 這顆晶片的第二市場是什麼？

06 第一個付費客戶是誰？請說出名字。

以下是我們可以透過技術交流與技術合作一同探索的領域：客製化晶片、AI 開發，以及 AI × 加密貨幣系統。

i@tanshuai.com · tanshuai.com