研究筆記 · 公開版

2026 · 11



有用工作量證明 · 加密貨幣 × 矽

算力即共識

2026 年的 AI × 加密貨幣 × 晶片，從 Pearl 的有用工作量證明談起

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

> **結論**
>
> **Pearl 證明了矩陣乘法可以保護一條區塊鏈，但還沒證明這份工作有用。綜觀 AI × 加密貨幣，付費需求集中在推論、資料與隱私；而 ASIC 只在盤子夠大、規則穩定、晶片有第二市場時才划算。**

譚帥

技術人與創業者 · AI 研發者

tanshuai.com · i@tanshuai.com

資料截至 2026 年 11 月 13 日

金額單位：美元

目錄

目錄



◆ **摘要** 04
定理成立，激勵不成立

01 **範圍與方法** 06
範圍、方法與四項檢驗

02 **Pearl · 機制** 07
Pearl：以矩陣乘法作為共識

03 **Pearl · 經濟** 09
Pearl：規模、排放與有用性落差

04 **Pearl · 規則** 11
Pearl：規則風險、數值與治理

05 **有用工作鏈** 12
有用工作鏈：矩陣和零知識都擋不住 ASIC

06 **更廣的版圖** 14
AI × 加密貨幣的其餘部分：真實但不大的需求，價值移向股權

07 **ASIC 經濟學** 16
ASIC 問題：一條公式，三把尺

08 **逐類看晶片** 18
五類晶片，五種答案

09 **製程節點** 21
製程節點：讓最大的終生成本來選擇

10 **分階段預算** 24
從模型到矽：第一顆晶片的分階段預算

11 **機會** 25
機會在哪裡，以及我會怎麼做

12 **觀察指標** 27
觀察重點，2026 年 11 月至 2027 年

13 **該問的問題** 28
你沒問但該問的問題

◆ **關於作者** 29
譚帥

◆ **資料來源** 30

圖表

圖表



圖 01 AI × 加密貨幣六大領域：哪裡有真實付費需求 05
圖 02 在 Pearl 的整數工作上，GPU 共享同一能耗上限 08
圖 03 Pearl 的前六個月：算力跟著價格走，規則一改再改 10
圖 04 補貼倍數：一個網路支付的是外部收入的幾倍 13
圖 05 效率為何不再帶來利潤：ASIC 最多保留收入的 1 − 1/k 16
圖 06 多數盤子比不上一顆晶片的設計預算 18
圖 07 五類晶片，五種答案 21
圖 08 一片先進製程晶圓的價格是成熟製程的十倍 22
圖 09 先買證據，再買光罩：第一顆晶片的分階段預算 24

文中標記

- 估算 — 作者依所引資料所做的計算或推論
- 廠商宣稱 — 由銷售該產品的公司發布，未經獨立驗證
- 分析 — 作者對證據的解讀

本文譯自英文版；兩者如有出入，以英文版為準。

資料截至 2026 年 11 月 13 日 · 金額單位：美元

摘要

定理成立，激勵不成立

結論

Pearl 證明了「算力即共識」在工程上可行，但還沒證明它有用。

≈90 EH/s
Pearl 全網算力（2026 年 11 月 13 日），1 H 即一次 INT7 乘加

≈1%
的 Pearl 區塊承載真實 AI 工作（Blockworks，2026 年 10 月 28 日）

≈7,000 萬美元
Bittensor 每年可驗證的外部收入，對比逾 3 億美元的排放

175–180×
Aleo 在 2025 年第三季的證明者獎勵與手續費之比

R × (1 − 1/k)
比邊際礦工便宜 k 倍的 ASIC 的利潤上限
估算

≈150 萬美元
經模型、FPGA 與 MPW 在 N7 上拿到實測的矽，之後才是 ≈350 萬美元的光罩組
估算

Pearl

2026 年 11 月 13 日，Pearl 全網算力約 90 EH/s。在其共識程式碼中，一次「雜湊」就是一次整數乘加，因此全網相當於約 12.2 萬張 H100 的整數吞吐量。然而只有約 1% 的區塊承載真實 AI 工作，而唯一公開的推論合作已不在其供應商的 serverless API 上提供。原因在經濟而不在密碼學：一張邊提供推論服務邊挖礦的 GPU，只能拿到專用礦卡約 1% 到 27% 的算力，所以理性的礦工會去乘隨機矩陣。

付費需求

綜觀 AI × 加密貨幣，可驗證的付費需求出現在三處：賣推論、賣資料、賣隱私。Bittensor 可驗證的外部收入每年約 7,000 萬美元，其中約五分之四來自算力與基礎設施類子網。Grass 自報 2026 年上半年資料收入 1,700 萬美元。可信執行環境中的機密推論已上線生產。相較之下，真正由 AI Agent 發起的支付每月只有約 5,000–11,000 美元，zkML 與去中心化訓練則尚無已披露的付費需求。

補貼與價值

補貼倍數是最誠實的健康檢查。Aleo 的證明者獎勵約為其手續費的 175–180 倍；Bittensor 的排放約為其可驗證收入的 4–11 倍；Render 的市值約為其鏈上手續費的 360 倍；而 Pearl 每年約 4.6 億美元的礦工收入以區塊補貼為主，與付費 AI 需求幾乎脫鉤。補貼是冷啟動的燃料，不是商業模式。與此同時，價值正從代幣移向股權：四家使用中心化基礎設施、做加密原生分發的股權公司估值約 85 億美元，大約等於協議層與應用層 AI 代幣的總和。

ASIC

就晶片而言，ASIC 的利潤上限大致是單位算力收入乘以 (1 − 1/k)，其中 k 是它比邊際硬體便宜的倍數。由於這一項是凹函數，k 超過 5–10 之後，效率再提升幾乎不增加利潤；決定成敗的是盤子的大小、規則能維持多久，以及晶片有沒有第二市場。我依晶片類型給出的答案：現在不要投片做專用 INT7 Pearl 晶片，改為押注也能挖礦的推論優先加速器；新進者別進入商用 Bitcoin 礦機市場；小團隊不要做獨立的訓練晶片；已簽下客戶時就做推論晶片；ZK 加速器避險，FHE 提早布局。

節點與預算

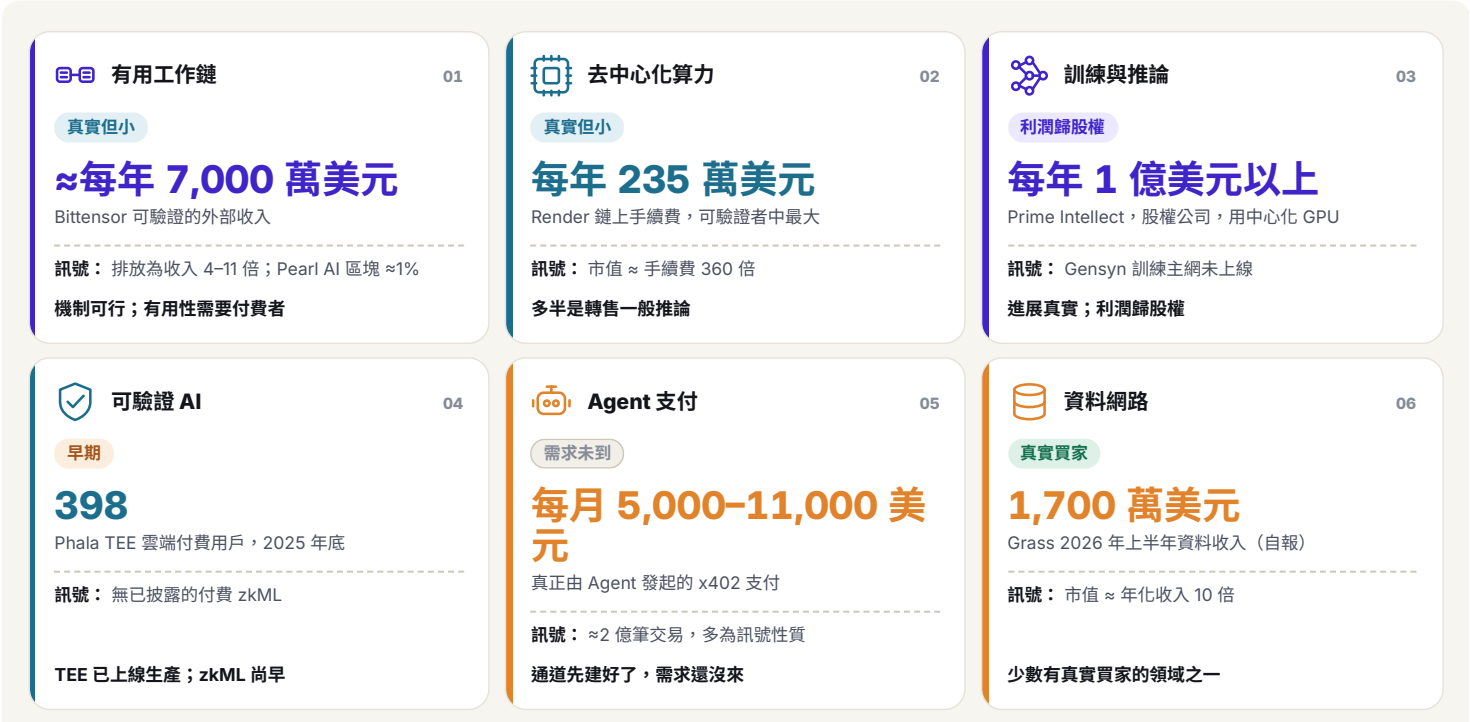
製程節點應依晶片終生成本中最大的一項來選擇：全天候運轉的晶片看能耗，訓練晶片看封裝與記憶體，推論晶片看 SRAM 還是 HBM。而第一顆晶片應分階段購買：先模型、再 FPGA、再多專案晶圓，

最後才是光罩組，這樣協議一旦改變，損失的只是一個原型的價格，而不是一次投片的價格。機會在領域交會之處：加密貨幣是第一個客戶，AI 是第二市場。

問題	判斷	關鍵數字（來源見各章）
① **Pearl 可行嗎？它的工作有用嗎？**	可行：一條以大規模矩陣乘法保護的區塊鏈。還談不上有用：幾乎所有挖礦都在乘隨機矩陣	2026 年 11 月 13 日約 90 EH/s；1 H = 1 次 INT7 乘加；約 1% 的區塊承載 AI 工作
② **AI × 加密貨幣的真實付費需求在哪裡？**	推論、資料與隱私。Agent 支付、zkML 與去中心化訓練仍處於需求出現之前	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；Agent 支付每月約 5,000–11,000 美元
③ **值得做 ASIC 嗎？**	只有在盤子大、規則穩、晶片有第二市場時才值得。目前沒有網路三者兼具	利潤上限 ≈ R × (1 − 1/k)；Bitcoin 礦工收入每年約 115 億美元，Pearl 約 4.6–4.9 億美元，Kaspa 約 1,800 萬美元
④ **小團隊該做哪些晶片？**	推論優先、也能挖礦的加速器；為已簽約客戶做的推論晶片；提早投入 FHE。不做商用 Bitcoin 礦機或訓練晶片	Kaspa 最好的 ASIC 每天賺 0.86 美元；3/2 nm 設計預算 6,000 萬–4 億美元以上
⑤ **選哪個製程節點？**	由最大的終生成本決定：能耗、封裝與記憶體，或記憶體架構	台積電 N2 每片晶圓約 30,000 美元，N28 約 3,000 美元；HBM 與 CoWoS 約占 H100 成本的 63%
⑥ **第一顆晶片要花多少錢，該怎麼買？**	分四個階段：模型、FPGA、多專案晶圓，然後才是光罩。若規則或買家尚未確定，就在光罩之前停下	商用 MPW 名額 50,000–500,000 美元；N7 光罩約 350 萬美元；7/6 nm 設計預算 1,500 萬–1 億美元

圖 01 **AI × 加密貨幣六大領域：哪裡有真實付費需求**

可驗證的付費需求對比補貼與估值訊號，2026 年 11 月



資料來源: DefiLlama、SubConnect（經 hoge.gg）、TRM Labs、Phala、Dealroom、SiliconANGLE、CoinGecko、Blockworks；作者綜合整理。

第 01 章

01 範圍、方法與四項檢驗

範圍與方法

為什麼寫這份報告，為什麼是現在

2026 年 4 月，一條新的區塊鏈 Pearl 把一個由來已久的想法投入了生產：讓礦工以 AI 所依賴的矩陣乘法來競爭出塊，而不是做雜湊。六個月內，其全網算力達到約 90 EH/s，代幣市值約 5 億美元。同一時期，AI 算力市場、去中心化訓練網路、Agent 支付通道與資料網路募集了數十億美元，Bitcoin 礦工也開始把電力場址改建成 AI 資料中心。我想知道其中哪些有真實客戶、客製化晶片在其中是否有任何用武之地，以及一個晶片團隊實際上能用哪個製程節點、哪家晶圓代工廠。

檢驗任何 AI × 加密貨幣專案的四項標準

2017 年一份關於 Gridcoin 的安全研究主張：有用計算要能保護區塊鏈，必須難以求解、易於驗證、易於獎勵。我再加上第四項。這四項共同決定了下文的大部分內容。

01 **難以求解。** 誠實計算必須是產生有效證明最便宜的方法；不能有捷徑。

02 **易於驗證。** 檢查工作的成本必須遠低於做工作的成本，否則網路要付兩次錢。

03 **易於獎勵。** 協議必須能僅憑證明本身算出獎勵，無須信任第三方。

04 **有人為產出付費。** 除非網路外部有客戶為結果付錢，否則「有用」的工作只是一筆附帶故事的補貼。

雜湊謎題通過前三項，卻過不了第四項。真實的 AI 任務通過第四項，卻過不了第二項：以零知識證明一次 AI 計算，成本是計算本身的 100 到 10,000 倍，而學習證明（proof-of-learning）方案已被證明可以低成本偽造。Pearl 的加噪矩陣乘法，是第一座可信的橋樑：既通過驗證檢驗，又保持與 AI 計算相同的形狀。

我的研究方式

這是案頭研究，做法就像我審查一顆晶片或一份商業計畫。我讀了 Pearl 的程式碼、協議提案與白皮書；來自獨立全節點的鏈上資料；公司申報文件與財報；密碼學、計算機架構與機器學習的論文；晶圓代工與廠商的價格資料；以及產業與科技媒體。每個數字都附有日期。我自行推導的數字會說明，並標為 估算。僅由賣方公布的數字標為 廠商宣稱；我對證據的解讀標為 分析。金額單位為美元。狀態以 2026 年 11 月 13 日為準。

第 02 章

02

Pearl · 機制

Pearl：以矩陣乘法作為共識

從定理到主網

2025 年 4 月，Ilan Komargodski 與 Omri Weinstein 發表了〈Proofs of Useful Work from Arbitrary Matrix Multiplication〉。他們為任意矩陣乘積構造了一種有用工作量證明，額外開銷只有樸素乘法的 1 + o(1) 倍；其安全性建立在求解成批隨機低秩線性方程組的困難度上，而這是一個猜想，不是證明。論文點出了這個領域真正的難處：常數倍開銷的有用工作量證明很容易做到，但沒有用；難的是在礦工自選輸入時，仍讓誠實計算保持為最便宜的獲勝方式。

Pearl 主網於 2026 年 4 月 27 日 09:00 UTC 上線。礦工計算加噪乘積 (A + E)(B + F)，其中低秩雜訊由 BLAKE3 承諾導出，然後去除雜訊還原 A·B。每個輸出 tile 的累加器狀態被雜湊成一張彩券；中獎的 tile 被打開，並以小於 60 KB 的遞迴 Plonky2 零知識證明證實，放在上限 65 KB 的區塊憑證中。驗證只需一個常數大小的小證明，與矩陣大小無關：檢查起來和雜湊謎題一樣便宜，而計算本身卻可以有用。

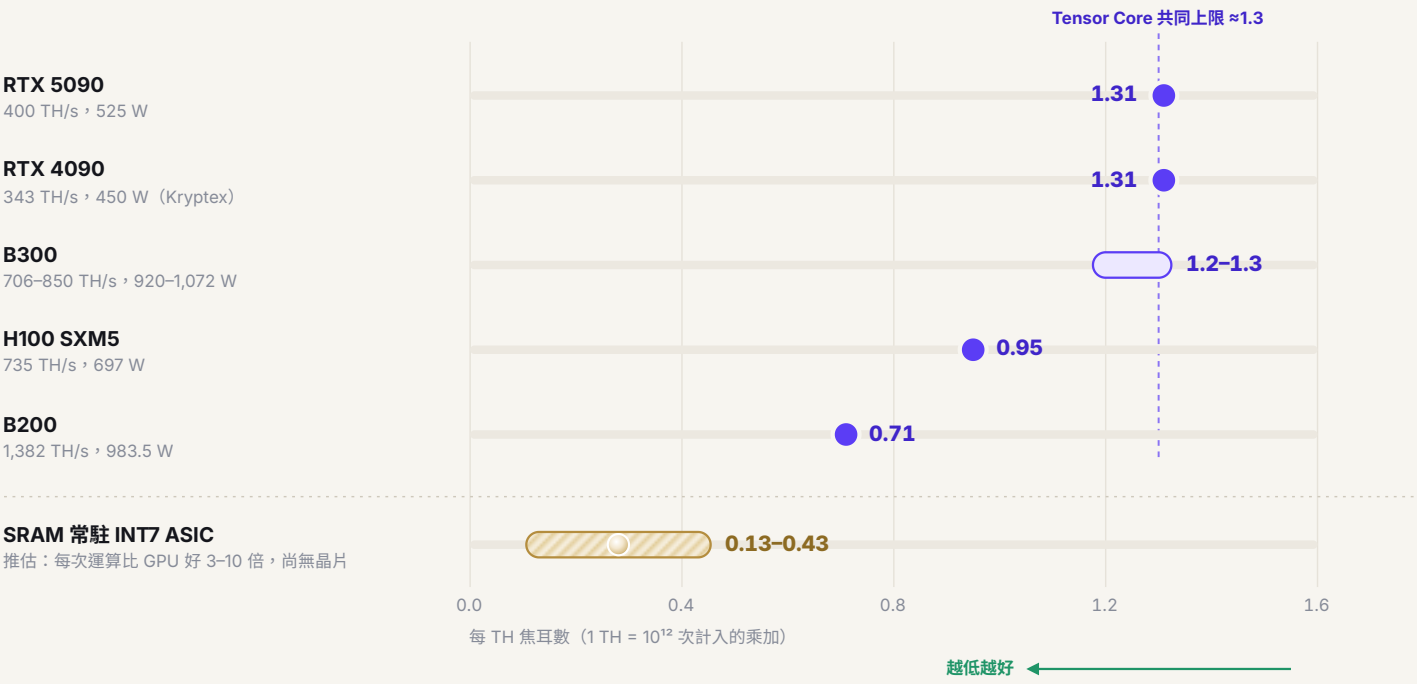
一次乘加就是一次「雜湊」

對晶片設計者而言，最重要的事實是單位。Pearl 的共識程式碼把每次嘗試的目標值乘以 tile 大小與點積長度，因此 **1 H 恰好是一次計入的 INT7 × INT7 → INT32 乘加（MAC）**。自區塊 96,251 起，秩懲罰要求雜訊秩至少為 128；在最低秩下，1 H 仍等於 1 次 MAC。因此 Pearl 的「EH/s」字面意思就是每秒 10^18 次整數乘加：**區塊鏈的安全預算第一次以 AI 加速器的張量吞吐量計價。** 實測的 GPU 算力落在各卡稠密 INT8 乘加峰值的 60% 到 95%，與這種解讀相符。

硬體	Pearl 算力	功耗	每兆次 MAC 焦耳數（J/TH）	來源（日期）
RTX 5090	400 TH/s	525 W	1.31 估算	Kryptex（11 月 12 日）
RTX 4090	約 305 TH/s（社群區間 280–330）；Kryptex 列為 343 TH/s	450 W（Kryptex）	1.31（Kryptex 數字）估算	prlstats（10 月 3 日）；Kryptex
H100 SXM5	735 TH/s	697 W	0.95 估算	PeakMiner，經 prlstats（9 月 19 日）
B200	1.382 PH/s	983.5 W	0.71 估算	PeakMiner，經 prlstats
B300	706–850 TH/s	920–1,072 W	1.2–1.3 估算	prlstats；SimeonOnSecurity

圖 02 **在 Pearl 的整數工作上，GPU 共享同一能耗上限**

以實測 Pearl 算力計，每兆次 INT7 乘加的焦耳數（J/TH）；越低越好



資料來源: Kryptex（2026 年 11 月 12 日）；PeakMiner 與 SRBMiner 基準測試（經 prlstats）；SimeonOnSecurity；ASIC 區間為作者推估，並非實測。

這張表裡有兩個細節對晶片設計者很重要。第一，消費級 RTX 4090、5090 與資料中心級的 B300 都收斂在約 1.3 J/TH，即使最好的 B200 也只到約 0.71 J/TH。一張售價數萬美元的資料中心 GPU，每次整數乘加耗費的能量幾乎和遊戲顯示卡一樣，這指向一個 Tensor Core 每次 INT8 MAC 能耗的共同上限，而這個上限正是專用晶片可能突破之處。第二，B300 比 B200 慢：輝達在 Blackwell Ultra 中大幅削減了 INT8 吞吐量，所以整數工作在這顆晶片上只能走較慢的路徑。主流 AI 晶片正從 INT8 轉向 FP8 與 FP4。當共識選定的數字格式與硬體發展方向分道揚鑣時，協議就不得不修改規則，這正是 FP8 分叉的根源，也是本報告後面我對 ASIC 判斷的根源。

第 03 章

03 Pearl · 經濟
Pearl：規模、排放與有用性落差

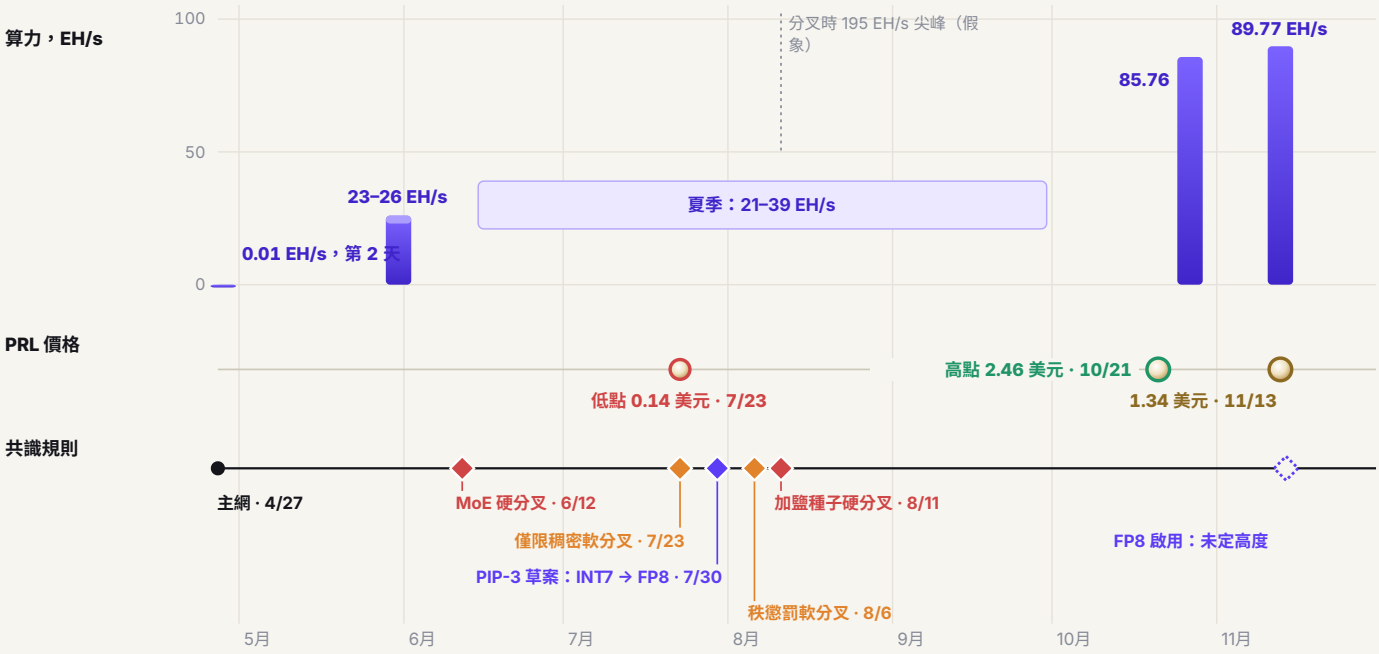
六個月從 0.01 到 90 EH/s

指標	數值（2026 年 11 月 13 日）	依據與來源
全網算力	約 90 EH/s（基準 89.77；同日區間 88.20–93.22；11 月 12 日盤中高點 110–123）	獨立全節點 prlstats；Kryptex
難度與區塊高度	58,841,982 與 142,530	prlstats
等效硬體	約 12.2 萬張 H100 或 22.5 萬張 RTX 5090	以每卡 735 與 400 TH/s 計 估算
價格、市值與完全稀釋估值	1.32–1.34 美元；約 5 億美元；約 28 億美元（CoinGecko 排名 101）	CoinGecko
歷史高點與低點	2.46 美元（10 月 21 日）與 0.1399 美元（7 月 23 日）	CoinGecko
已挖出幣量	3.776 億 PRL，占 21 億上限的 17.98%	prlstats
區塊補貼與每日排放	約 2,173 PRL 與約 97–103 萬 PRL	prlstats；Kryptex
未來 12 個月新增供給	約為目前供給的 78%	prlstats
礦工收入	每天約 125 萬美元（模型），每年約 4.6 億美元	prlstats
單位算力收入 R	每 PH/s 每天約 14–15 美元；一張 RTX 5090 每天約賺 5–6 美元	估算；Kryptex
承載真實 AI 工作的區塊	約 1%（10 月 28 日的估計）	Blockworks
礦池集中度	Kryptex 在過去 24 小時挖到 46.4% 的區塊；前兩大礦池約 62%	prlstats
持幣集中度	地址吉尼係數 0.969；前 100 個地址持有 53.0%	prlstats

Pearl 的算力近似於其價格的滯後函數。上線隔天全網約 0.01 EH/s；到 5 月底達到 23–26 EH/s。夏季價格從 5 月高點下跌約 86%，算力在 21–39 EH/s 之間橫盤。9、10 月價格上漲約十倍後，算力在 10 月 27 日達到 85.76 EH/s，11 月約 90 EH/s。8 月 11 日飆到 195 EH/s 的尖峰恰逢分叉，應視為估算假象。能耗隨之成長：一項研究估計全網在 24 EH/s 時約 112 MW，prlstats 的模型則估計目前約 190–215 MW。

圖 03 **Pearl 的前六個月：算力跟著價格走，規則一改再改**

全網算力、三個價格標記與每次共識變更，2026 年 4 月 27 日至 11 月 13 日



資料來源: prlstats 全節點與時間序列；Kryptex；CoinGecko；Pearl 的 params.go 與 PIP-3。8 月 11 日的尖峰是分叉時的估算假象。

排放放大了反身性

供給上限為 21 億枚，沒有減半：區塊補貼依 E(t) = S·H / ((t + H)(t + H − 1)) 平滑遞減，其中 H = 650,226。但排放以區塊計，而非以時間計，而早期難度起點太低、調整又慢。**第一天挖出約 4,406 萬枚，前六天約 1.2 億枚**，約占目前供給的 32% 估算。近期出塊時間約 171–183 秒，仍快於 194 秒的目標。結果是未來 12 個月供給將成長約 78%，這是礦工、硬體廠商與持幣者都必須面對的稀釋。

礦工經濟隨之而來。全網礦工收入每天約 125 萬美元（模型）；以 Kryptex 的每日排放乘以目前價格，約為每天 135 萬美元，因此**單位算力收入 R ≈ 每 PH/s 每天 14–15 美元** 估算。一張 RTX 5090 每天約賺 5–6 美元。一張 H100 或 H200 每天約賺 11 美元，而最便宜的公開隨選租用價約為每卡每小時 2.09 美元，約每天 50 美元，所以只為挖礦而租卡會大幅虧損。R 波動很大：依 prlstats 的序列，8、9 月約 10 美元，10 月中曾短暫達到約 33 美元 估算。上線後幾週內，RTX 5090 的估計日收入就從約 33.80 美元減半至約 17.19 美元。租用雲端 GPU 挖礦，只在最初幾週與 10 月價格飆升期間有利可圖。

定理成立，激勵不成立

真正的問題在需求，不在密碼學。Pearl 唯一公開的商業整合，是 Together AI 的 Gemma-4-31B-it-pearl 端點，5 月 15 日推出，價格比一般低 25% 以上，折扣由排放的預期未來價值支應。11 月 13 日，模型頁面顯示它**未在 Together 的 serverless API 上提供**。6 月，一項針對 8,012 個線上挖礦實例（約占全網 21%）的普查得出結論：網路根本沒有產生任何有用的 AI 計算（作者稱該證據具提示性，而非決定性），並顯示由純隨機矩陣構成的 share 也被礦池接受。10 月 28 日，Blockworks 估計**只有約 1% 的區塊承載真實 AI 工作**；它寫道，少了這一點，Pearl 就是一個更小、更不安全、通膨更快的 Bitcoin。

原因是可以算出來的。推論端的開銷確實很小：Pearl 公布在四張 H200 上跑 Llama 70B，端到端時間增加 5.08%；一項獨立測試在單張 Hopper GPU 上測得吞吐量損失 9.2%。挖礦端則收益太少。官方 vLLM 外掛只在至少 1,024 個 token 的

prefill 批次上挖礦，從不在 decode 步驟上挖礦。一張提供推論服務的卡，在純 prefill 流量下約得到專用礦卡 27% 的算力，在 80% 為 decode 的聊天混合流量下約 5.4%，在以 decode 為主的流量下只有約 1%。沒有付費推論需求，理性的礦工就會去乘隨機矩陣；協議驗證的是承諾的矩陣是否被誠實相乘，而不是它們是否有用。**定理成立，激勵不成立。** Pearl 的有用性是鏈下的商業問題：總得有人為推論付錢。

第 04 章

04 Pearl · 規則
Pearl：規則風險、數值與治理

兩個月四次分叉

Pearl 的另一面，是規則變動之快。2026 年 6 月到 8 月，實驗室在寫死的區塊高度上推動了四次共識變更：混合專家硬分叉（區塊 71,935，約 6 月 12 日）、僅限稠密軟分叉（91,630，約 7 月 23 日）、秩懲罰軟分叉（96,251，約 8 月 6 日）與加鹽種子硬分叉（99,000，約 8 月 11 日）。加鹽種子分叉之後，舊礦機只能產生無效 share；秩懲罰使高秩配置的有效算力減少 50% 到 87.5%。

下一步是 PIP-3，目前仍是草案：它把挖礦從 INT7 改為 FP8 × FP8 → FP32，並要求逐位元精確的裝置設定檔，**只支援 Hopper 與 Blackwell 兩種架構**。文件稱硬體依賴是浮點協議的必要之惡，並警告驗證中的任何容差都會招來 grinding 攻擊。11 月 12 日，fp8-scheme 分支的主網參數未設定啟用高度。依目前草案，RTX 40 系列、A100 與 AMD 顯示卡都不被接納，而 prlstats 一個低信心模型估計約 82% 的算力來自消費級顯示卡。強推分叉，有鏈分裂或礦工反彈的風險。

數字格式的三難

Pearl 面臨一個三難：一種數字格式可以對 AI 有用（FP8 或 FP4）、跨硬體逐位元可驗證、硬體中立，但三者最多只能兼顧兩項。INT7 方案可驗證且中立，卻與 AI 晶片的發展方向背道而馳。帶白名單的 FP8 有用且可驗證，卻把共識綁在單一廠商身上。帶容差的 FP8 有用且中立，卻為 grinding 攻擊打開了大門。Tensor Core 中的浮點運算一般不遵循數值標準，跨世代也無法重現；例如在 Hopper 上，FP8 累加只保留 13 個小數位元並做截斷。從晶片設計者的角度看，「Hopper 設定檔」是一套完全確定的算術，ASIC 可以逐位元實作，或許還比 GPU 更有效率。但這麼做會是違背協議明示意圖的灰色地帶生意，治理風險極高 分析。

治理

治理高度集中。所有協議提案都由實驗室撰寫；分叉在寫死的高度啟用，沒有礦工訊號；沒有第二套客戶端實作；而截至 10 月初，節點與零知識電路都沒有公開的第三方稽核。以色列報紙 TheMarker 報導，實驗室在一輪隱密融資中募得約 1.2–1.3 億美元（約 5,500 萬美元股權，加上約 7,500 萬美元的 GPU 基礎設施基金）；Pearl 未透過官方管道證實。「代幣沒有投資人配額」與「一家有創投股東的公司」可以同時為真，但張力依然存在：AI 收入可能流向股權，稀釋卻落在持幣者身上。

綜合來看，Pearl 是迄今最乾淨的「算力即共識」實驗：機制新穎、可在鏈上驗證、單位與 AI 硬體一一對應。但有用性尚未到來，而它的安全預算、算力與礦工熱情，全都繫於一個主要需求尚未成形、供給 12 個月內還將成長約 78% 的代幣。Blockworks 提出的三個訊號值得追蹤：升級能否順利落地、AI 工作區塊的比例是否實質上升，以及是否有任何推論供應商把挖礦收入回饋給客戶。

第 05 章

05

有用工作鏈

有用工作鏈：矩陣和零知識都擋不住 ASIC

Kaspa：矩陣既不有用，也擋不住 ASIC

Kaspa 是教科書級的案例。它的 kHeavyHash 在兩次雜湊之間做一次 4 位元數值的 64 × 64 矩陣—向量乘積，而乘積隨即被丟棄。在 2021 年 11 月公平啟動約 16 個月後，IceRiver 於 2023 年 3 月 14 日發表了首批 Kaspa ASIC，到 2023 年底 GPU 挖礦已經結束。比較 3.8 GH/s、300 W 的 RTX 4090 與 77 J/TH 的比特大陸 KS7，效率差距約為 **1,000 倍** 估算。盛宴之後是壓縮：11 月 13 日，全網算力為 358.9 PH/s，比 2024 年 8 月的 1 EH/s 低約 64%，而最好的 KS7 在每 kWh 0.10 美元的電價下每天只賺 **0.86 美元**。

Aleo：零知識也擋不住專用硬體

Aleo 的證明者謎題設計來模擬產生 SNARK 證明的工作；它並不證明使用者的交易，專案也公開歡迎 ZK ASIC。2024 年 9 月主網上線約五個月後，專用機器就已出貨。2025 年第三季，證明者獲得 3,120 萬 ALEO（約 780 萬美元），而網路只收到約 43,000–44,000 美元的手續費：**補貼倍數約 175–180**。價格從早期交易時的約 9 美元跌到該季末的 0.22 美元，而 ARC-46 現在要求每個解質押 10 萬到 250 萬 ALEO，把挖礦變成了質押門檻。

Qubic 與 Bittensor

Qubic 宣傳的是訓練其 Aigarth 神經網路的「有用工作量證明」，但它的算力在 2025–2026 年最顯眼的產出，卻是別條鏈的區塊。它先是挖 Monero，占比從 2025 年 5 月中旬的不到 2%，提高到 7 月底的 25% 以上，並在 8 月宣稱達到 51%，造成一次六個區塊的重組（另一來源稱 18 個）。2026 年 4 月 1 日，它改用 ASIC 挖 Dogecoin，收益用於回購與銷毀。沒有獨立證據顯示其 AI 訓練有用，其市值從約 2.8–3 億美元跌到 11 月 13 日的約 5,000 萬美元。它也暴露了一種外部性：一條為通用算力付費的鏈，會創造出一個龐大、可租用、協調一致的算力池，可以被拿來對付對 CPU 友善的鏈。

Bittensor 不是工作量證明，而是以質押加權的主觀評分：驗證者為礦工評分，權重在質押加權中位數處截斷。它是這群網路中唯一具規模化外部收入者。只計入可驗證外部客戶的 SubConnect 指數顯示，2026 年 11 月初約為**每年 7,000 萬美元**（9 月 1 日約 3,500 萬美元），其中 78% 到 82% 來自算力與基礎設施；但以 11 月初的價格計，其排放每年超過 3 億美元，所以收入只能覆蓋 9% 到 23%。收入估計隨口徑差異很大，從約 1,700 萬美元（Artemis）到依自報總額年化的 1.72 億美元。4 月時，128 個子網中有 67 個銷毀了 99% 以上的激勵；當領先團隊 Covenant 因治理問題離開時，TAO 在數小時內下跌 24%。

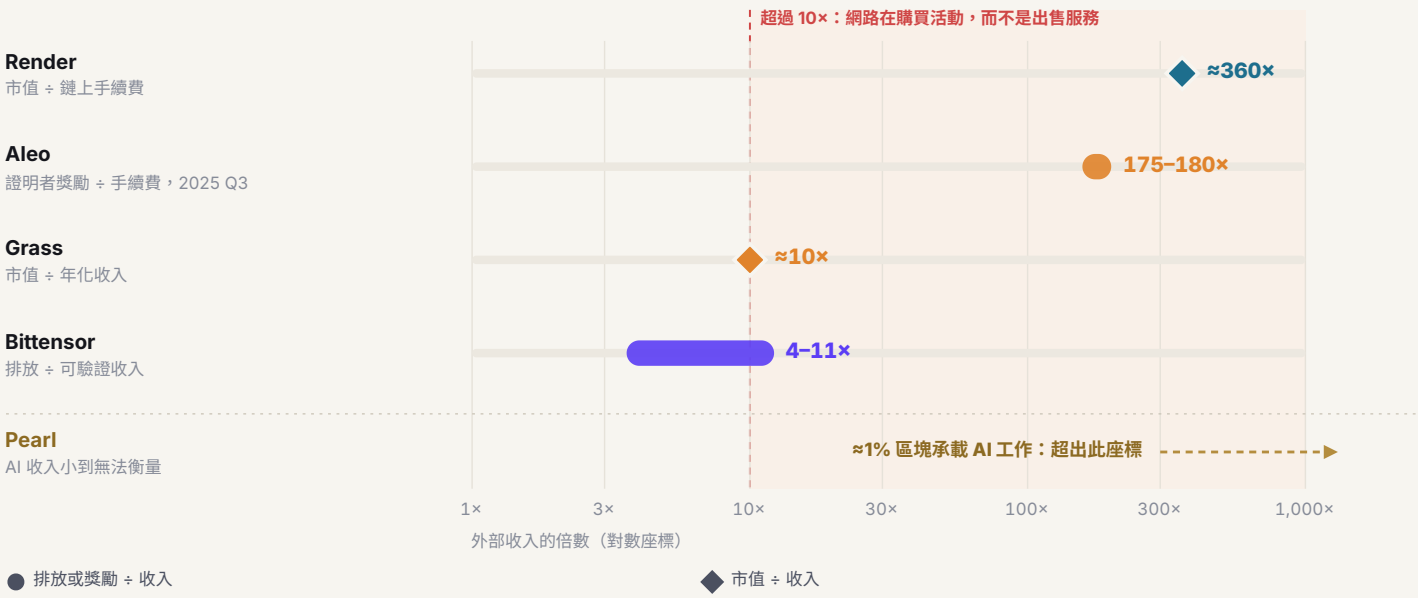
歷史給出同樣的答案

Primecoin 的質數鏈驗證很快，但沒有人需要它們。Gridcoin 依賴第三方統計網站來證明 BOINC 貢獻，研究人員在不做任何計算的情況下偽造了區塊。Filecoin 的儲存證明在技術上可行，但 2025 年第三季使用率只有 36%，其 793,000 美元手續費中 99.5% 是罰金，基本手續費僅 4,100 美元。

專案	工作或共識	市值（日期）	硬體路徑	付費需求對比補貼	判斷
Pearl	加噪矩陣乘法（INT7 MAC 加 ZK 憑證）	約 5 億美元（11 月 13 日）	GPU；FP8 草案將以白名單接納 Hopper 與 Blackwell	約 1% 的區塊承載 AI 工作；礦工收入以補貼為主	最可信的機制；需求未經證實
Kaspa	kHeavyHash（雜湊之間的 64 × 64、4 位元矩陣—向量乘積）	約 8.4 億美元（11 月 13 日）	上線約 16 個月後出現 ASIC；現已全為 ASIC	不宣稱有用；礦工收入每年約 1,800 萬美元 估算	矩陣既不有用，也擋不住 ASIC
Aleo	合成 SNARK 謎題加權益證明	約 1.18 億美元（2025 年第三季末）	約五個月後出現專用機器	證明者獎勵約為手續費的 175–180 倍	合成工作，由補貼驅動
Qubic	「uPoW」（宣稱訓練 Aigarth）	約 5,000 萬美元（11 月 13 日）	CPU 與 GPU；自 2026 年 4 月起以 ASIC 挖 Dogecoin	無有用性的獨立證據；算力用於外部挖礦與回購	披著 AI 故事外衣的算力聚合
Bittensor	Yuma 共識（質押加權評分）	約 25.5 億美元（11 月 11 日）	通用 GPU；沒有 ASIC 路徑	每年約 7,000 萬美元可驗證收入，對比逾 3 億美元排放	唯一具規模化外部收入者；仍是 4–11 倍的補貼
Filecoin（參照）	複製證明與時空證明	約 15 億美元（2025 年第三季末）	—	使用率 36%；每季基本手續費 4,100 美元	有用，但需求不足

圖 04 **補貼倍數：一個網路支付的是外部收入的幾倍**

排放或市值除以來自網路外部的付費收入，對數座標



資料來源: Blockworks（Aleo 2025 年第三季）、DefiLlama（Render 手續費）、CoinGecko、hoge.gg（Bittensor）、Dealroom（Grass）、Blockworks 0xResearch（Pearl）；作者計算。

對硬體的教訓：以流動性代幣支付的固定、規律的工作，約 3 到 16 個月內就會出現 ASIC，而且往往先來自挑戰者，而非既有業者。「有用」的說法只在外部客戶為產出付費時才站得住腳。而硬體被擱置的主要驅動因素，是相對於收入過高的補貼，以及開發者對工作函數的控制。

第 06 章

更廣的版圖

06 AI × 加密貨幣的其餘部分：真實但不大的需求，價值移向股權

去中心化算力市場

去中心化算力有付費客戶，但需求小、集中，且多半是轉售開源模型推論。可在鏈上驗證的手續費很少：DefiLlama 顯示過去一年 Render 約 235 萬美元、Livepeer 約 68 萬美元，整個 DePIN 領域 2025 年的鏈上收入只有約 7,200 萬美元。自報數字較大但定義鬆散：Aethir 公布 2025 財年營收「超過 1.278 億美元」，卻沒說明這是總帳單還是協議抽成。代幣價值與收入在兩個方向上都已脫節：Render 的市值約為其鏈上手續費的 360 倍，而 Aethir 約 8,770 萬美元的市值卻低於其自報營收 估算。

便宜 70% 到 85% 的說法，只在對比超大規模雲端業者的隨選價格時成立。11 月 3 日，Akash 上 H100 的加權平均價格約為**每 GPU 小時 2.73 美元**（區間 2.04–3.16 美元），低於 AWS 的約 6.88 美元與 Google Cloud 的 11.06 美元，但高於 Vast.ai 的約 1.73 美元、RunPod 社群雲的 1.99 美元，以及一年期預留的約 2.44 美元（其他平台價格為 9 月 12 日讀數；發布者 Akash 為利害關係人）。需求多半是透過 OpenRouter 分發的一般推論，AkashML 每天約 17 億個 token，io.net 超過 40 億個，與每一家新興雲端業者正面競爭。最大筆的「去中心化算力」資金正在重新中心化：把 Aethir 代幣當作庫藏資產持有的 Axe Compute，簽下了一份價值 15 億美元的五年合約，出租自己的 9,200 張 B300 叢集，而其 2026 年第一季營收只有 35,000 美元。

去中心化訓練與推論

透過網際網路訓練已在 80 到 400 億參數的規模上得到展示。Pluralis-8B 在 330 個以消費級 GPU 為主的節點上訓練了 40 天，達到中心化 H100 基準 63% 的效率，但其論文承認，這次訓練並非去中心化，需要 Pluralis 自己的節點與准入機構。Nous Research 的 Psyche 完成了 400 億參數的 Consilience 預訓練。到了前沿規模，工作又重新中心化：Prime Intellect 的 INTELLECT-3 是一個 1,060 億參數的混合專家模型，在以 400 Gbps InfiniBand 連接的 512 張 H200 上訓練了兩個月。限制很明顯：節點需要至少 200 Mbit/s 頻寬與約 100 倍的通訊壓縮，而信任與驗證仍仰賴營運者的特權角色。

錢流向了販售中心化產品的股權公司。Prime Intellect 在 7 月以 10 億美元估值募得 1.3 億美元之前，年化營收已超過 1 億美元；私密推論應用 Venice 公布年化營收超過 7,000 萬美元，且自 2026 年第一季起獲利（公司數字），以 10 億美元估值募得 6,500 萬美元，使用的是租賃 GPU。代幣這一側，Gensyn 的核心訓練網路仍「待定」，其代幣價值約 1,720 萬美元；AI 原生 L1 Ritual 的代幣在主網上線後從高點下跌 72%（僅見於標題）。

可驗證 AI

生產環境選擇了可信執行環境（TEE）。Hopper 的機密運算對典型 LLM 查詢增加不到 7% 的開銷，對大型模型則幾乎沒有；Phala 的生產開銷約 0.5% 到 5%，但到 2025 年底，其 10,004 位使用者中只有 398 位付費。TEE 的信任根是晶片廠商：2025 年 10 月披露的 TEE.fail，以一個成本不到 1,000 美元的 DDR5 匯流排中介器，從完全更新的 Intel TDX 與 AMD SEV-SNP 機器中取出遠端證明金鑰，進而動搖輝達的 GPU 機密運算，而兩家廠商都表示實體攻擊不在其威脅模型內。這恰恰就是 DePIN 的情境，節點營運者擁有實體接觸權。zkML 現在已能證明完整的 LLM：Lagrange 的 DeepProve 證明 GPT-2 約每分鐘 174 個 token，Gemma 3 約 86 個，與生產級推論相差幾個數量級，且沒有已披露的付費使用。

Agent 支付與資料

x402 是最好的警示案例。TRM Labs 統計，自 2025 年 5 月以來，已知協調者結算了約 1.989 億筆交易、5,270 萬美元，其中 99.6% 為 USDC；扣除自我支付、批次流量與買家少於十位的賣家之後，真正由 Agent 發起的比例只有 0.6% 到 7.5%，**約每月 5,000–11,000 美元**。Artemis 判斷超過 95% 的活動是協議訊號，而非買賣。與此同時，通道正被既有業者標準化：x402 Foundation 於 7 月 14 日在 Linux Foundation 之下成立，Visa、Mastercard、Stripe、Google、AWS、Cloudflare 與 Coinbase 為核心成員；而與 Stripe 共同撰寫 Machine Payments Protocol 的 Tempo，於 3 月以 50 億美元估值推出主網。Agent 代幣平台仍按發射平台的邏輯運作：Virtuals 自報 4.79 億美元的「aGDP」，ElizaOS 的創辦人則在一起集體訴訟和解後宣告其代幣已死。價值更可能被穩定幣發行者與支付業既有業者拿走；加密貨幣在這裡的獨特角色，或許是 Agent 的身分與問責。

資料是少數有真實鏈下買家的子領域之一。Grass 公布 2025 年資料收入 1,700 萬美元，2026 年上半年又是 1,700 萬美元，全年目標 7,500 萬美元，並表示已獲利；GRASS 價值約 3.28 億美元，約為其上半年年化收入的十倍 估算。它的護城河是分散式住宅頻寬的蒐集規模，而不是加密貨幣本身。資料 DAO 與資料市集缺乏可見的付費需求：Vana 價值約 2,150 萬美元，Ocean 約 2,760 萬美元，且 Ocean 正與 Fetch.ai 打官司。隨著 Agent 增多，人格證明正獲得真實的整合：World 表示已驗證近 1,800 萬人，Zoom、Docusign 與 Tinder 支援部分 World ID 功能。

資本已經投票

領域	可驗證的付費需求	補貼與估值訊號	判斷
有用工作鏈	Bittensor 每年約 7,000 萬美元可驗證外部收入；Pearl 約 1% 的區塊承載 AI 工作	Aleo 175–180 倍；Bittensor 4–11 倍；Pearl 以補貼為主	機制有價值；有用性需要付費客戶
去中心化算力市場	鏈上手續費每年約 68–235 萬美元（Livepeer、Render）；自報 400 萬–1.28 億美元	Render 市值約為手續費的 360 倍	真實但小，多半是轉售一般推論
去中心化訓練與推論	股權公司：Prime Intellect 每年逾 1 億美元，Venice 逾 7,000 萬美元（中心化基礎設施）	Gensyn 訓練主網未上線；Ritual 代幣從高點 −72%	技術進展真實；利潤歸股權
可驗證 AI	TEE 已上線生產（Phala 398 位付費用戶）；無已披露的付費 zkML	—	TEE 有用；zkML 尚早
Agent 支付	由 Agent 發起的流量每月約 5,000–11,000 美元	約 2 億筆交易，多為訊號與投機	先有通道，後有需求
資料網路	Grass 2026 年上半年 1,700 萬美元（自報）	GRASS 約為年化收入的 10 倍	少數有真實買家的領域之一

把六個領域並排來看，結論一致：**補貼是冷啟動的燃料，不是商業模式。** 11 月 13 日，CoinGecko AI 類別總值約 186 億美元，但其中約 56% 是 NEAR、ICP 等通用 L1，加上 TAO、質押 TAO（可能與 TAO 重複計算）與 Pearl 等共識層級的專案；協議層與應用層的 AI 代幣合計約 80 億美元或更少 估算。這大約等於四家股權公司的估值總和：Tempo（50 億美元）、Nous（報導值 15 億美元）、Prime Intellect（10 億美元）與 Venice（10 億美元）。加密貨幣創投資金卡在每季約 45–50 億美元，增量來自 AI 相關基礎設施，其占已披露金額的比例在 2026 年第三季從 8.1% 升至 18.2%；而 2025 年發行的 118 個代幣中，84.7% 的交易價格低於發行價。一句話：**加密貨幣負責分發與結算，利潤歸股權**，至少 2026 年是如此。

第 07 章

07 ASIC 經濟學
ASIC 問題：一條公式，三把尺

一條公式：為何 k = 5 之後效率就不再帶來利潤

設 R 為單位算力的每日收入（全網礦工收入除以全網算力），c 為邊際硬體（在 Pearl 上是 GPU）上單位算力的每日成本，k 為 ASIC 比該邊際硬體便宜的倍數（c_ASIC = c/k）。只要 GPU 仍是邊際礦工，自由進出就會把 R 推向 c，於是 ASIC 每單位算力賺得 R − c/k：

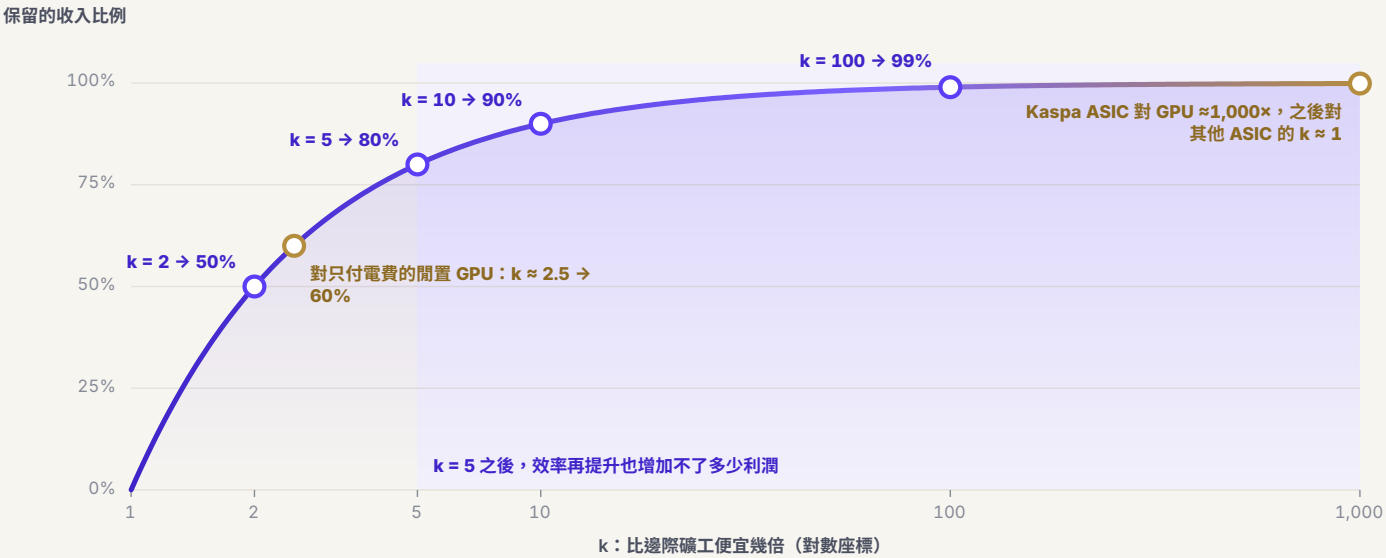
ASIC 利潤上限 ≈ R × (1 − 1/k)

就全網而言，一支 ASIC 機隊的年毛利上限大致是全網礦工收入 × (1 − 1/k)，而且只維持到 ASIC 取代 GPU 成為邊際礦工為止。

這條公式有三個推論。第一，(1 − 1/k) 是凹函數：k = 2 時 ASIC 保留 50% 的收入，k = 5 時 80%，k = 10 時 90%，k = 100 時 99%。**k 超過 5–10 之後，效率再提升幾乎不增加利潤**；決定性的是 R 與盤子的大小。第二，基準會重置：一旦 ASIC 成為邊際礦工，k 就必須以其他 ASIC 為基準來衡量。Kaspa 的 ASIC 對 GPU 曾有約 1,000 倍的效率優勢，換來的只是短暫的意外之財；如今最好的 KS7 每天只賺 0.86 美元。第三，在 Pearl 這種對 GPU 友善的鏈上，基準往往不是 GPU 的購買價格，而是**閒置 GPU 的電費**：一張自有的 RTX 5090，525 W、每 kWh 0.10 美元，每天電費約 1.26 美元，收入約 5–6 美元 估算。面對已是沉沒成本的 GPU，即使是只用五分之一能耗的 ASIC，若其折舊等於電費，有效的 k 也只有約 2.5，利潤上限約為 R 的 60%（示意性假設）。

圖 05 **效率為何不再帶來利潤：ASIC 最多保留收入的 1 − 1/k**

ASIC 相對邊際礦工可保留的收入比例，依其成本優勢 k



資料來源: 作者模型：當邊際硬體決定價格時，單位算力收入趨近其成本；Kaspa 與 RTX 5090 數字取自本報告。

三把尺：盤子、回本規模與規則

第一把尺是**盤子**。以 11 月第一週約 2,893 BTC 的區塊獎勵（約 2.22 億美元）年化，Bitcoin 礦工每年約賺 115 億美元 估算。Pearl 礦工約賺 4.6–4.9 億美元（以目前價格計）；Aleo 的證明者獎勵以 2025 年第三季年化約 3,100 萬美元；Kaspa 礦工以 1.945 KAS 的區塊獎勵、每秒十個區塊計，約 1,800 萬美元 估算。**Kaspa 一整年的礦工收入，還不到一顆 5/4 nm 晶片設計預算的低標（約 3,000 萬美元）。**

第二把尺是**回收 NRE 所需的算力**：

h* = NRE ÷ [R × (1 − 1/k) × T × p]

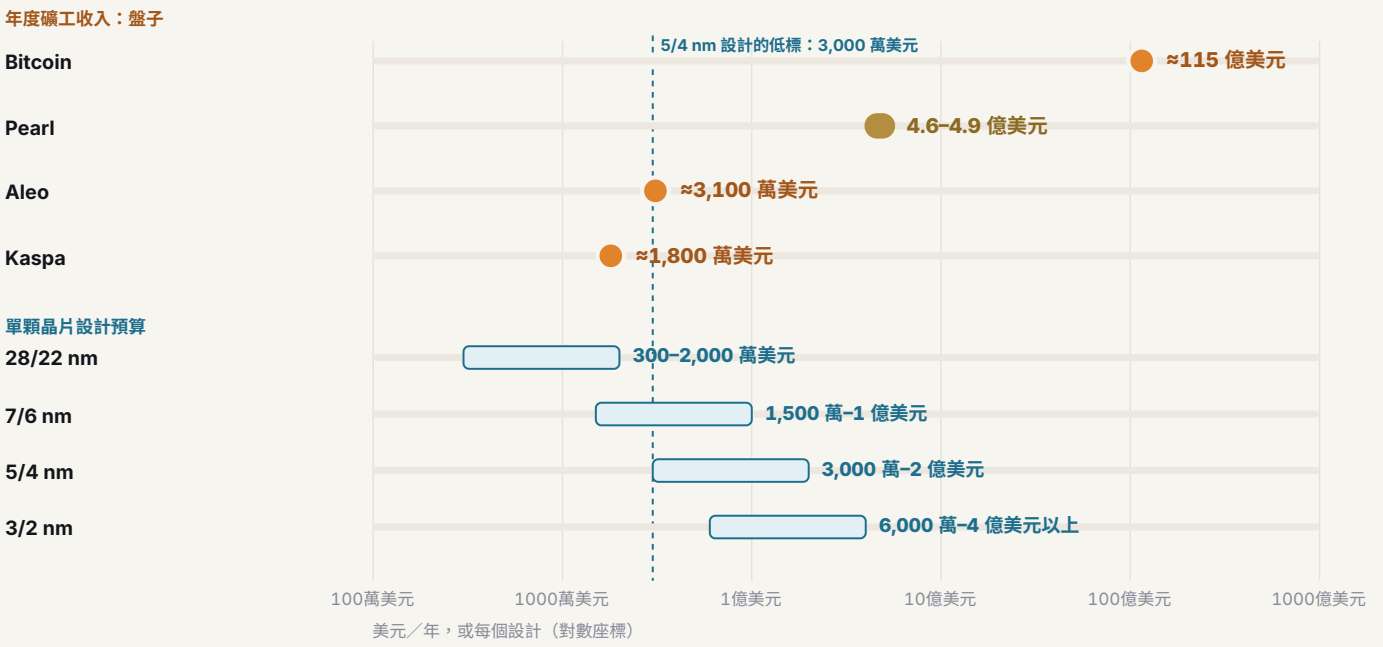
其中 T 是以天計的有效窗口，p 是規則在該窗口內維持不變的機率。就 Pearl 而言，取 R = 每 PH/s 每天 14 美元、k = 5、T = 365 天，NRE 為 2,000 萬美元（N7/N6 重複陣列晶片；取 Silicon Analysts 中階節點 500 萬–3,000 萬美元與 AnySilicon 7/6 nm 運算 ASIC 1,500 萬–1 億美元兩個區間的低端，因為礦機晶片用的 IP 少、結構重複；這是我的假設）。p = 1 時，需要約 **4.9 EH/s** 運轉整整一年，約占全網 5%；p = 0.5 時，約 **9.8 EH/s**，約 11%；若 R 回落到夏季約 10 美元的水準，即使 p = 1 也需要約 6.9 EH/s 估算。這個規模並非遙不可及。問題在 p 與 T。

第三把尺是**規則風險**，而它往往是決定性的。Monero 2018 年的反 ASIC 分叉讓比特大陸的 X3 被擱置，網路一度損失近一半算力。Sia 同年的分叉讓比特大陸與 Innosilicon 的礦機變磚，而與開發者有關聯的 Obelisk 礦機二手價卻從 2,499 美元漲到 5,000 美元以上。Ethereum 合併後一個多月，前 Ethereum 礦工中找到新工作的不到 20%。**誰控制工作函數，誰就掌握硬體投資者的命運**，而 Sia 顯示「抗 ASIC」可以變成開發者自己的護城河。有第二市場的硬體才活得下來：合併之後，GPU 轉向 AI 與雲端，而單一演算法的 ASIC 則擠進了 Ethereum Classic。窗口也在縮短：Kaspa 的第一顆 ASIC 花了約 16 個月，Aleo 約五個月，而最先觸及效率前沿的往往是挑戰者，而非既有業者。

網路	年度礦工收入（約）	邊際或基準硬體	規則穩定性	新進者可得的 k	判斷
Bitcoin	115 億美元	比特大陸 S23 XP Hyd（8.9 J/TH，每 TH 25.5 美元）	非常高	≤1	盤子大，但 k 屬於既有業者
Pearl	4.6–4.9 億美元（以目前價格計）	自有或閒置 GPU（邊際成本 ≈ 電費）與資料中心 GPU	非常低：兩個月四次分叉；FP8 白名單待定	效率上或許 3–10 倍 分析；對沉沒成本 GPU 則更低	盤子夠大；規則風險一票否決
Aleo	約 3,100 萬美元（2025 年第三季，年化）	IceRiver AE2 等專用機器	中等：ARC-46 質押門檻	≈1	盤子小，且門檻在提高
Kaspa	約 1,800 萬美元	KS7（77 J/TH）	高	≈1	年收入低於一顆 5/4 nm 設計預算的低標

圖 06 **多數盤子比不上一顆晶片的設計預算**

四個網路的年度礦工收入對比各製程節點單顆晶片的設計成本，對數座標



資料來源: Hashrate Index（Bitcoin，2026 年 11 月）、prlstats 與 Kryptex（Pearl）、Blockworks（Aleo，2025 年第三季）、minerstat（Kaspa）、AnySilicon（設計預算，2026）；作者年化。

「大盤子、穩定規則且 k > 1」這個象限目前是空的：Bitcoin 有盤子也有穩定規則，但 k 屬於既有業者；Pearl 的盤子夠大，但規則最不穩定；Kaspa 與 Aleo 的規則夠穩定，盤子卻太小。

第 08 章

08 逐類看晶片 五類晶片，五種答案

Pearl 類 PoUW：不做專用 INT7 晶片；押注能提供推論服務的礦機

支持 ASIC 的理由是真實的。目前只有約 1% 的區塊承載 AI 工作，所以白皮書的經濟論證——專用 ASIC 失去做有用工作的能力，因此賺得更少——此刻正處於最弱的時候。GPU 最昂貴的部分，HBM 與 CoWoS 封裝，約占 H100 製造成本的 63%，邏輯晶粒只占約 9%。一顆只做 7 位元整數乘加、把運算元放在晶片內 SRAM、以低電壓運行的晶片，有理由在每次運算的能耗上達到同節點 GPU 的 3 到 10 倍，在每次運算的成本上優勢更大 [分析；尚無實測]。反對的理由則更硬。先進節點的晶圓代工交期可能超過 50 週，新團隊從起步到量產約需 18 到 24 個月 估算；等晶片到貨時，Pearl 很可能已改用 FP8，接著是 FP4。而由於 PIP-3 以裝置白名單來定義被接納的算術，一旦它啟用，INT7 晶片就會直接停擺。

所以我的結論是：**現在不要投片做專用 INT7 Pearl 晶片。** 有兩個更好的押注。一是也能挖礦的推論優先加速器：圍繞通用 INT8/FP8 GEMM 與 SRAM 常駐運算元打造，這樣一旦挖礦之路被拒，價值也能落在真實的推論市場上。二是參與協議辯論，推動一套 ASIC 可以精確實作、廠商中立的標準算術，同時爭取演算法穩定的承諾，這是「大盤子、穩定規則、k > 1」

象限得以存在的前提。在那之前，架構可以先在 FPGA 或成熟節點的多專案晶圓（MPW）上驗證，把 NRE 風險控制在百萬美元等級。第 10 章會把這一點落實為分階段預算。

Bitcoin 類礦機：既有業者擁有 k，電力才是稀缺資產

Bitcoin 的規則風險最低，但競爭把新進者的 k 壓到 1 以下。比特大陸的 S23 XP Hyd 達到 8.9 J/TH，售價每 TH 25.5 美元，11 月起出貨；旗艦效率從 2023 年 S21 的 17.5 J/TH 降到 8.9 J/TH，三年約 49%。在 2027–2028 年量產出貨的新進者，需要約 8 J/TH 或更好才站得住腳 估算。挑戰者正在離場：嘉楠公布 2026 年第二季營收 3,190 萬美元、毛損 2,930 萬美元，第三季指引僅 1,100–1,500 萬美元；Bitdeer 第三季對外銷售自有礦機僅 30 萬美元，集團毛利率 3.4%；Auradine 更名為 Velaura AI，轉向 AI 晶片；Core Scientific 取消了向 Block 旗下 Proto 部門訂購的約 15 EH/s 3 nm 礦機，認列 4,190 萬美元損失。

需求也在萎縮。11 月 9 日，hashprice 約為每 PH/s 每天 31.89 美元，至 2027 年 4 月的遠期曲線平均約 32.7 美元，手續費僅占區塊獎勵的 0.72%。以每 kWh 0.045 美元計，S23 XP Hyd 約 3.1 年回本 估算，接近預計在 2028 年左右的下一次減半。更重要的是電力的機會成本：AI 與高效能運算租約現在每簽約百萬瓦每年約賺 167–190 萬美元，以 80% 到 85% 的營業淨收入計，約為每百萬瓦挖礦毛利（約 56–90 萬美元）的 1.5 到 2.9 倍 [估算；兩者的百萬瓦基準不同]。Core Scientific 將在第四季停止挖礦；Bitfarms（現名 Keel）已關閉所有美國挖礦場址；IREN 一季從 AI 雲端賺了 2 億美元，從挖礦只賺 2,800 萬美元。**電力與資料中心容量才是資產；礦機是耗材。**

NRE 的帳同樣不留情面。前沿效率現在需要 3 nm 級製程（據二手來源，MicroBT 使用三星 SF3，Auradine 與 Proto 的晶片為 3 nm）。光罩約 1,000–2,000 萬美元，完整 NRE 3,000 萬–1 億美元或更多；以每 TH 20–25 美元、30% 毛利率計，每賣出 1 EH/s 約賺 600–750 萬美元毛利，所以要覆蓋 Bitdeer 規模的年度研發（約 1.1–1.6 億美元），每年需對外銷售約 20–25 EH/s，約占全網 2% 估算。結論：**新團隊不應進入商用 Bitcoin 礦機市場。** 仍有三種情況說得通：與自有的廉價電力垂直整合；家用與供暖礦機等利基形態（嘉楠也在推出家用供暖產品）；以及透過 IP 與設計服務參與既有業者的產品路線圖。

AI 訓練晶片：小團隊別做

訓練晶片的 k 最難掙得。在相同世代與精度下，Google 的 Ironwood 在晶片級 FP8 效率上只領先 B300 約 1.1 到 1.8 倍（Ironwood 的功耗為記者估計） 估算；常被引用的 TPU v1 論文中 30 到 80 倍的數字，是對比沒有 Tensor Core 的 K80 測得的。真正的槓桿是數字格式：從 FP8 改為 FP4，通常能在同一塊矽上獲得 2 到 3 倍的吞吐量，而輝達在這方面動作最快：它宣稱 Rubin 有 50 PF 的 NVFP4 推論算力，2026 年下半年量產。成本與供應門檻更高：3/2 nm 設計預算達 6,000 萬–4 億美元或更多；2026 年 CoWoS 產能約每月 10.6–13 萬片晶圓，據報台積電正考慮漲價最多 20%；以 HBM3E 每 GB 15.6 美元的合約價計，一顆 288 GB 加速器光是 HBM 就約 4,500 美元 估算。這個市場屬於博通式的與超大規模雲端業者共同開發（第 11 章）。結論：**小團隊不應做獨立的訓練晶片**；改做 IP、chiplet 或設計服務。

AI 推論晶片：以通用性換取 k，而且划算

推論是 ASIC 空間最大的地方，因為 k 可以用放棄通用性來換。Etched 宣稱其八晶片伺服器跑 Llama-70B 超過每秒 50 萬個 token，約為八張 H100 的 20 倍；Taalas 把模型權重固化在光罩 ROM 中，宣稱功耗低 10 倍、製造成本低 20 倍（兩者皆為 廠商宣稱）。以 SRAM 為核心的架構避開了 HBM 與 CoWoS，節點也較容易掌握：Taalas 使用台積電 6 nm，Groq 從 14 nm 轉到三星 4 nm。加密貨幣的分發對推論晶片沒有幫助，因為去中心化算力網路幾乎全跑在輝達上；切入點是新興雲端業者的採購經濟，以及中國龐大的國內推論市場：在那裡，國家資助的資料中心必須使用國產 AI 晶片，H200 進口正被限縮，北京也希望大型網路公司以國產晶片執行推論。結論：**值得做**，前提是有明確的客戶，並且對模型與架構的鎖定程度是刻意選擇的結果。它也是 PoUW 礦機晶片最好的第二市場。

ZK 與 FHE 加速器：ZK 避險，FHE 提早布局

GPU 已經追上了即時 ZK 證明：Succinct 的 SP1 Hypercube 在 16 張 RTX 5090 上，於 12 秒內證明了 99.7% 的 Ethereum 區塊。Cysic 宣稱其 ZK C1 晶片效率是 GPU 證明器的 10 到 100 倍，將於 2026 年出貨，但其需求很大程度來自它自己的代幣獎勵 廠商宣稱；我沒有找到 Aleo 謎題 ASIC 被用於真實 ZK 證明的公開證據。ZK 證明是整數且確定性的，形狀接近礦機晶片所做的事，但證明系統變化很快（SP1、RISC Zero、Halo2、Plonky2 等）。結論：**觀望避險**，做可程式化的 MSM、NTT 與雜湊引擎，先上 FPGA，再做 ASIC。

FHE 是最受硬體限制、上檔空間也最大的密碼學基元。Intel 的 Heracles 採用 Intel 3、197 mm²、176 W 與 48 GB HBM3，執行 FHE 運算比 24 核心 Xeon 快 1,074 到 5,547 倍，但 Intel 沒有商業化計畫，專案負責人也於 2025 年 12 月離職。Niobium 以 SemiFive 為設計夥伴（開發合約約 686 萬美元），在三星 8LPU 上打造晶片，已募得逾 2,300 萬美元；採光子路線的 Optalysys 募得 3,100 萬美元，並表示完整的商用晶片還要兩到三年；Zama 的開源 FPGA 設計在約 200 W 下達到每秒約 13,000 次可程式化自舉，這是任何 ASIC 都必須明顯超越的公開基準。結論：**提早布局，以輕資產驗證**，瞄準 2027–2029 年左右的窗口。需求更可能錨定在企業與政府的加密 AI，而非加密貨幣本身；而且 FHE 需要 HBM，所以其成本結構類似訓練晶片。

晶片類型	k 從何而來	需求與盤子	NRE 與門檻	規則或鎖定風險	第二市場	判斷
Pearl 類 PoUW 礦機晶片	拿掉 HBM、CoWoS 與通用單元：J/op 或許 3–10 倍 分析	礦工收入每年約 4.6–4.9 億美元，波動大	N7/N6 重複陣列約 1,000–3,000 萬美元 分析	非常高：協議決定數字格式與裝置白名單	AI 推論，若做成通用 INT8/FP8 GEMM	不做專用 INT7 晶片；做推論優先、可挖礦的晶片，或等待標準算術
Bitcoin SHA-256 礦機晶片	對比特大陸 k ≤ 1	每年約 115 億美元，商用市場由兩家公司把持	3 nm 級光罩 1,000–2,000 萬美元；完整 NRE 3,000 萬–1 億美元或更多	低（演算法穩定）；競爭與減半風險高	幾乎沒有（單一演算法）	新進者避開商用市場；只考慮自有電力、利基形態或 IP
AI 訓練晶片	同世代脈動陣列只有 1.1–1.8 倍；格式才是槓桿	最大（博通 2026 財年 AI 半導體營收約 580 億美元）	3/2 nm 設計 6,000 萬–4 億美元或更多；CoWoS 與 HBM	輝達的年度更新節奏	—	小團隊做 IP、chiplet 與設計服務，不做獨立晶片
AI 推論晶片	放棄通用性：宣稱 10–20 倍 廠商宣稱	大而分散；中國大陸的國內市場本身就很大	N6/N7–N4 的 SRAM 架構較易掌握	對模型與架構的鎖定	它就是主要市場	值得做：先簽下客戶，再選擇鎖定
ZK 加速器	宣稱為 GPU 的 10–100 倍 廠商宣稱	小，主要由代幣獎勵驅動	N7/N6 再到 N5；先上 FPGA	證明系統變化快	ZK 以外有限	觀望避險：可程式化 MSM 與 NTT 引擎
FHE 加速器	Xeon 的 1,074–5,547 倍（Heracles）	尚未成形；錨定在企業與政府	需要 HBM；成本結構接近訓練晶片	標準與生態系未定	加密運算、隱私 AI	提早布局，以輕資產驗證；2027–2029 年窗口

圖 07

五類晶片，五種答案

成本優勢 k 從何而來、規則改變時晶片能轉賣到哪裡，以及結論



資料來源: 作者對第 7、8 章的綜合整理；廠商數字依報告中的標示。

第 09 章

09

製程節點

製程節點：讓最大的終生成本來選擇

成本階梯：先進製程晶圓的價格是成熟製程的十倍

先看帳本。一片先進製程晶圓現在的價格約為成熟製程的十倍：台積電 N2 約 30,000 美元，N3 約 20,000 美元，N7 約 9,500 美元，N28 約 3,000 美元；三星 SF3 約 15,000 美元，比 N3 低約 25%；而據報中芯 7 nm 級的製造成本比台積電高 40% 到 50%。據報台積電將自 2027 年 1 月起再漲價 3% 到 6%，以 2 nm 與 3 nm 漲幅最大。光罩與設計成本的差異更大，各來源說法不一，所以下表兩者並列。

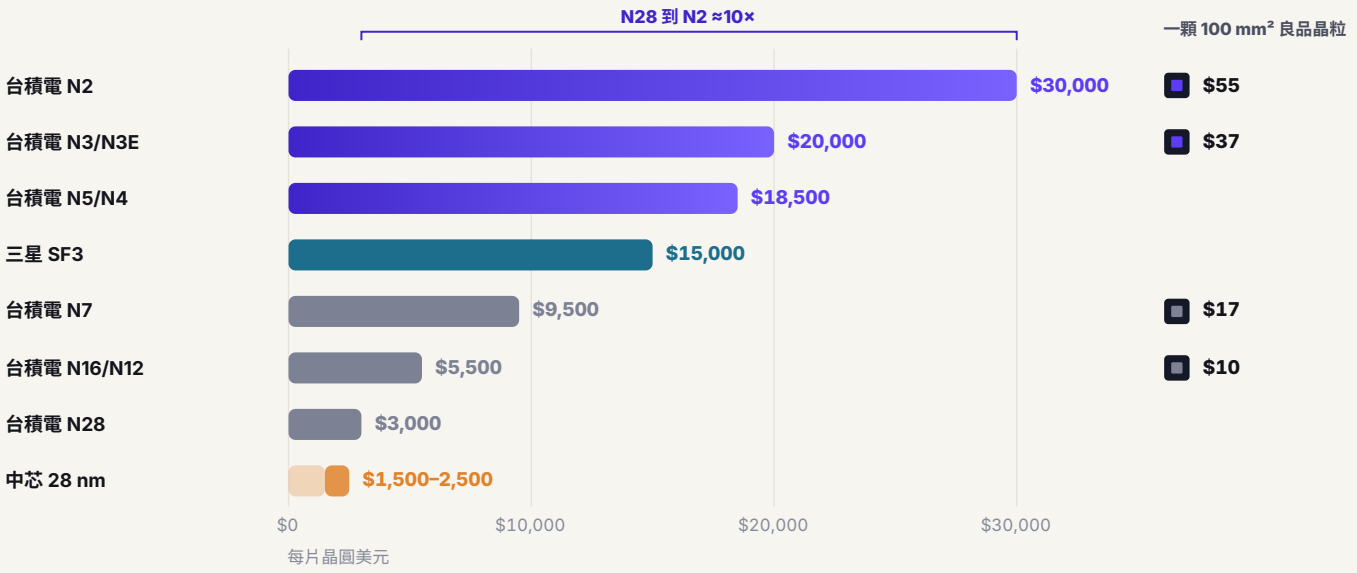
節點	晶圓價格（估計）	光罩組（模型值／指引區間）	設計預算（AnySilicon）	MPW（每個專案）
台積電 N2	約 30,000 美元	—	3/2 nm：6,000 萬–4 億美元或更多	—
台積電 N3/N3E	約 20,000 美元（18,000–27,000 美元）	1,500 萬美元／1,000–2,000 萬美元	同上	—
三星 SF3	約 15,000 美元（13,000–17,000 美元）	1,200 萬美元	—	—
台積電 N5/N4	約 18,500 美元（16,000–21,300 美元，信心度低）	650 萬美元／1,000–2,000 萬美元	5/4 nm：3,000 萬–2 億美元	—

節點	晶圓價格（估計）	光罩組（模型值／指引區間）	設計預算（AnySilicon）	MPW（每個專案）
台積電 N7	約 9,500 美元（8,100–10,900 美元）	350 萬美元／500–1,000 萬美元	7/6 nm：1,500 萬–1 億美元	商用 10 萬–50 萬美元
台積電 N16/N12	約 5,500 美元	180 萬美元	16/12 nm：600 萬–4,000 萬美元	學術每 mm² 約 35,000 美元
台積電 N28	約 3,000 美元	100 萬美元／100–300 萬美元	28/22 nm：300 萬–2,000 萬美元	商用 5 萬–15 萬美元；學術每 mm² 約 12,000 美元
中芯 28 nm	1,500–2,500 美元	—	—	—
中芯 7 nm 級（N+2/N+3）	比台積電高 40–50%	—	—	—

圖 08

一片先進製程晶圓的價格是成熟製程的十倍

各節點 300 mm 晶圓估計價格，以及良率 85% 時一顆 100 mm² 良品晶粒的成本



資料來源: Silicon Analysts 晶圓定價（估計值，N5 信心度低）、Wccftech（中芯）；晶粒成本為作者依假設良率計算。

再看物理。Horowitz 的經典量測顯示，一條可程式化指令約耗 70 pJ，而算術本身只耗幾 pJ：**算術便宜，開銷昂貴**，這正是脈動陣列與專用晶片存在的理由。特徵尺寸減半大致讓每次運算的能耗減半，但供電電壓已停滯在約 0.9–1.1 V。N2 晶圓比 N3 貴 50% 到 67%，所以除非密度提高超過約 1.5 倍，否則每顆電晶體的成本不降反升 估算：先進節點必須靠效率與效能來回本。以 100 mm² 晶粒、85% 良率計，每顆良品晶粒的成本在 N2 約 55 美元，N3 37 美元，N5 29–34 美元，N7 17 美元，N16 10 美元 [估算；良率為假設]。

依晶片類型與團隊選擇節點

我的原則是：**讓晶片終生成本中最大的一項來選擇節點。** 對全天候滿載運轉的運算晶片（挖礦、ZK），電費主導終生成本，所以演算法一旦穩定，就應轉到 N5/N4 與 N3/SF3；在演算法未定或資金不足時，先在成熟節點 MPW 上驗證。對訓練晶片，瓶頸是封裝與記憶體（HBM 與 CoWoS 約占 H100 物料成本的 63%），所以節點是次要的。對推論晶片，首要決策是記憶體架構：以 SRAM 為核心的設計可以停留在 N6/N7 到 N4，而 HBM 設計則承襲訓練晶片的成本結構。FHE 受記憶體頻寬限制，避不開 HBM。

晶片類型	新創或小團隊	規模化公司	中國大陸路徑	重點
矩陣乘法 PoUW 礦機晶片（SRAM 常駐，無 HBM）	在 28 nm 或 16/12 nm MPW 上做原型；首批量產用 N7/N6；演算法與收入穩定後用 N5/N4；50–150 mm² 晶粒，標準覆晶封裝	N3/N3E 或三星 SF3	中芯 N+1/N+2 可行（不需 HBM 或 CoWoS），每顆良品晶粒貴約 40–50%	能耗主導；協議規則是最大風險
SHA-256 礦機晶片	別追最先進製程；利基形態可用成熟節點	3 nm 級；既有業者從台積電 5 nm 轉向 2 nm、從三星 SF3 轉向 2 nm（二手來源）	難以匹敵先進節點的效率	電價與減半週期決定利潤率
AI 訓練晶片	不做獨立晶片：IP、chiplet、設計服務	N3P 再到 N2/A16；2–8 個 chiplet；及早確保 CoWoS 與 HBM	中芯 N+2/N+3 搭配國產 HBM（華為模式）；單晶片 FP8 約為輝達的 0.2–0.5 倍，以系統規模彌補	封裝與 HBM 是瓶頸
AI 推論晶片	以 SRAM 為核心或固化設計，N6/N7 或 N4/N5/SF4；只做 INT8、FP8 與 FP4	N3/N2 搭配 HBM（長上下文、混合專家），或多 chiplet SRAM	中芯 N+2 搭配 LPDDR 或 GDDR；HBM 級記憶體是卡脖子之處	架構鎖定的程度是核心決策
ZK 加速器	從 FPGA 或 16/12 nm MPW 起步；再到 N7/N6 與 N5	N5/N3	中芯 N+1/N+2 可行	整數且確定性；易於驗證
FHE 加速器	FPGA（對照開源基準）或 16/12 nm MPW；量產需要 HBM	N5/N3 搭配 HBM	受限於 HBM 的取得	決定速度的是記憶體頻寬，而不是算術

先進或成熟、四種晶圓代工廠，以及 chiplet

選項	主要優勢	主要劣勢	最適合
先進節點（N3/N2、SF3/SF2、Intel 18A）	每個完整節點大致讓每次運算能耗減半；高密度 SRAM	晶圓是成熟節點的 3–10 倍、光罩 5–15 倍、設計預算 10–20 倍；交期超過 50 週；N2 每顆電晶體成本可能上升	演算法穩定、全天候運轉的運算晶片；訓練晶片
成熟與中階節點（N7/N6、N16/12、N28）	光罩在百萬美元等級、MPW 便宜、迭代快、晶圓代工廠多（台積電、聯電、GlobalFoundries、中芯）	全天候滿載時效率缺乏競爭力	原型、利基市場、邊緣推論
台積電	最好的良率與生態系	價格最高；N2/N3 產能吃緊；CoWoS 排隊時間長	追求效率前沿、有量產承諾的團隊
三星晶圓代工	晶圓便宜約 20–25%（SF3 約 15,000 美元，N3 約 20,000 美元）；Groq 第二代等採用	晶圓代工業務虧損，目標 2027 年底損益兩平	對成本敏感的運算晶片
Intel Foundry	Heracles 等複雜晶片已在 Intel 3 上驗證	18A 沒有公開的外部定價或客戶資料；晶圓代工業務虧損	逐案評估生態系與支援
中國大陸的晶圓代工廠（中芯等）	貼近龐大的國內市場；28 nm 晶圓 1,500–2,500 美元	7 nm 級產能每月約 45,000–60,000 片，大部分由華為吸收；良率約為台積電的三分之一；成本高 40–50%；只有 DUV	面向國內市場的推論、挖礦與 ZK 晶片
Chiplet	突破光罩尺寸與良率限制；HBM 系統的標準做法（MI355X、Ironwood、Trainium3）	封裝成本較高且依賴 CoWoS；已知良品晶粒（KGD）測試增加成本	訓練與大型推論晶片；小型挖礦或 ZK 晶片不需要

第 10 章

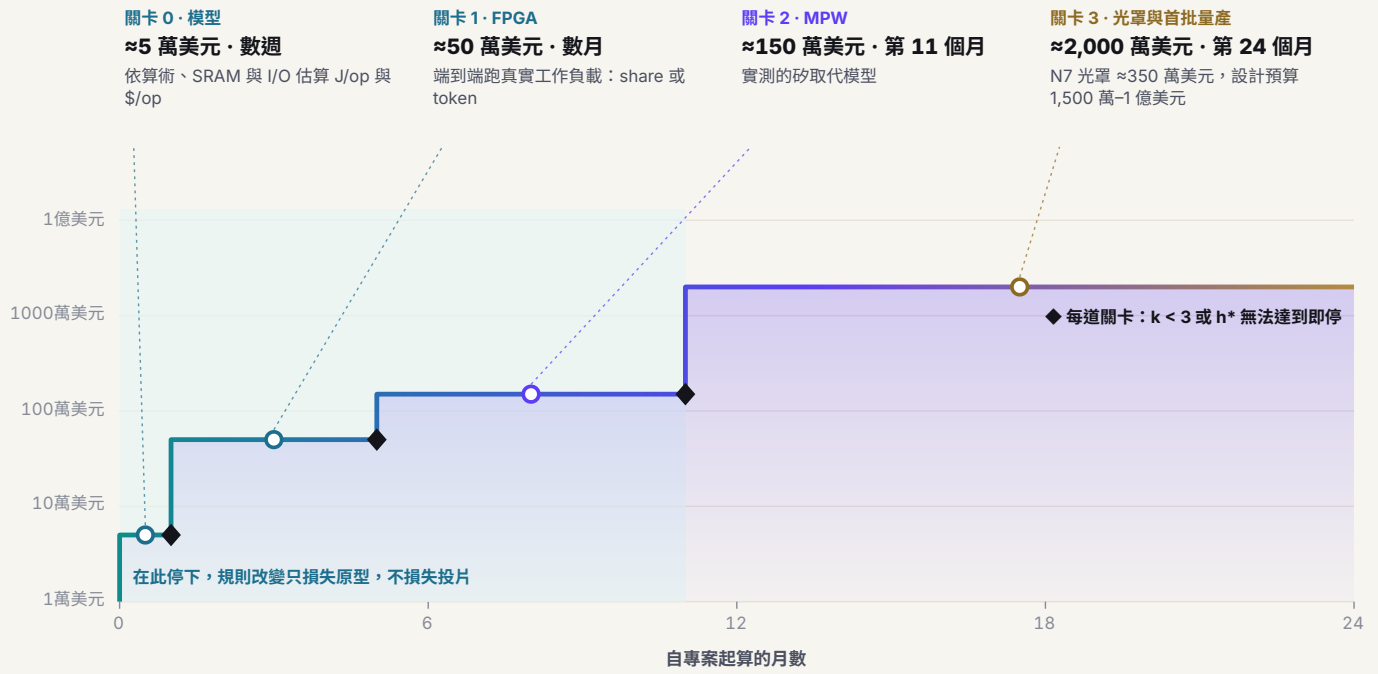
10 分階段預算 從模型到矽：第一顆晶片的分階段預算

先買證據，再買光罩

一顆全客製化晶片是一連串押注，每一注都比上一注大，而紀律在於先買證據，再買光罩。我使用四道關卡 分析。關卡 0 是模型：一份架構研究，依算術、SRAM 與 I/O 估計 J/op 與 $/op，並對照第 7 章的基準硬體；花費數週與數萬美元。關卡 1 是 FPGA 原型，端到端跑真實工作負載，挖出 share 或產生推論 token，證明資料路徑與協議整合；花費數個月與數十萬美元。關卡 2 是多專案晶圓：商用名額在 N28 約 50,000–150,000 美元，在 N7 約 100,000–500,000 美元，實測的矽取代模型的能耗估計。關卡 3 是完整光罩組與第一批量產：光罩在 N28 約 100 萬美元、N7 約 350 萬美元、N3 約 1,500 萬美元，而 7/6 nm 的設計預算為 1,500 萬–1 億美元。每道關卡都需要一個讓專案停下的數字，例如相對邊際硬體的 k 低於 3，或窗口內無法達到的回本算力 h*。

圖 09 **先買證據，再買光罩：第一顆晶片的分階段預算**

N7/N6 專案通過四道關卡的累計支出（美元），對數座標；每道關卡都有讓專案停下的數字



資料來源: 晶圓、MPW 與光罩價格同第 9 章（Silicon Analysts、AnySilicon、模型值）；關卡時程與支出為作者的示意性假設。

這道階梯很陡。在一個 N7/N6 專案中，前三道關卡合計約 150 萬美元、約十一個月；第四道的花費是其十倍以上 估算。所以順序比節點更重要：如果協議改了算術，或買家走了，停在關卡 2 的團隊損失的是一個原型的價格，而不是一次投片的價格。

每類晶片要花多少，以及什麼必須成立

專案	關卡 2（原型）	關卡 3（節點與設計預算）	一顆 100 mm² 良品晶粒	回本必須成立的條件
能挖礦的推論優先加速器	16/12 nm 或 N7 MPW，10 萬–50 萬美元	N6/N7，約 1,500 萬–3,000 萬美元 估算	N7 約 17 美元，未計封裝與記憶體	由已簽約的推論客戶承擔大部分 NRE；挖礦收入是額外收益，不是基本情境
專用 Pearl INT7 礦機（目前不建議）	28 nm MPW，5 萬–15 萬美元	N7/N6，約 2,000 萬美元	N7 約 17 美元	p = 1 時約 4.9 EH/s 運轉整整一年，或 p = 0.5 時 9.8 EH/s（第 7 章）
ZK 加速器	FPGA，再到 16/12 nm MPW	N7/N6，再到 N5	N16 約 10 美元，N7 約 17 美元	證明系統收斂到固定設計就能服務的 MSM 與 NTT 核心
FHE 加速器	FPGA，對照開源基準	N5/N3 搭配 HBM，3,000 萬美元或更多	由 HBM 與封裝主導	有大量採購加密 AI 的買家，而這樣的買家尚不存在

由此可得出兩個商業要點。第一，最便宜的效率來自架構：把運算元放在 SRAM 中、拿掉 HBM 與 CoWoS，在選定任何節點之前，就已去除 GPU 大部分的成本（約占 H100 物料成本的 63%）。第二，時間也是成本：新團隊從起步到量產約需 18 到 24 個月，先進製程交期超過 50 週，所以一個每隔幾個月就改一次算術的協議，可能在關卡 3 回本之前就讓晶片過時。

小團隊的三條規則

綜合這些數字，可得出三條規則 分析。第一，**在有具名買家或凍結的協議版本之前，停留在關卡 1 或 2**；代幣價格與算力都無法取代這兩者。第二，**先用架構買 k，再用節點買 k**：在單一工作負載上，N7 上的 SRAM 常駐陣列可以勝過 N3 上的通用晶片，而光罩成本只是其一小部分。第三，**在投片之前寫下回本算力或回本量，並註明 p**，並以鎖定的協議版本為里程碑付款定價，讓承擔規則風險的是客戶，而不是設計公司。

第 11 章

11 機會

機會在哪裡，以及我會怎麼做

客製化晶片：需求壓倒性來自 AI

2026 年客製化晶片的需求壓倒性來自 AI。博通 2026 財年第三季 AI 半導體營收 167 億美元，年增 221%，全年約 580 億美元，其中 73% 來自為六家客戶做的 XPU（依財報電話會議的自動逐字稿）。創意電子第二季營收年增 128%，其中 turnkey 量產營收成長 188%，毛利率 21.5%。世芯第一季營收依節點區分，3/2 nm 占 21%，7/5 nm 占 63%，12 nm 及以上占 16%。芯原 2026 年新簽訂單至 4 月底已達 82.4 億元人民幣（約 11.6 億美元），其中 91.37% 為 AI 算力。這個市場分三層：頂層是價值數十億美元的多年共同開發；中層是 7 nm 到 2 nm 的專案，NRE 從數百萬到逾億美元不等（中階節點 500 萬–3,000 萬美元，先進節點 3,000 萬–1 億美元或更多）；以及 NRE 50 萬–500 萬美元的成熟節點 ASIC 長尾。加密貨幣與挖礦客戶是小而具週期性的利基，但它們是今天為算力付費、速度最快、最不需許可的「第一個客戶」。

礦機晶片團隊最能移轉的能力——近閾值低電壓運作、大規模複製的運算陣列、千瓦級供電與散熱，以及快速的先進節點投片——正是推論晶片與 ZK、FHE 加速器所需要的。資本市場也為此定價：Velaura AI（前身為 Auradine）於 8 月以超過 10 億美元的估值募得 1.1 億美元。反例是嘉楠的邊緣 AI 晶片部門，2024 財年營收 90 萬美元，卻耗用 15% 的營業費用，於 2025 年 6 月關閉。差別在於獨立的市場通路，而不在於重複利用挖礦通路。

AI 開發：工時是大宗商品，價值在接縫處

在低端，AI 開發服務已經商品化：Clutch 上的典型費率為每小時 25–49 美元，在美國、加拿大等市場為 50–99 美元；一支區塊鏈開發團隊每月約 15,000 美元到 90,000 美元以上。賣工時沒有護城河。價值在領域之間的接縫：客製化晶片的 kernel 與編譯器、嵌入推論服務中的挖礦（Pearl 的 vLLM 外掛即為一例）、結合 TEE 與 ZK 抽查的可驗證推論，以及 Agent 的支付與身分。

AI × 加密貨幣系統：先簽下算力買家，再發代幣

對任何設計 AI 原生鏈或算力網路的人來說，2026 年的驗證工具箱已經成形。依每單位工作的成本由低到高排列：統計抽樣（Hyperbolic 的抽樣證明）、仲裁式委託（Gensyn 的 Verde，只需一位誠實驗證者，但要求逐位元精確執行）、TEE（接近原生速度，但須信任晶片廠商）、完全冗餘，以及通用 zkML。實務上的設計是分層的：以 TEE 或抽樣求低延遲，以爭議賽局或 ZK 抽查求最終性；2025 年 12 月的一篇論文模擬以 H100 機密運算搭配詐欺證明與隨機 ZK 抽查，達到中心化吞吐量的 99%，每次查詢的邊際成本為 0.07 美元。硬體哲學決定了安全性與分發：GPU 原生的 PoUW 起初由可租用的雲端 GPU 保護，所以攻擊成本與租用價格掛鉤，而 Qubic 顯示，建立在通用硬體上的工作量證明可能被外部激勵整批劫持。

成本與時間不是門檻。Pearl 從論文（2025 年 4 月）到主網約 12 個月，從 btcd 分叉而來，上線時就有全節點、錢包、輕客戶端與挖礦程式。多數 DeFi 稽核費用為 25,000–100,000 美元，企業或多鏈稽核 150,000–250,000 美元或更多，ZK 電路再多 80% 到 120%，而有真實價值面臨風險的專案每年編列 150,000–500,000 美元的資安預算。真正的門檻是分發與流動性。創辦人反映，Binance 曾要求上架以 0% 到 3.5%、據稱甚至 8% 的代幣供給作為條件（Binance 否認從上架中獲利）；Cointelegraph 檢視的六個採用「代幣借貸加買權」造市協議的專案全數下跌，Movement 的造市商在上架當天賣出約 3,800 萬美元的代幣。替代方案是鏈上流動性，例如 Hyperliquid 未在 Binance 上架就突破 100 億美元市值，其 HIP-3 永續合約市場的未平倉量在 6 月突破 32 億美元；以及透過大型交易所的公開發售，例如 Monad 透過 Coinbase 募得 2.69 億美元。高完全稀釋估值加上低流通量，是 2025–2026 年上線後下跌最明顯的預測指標。

代幣設計是系統設計的一部分。排放應跟隨付費需求，而不是走在它前面：本報告中補貼倍數最健康的網路，把獎勵綁在外部買家付費的工作上；最糟的則為背後空無一物的算力或質押付錢。一條實用的規則是在上線前公布網路第一、二、三年的目標補貼倍數，未達標時就削減排放 分析。

方向	誰買單，付費意願	窗口	關鍵能力	主要風險
能挖礦的推論優先加速器	新興雲端業者、私有部署、PoUW 網路	2027–2028 年（視 FP8 與 FP4 分叉而定）	INT8、FP8 與 FP4 GEMM；SRAM 架構；協議整合	協議准入、架構鎖定
SRAM 或固化推論晶片	新興雲端業者、中國大陸的資料中心、邊緣	現在	編譯器與模型適配；N6–N4 設計	模型變化太快
礦機晶片（利基或垂直整合）	擁有自有電力的礦工；家用與供暖礦機	現在，受減半與 hashprice 限制	低壓陣列、效率、量產供應鏈	既有業者的價格戰、電價
ZK 證明加速	證明者網路、rollup	等證明系統收斂	可程式化 MSM 與 NTT	需求取決於代幣獎勵
FHE 加速	企業與政府的加密 AI；隱私鏈	2027–2029 年	NTT、HBM 系統、密碼工程	需求尚未成形；銷售週期長
TEE 強化與可驗證推論	機密推論網路、DePIN	現在	具完整性的記憶體加密、獨立的證明信任根、ZK 抽查	依賴廠商生態系
AI 原生鏈或算力網路	推論買家、礦工、開發者	現在	驗證設計、排放設計、分發	上線後下跌、代幣流動性

我會走的三條路，各有第一步

如果必須選擇，我最多會走三條路，每條都有一小步，在投入資金之前先行驗證 分析。

- **路徑 A：推論優先、也能挖礦的加速器。** 第一步：為期四週的架構研究，針對 Pearl 的工作與 Transformer 推論，為 SRAM 常駐 INT8/FP8 GEMM 陣列對比 RTX 5090 與 H100 建立 J/op 與 $/op 模型，接著以百萬美元等級的 NRE 在 FPGA 或成熟節點 MPW 上驗證。
- **路徑 B：以加密貨幣為第一個客戶、AI 為第二市場的客製化晶片服務。** 第一步：把本報告的 NRE 與損益平衡模型，變成算力晶片專案的付費可行性研究，依里程碑付款，並以鎖定的協議版本驗收。
- **路徑 C：先簽下算力買家、再發代幣的 AI 原生網路。** 第一步：在任何代幣設計之前，與一位具名的推論買家共同撰寫一份設計說明，內容涵蓋分層驗證（TEE 加抽樣加 ZK 抽查）與廠商中立的標準算術。

第 12 章

12 觀察指標
觀察重點，2026 年 11 月至 2027 年

時間	觀察什麼	為什麼重要
隨時	Pearl 的 FP8 啟用高度	決定整數硬體與非輝達顯示卡是否仍被接納，以及鏈是否分裂
每月	Pearl 承載 AI 工作的區塊比例	檢驗「有用」是否正在成真的最佳單一指標
每月	推論供應商是否把挖礦收入回饋給客戶	付費需求與排放相遇：Pearl 需要的模式
每季	Bittensor 可驗證收入對比其排放	最大的有用工作網路是否正在縮小補貼缺口
每季	真正由 Agent 發起的 x402 流量比例	Agent 支付是否從訊號走向商業
2027 年 1 月	據報台積電漲價 3% 到 6%，以 2 nm 與 3 nm 漲幅最大	先進節點投片的成本
2027 年第一季	Pearl 導入 FP4（據創辦人 AMA 報導）	工作進一步轉向輝達最新的格式
2027 年底	三星晶圓代工的損益兩平目標	較便宜的第二供應來源能否保持健康
2028 年 4 月	Bitcoin 的下一次減半	SHA-256 礦工的盤子減半

第 13 章

13 該問的問題 你沒問但該問的問題

以下是我在把資金或晶片投入任何 AI × 加密貨幣專案之前會問的問題。

誰控制工作函數？ 如果一個小團隊可以在寫死的高度上更改算術，你的硬體壽命就由他們決定。請對方提供書面的穩定承諾，或設計有第二市場的硬體。

補貼倍數是多少？ 把排放（或市值）除以來自網路外部的付費收入。倍數超過 10，代表網路是在購買活動，而不是出售服務。

下一道關卡要花多少，什麼數字會讓你停下？ 一次多專案晶圓要花數萬到數十萬美元；一套光罩要花數百萬美元。在花錢之前先決定停損數字。

回本算力是多少，p 是多少？ 把 NRE 除以 R × (1 − 1/k) × T × p。如果答案占全網很大比例，這顆晶片押注的是規則，而不是矽。

這顆晶片的第二市場是什麼？ 如果協議分叉或代幣下跌，這塊矽還能賣到哪裡？GPU 撐過了 Ethereum 合併，因為它們有第二市場；單一演算法的 ASIC 則沒有。

價值落在代幣還是股權？ 2026 年賺錢的 AI × 加密貨幣公司，多半是做加密分發的股權公司；在募資之前，先決定你要建立的是兩者中的哪一個。

第一個付費客戶是誰？請說出名字。 本報告中每一個能持久的案例，從 Grass 到 Bittensor 的算力子網，都始於網路外部一位具名的買家。

以下是我希望透過技術交流與技術合作，與他人一同探索的領域：用於挖礦、AI 訓練與推論的客製化晶片，以及各類加速器；AI 開發；以及從鏈到節點到晶片的 AI × 加密貨幣系統。歡迎來信 i@tanshuai.com。

本報告的侷限

這是以截至 2026 年 11 月 13 日的公開文件為基礎的案頭研究。本版沒有做一手訪談，也沒有獨立量測。幾個關鍵數字屬於公司或廠商宣稱，例如 Aethir 的營收、Grass 的營收、Etched 與 Taalas 的效能，以及 Cysic 的效率；這些都已標明。Pearl 的鏈上指標來自一個獨立全節點與各礦池，且每小時都在變；我使用的是 11 月 13 日 07:13 UTC 前後的讀數，並給出同日區間。晶圓、光罩與設計成本是第三方估計與模型值，彼此並不一致；我列出的是區間。我的 ASIC 損益平衡計算與分階段預算使用示意性假設（k、T、p、NRE 與各關卡成本），讀者應換成自己的數字。



關於作者

譚帥是一位技術人與創業者，在晶片、硬體與系統軟體領域累積了二十多年的經驗，擁有 20 項已獲授權的專利。他有多年 fabless 晶片研發與管理經驗，包括加密貨幣礦機晶片的全客製化 ASIC 資料路徑設計，以及多媒體相機晶片，這也是本報告的視角：每次運算的能耗、每片晶圓的成本、協議允許你把什麼固化在矽中，以及誰來付錢。他的工作經歷橫跨矽谷、紐約、芝加哥、台灣、大灣區（深圳與香港）、越南與馬來西亞。如今他是一位 AI 研發者。

技術交流：i@tanshuai.com · tanshuai.com

說明與免責聲明

本報告是以截至 2026 年 11 月 13 日可取得的公開文件為基礎的獨立案頭研究。僅供資訊與學習之用，不構成投資或工程建議。本報告只討論技術與商業。價格、鏈上指標與協議規則都會變動；凡你所依賴的資訊，請對照原始來源查證。標為 廠商宣稱 、 估算 或 分析 的數字，應依其標記理解。加密資產價格波動極大。

© 2026 譚帥。歡迎在註明出處的前提下原樣分享本報告。

資料來源

全部於 2026 年 11 月 10 日至 11 月 13 日間存取。依章節分組。

Pearl：協議、程式碼與鏈上資料

- Komargodski 與 Weinstein，〈Proofs of Useful Work from Arbitrary Matrix Multiplication〉，arXiv 2504.09971：https://arxiv.org/abs/2504.09971
- Pearl Research Labs，INT 白皮書：https://pearlresearch.ai/research/int-whitepaper
- Pearl 原始碼：創世區塊：https://github.com/pearl-research-labs/pearl/blob/main/node/chaincfg/genesis.go ；共識參數與分叉高度：https://github.com/pearl-research-labs/pearl/blob/main/node/chaincfg/params.go ；算力計算：https://github.com/pearl-research-labs/pearl/blob/main/zk-pow/src/api/sanity_checks.rs ；加鹽種子分叉升級指南：https://github.com/pearl-research-labs/pearl/blob/main/docs/salted-seed-fork-upgrade-guide.md ；fp8-scheme 分支參數：https://github.com/pearl-research-labs/pearl/blob/fp8-scheme/node/chaincfg/params.go
- Pearl 改進提案：https://github.com/pearl-research-labs/pips ；PIP-3，浮點挖礦：https://github.com/pearl-research-labs/pips/blob/main/PIPS/pip-0003.md
- prlstats（獨立全節點）：網路：https://prlstats.com/api/network ；時間序列：https://prlstats.com/api/series ；首頁與礦工收入模型：https://prlstats.com/api/home ；已挖出供給：https://prlstats.com/api/mined ；礦池：https://prlstats.com/api/pools ；持幣者：https://prlstats.com/api/holders ；硬體與開銷假設：https://prlstats.com/api/assumptions
- Kryptex Pool：Pearl 網路：https://pool.kryptex.com/prl/about-coin ；算力：https://pool.kryptex.com/prl/hashrate ；RTX 5090：https://pool.kryptex.com/de/device/gpu/nvidia/nvidia-geforce-rtx-5090 ；RTX 4090：https://pool.kryptex.com/device/gpu/nvidia/nvidia-geforce-rtx-4090 ；〈Pearl FP8 fork〉：https://pool.kryptex.com/articles/pearl-fp8-fork-en
- CoinGecko，Pearl：https://api.coingecko.com/api/v3/coins/pearl-2 ；https://www.coingecko.com/en/coins/pearl-research ；價格歷史：https://api.coingecko.com/api/v3/coins/pearl-2/market_chart?vs_currency=usd&days=365&interval=daily ；「Perle」代號搜尋：https://api.coingecko.com/api/v3/search?query=perle
- SimeonOnSecurity，〈Mining Pearl (PRL) in 2026〉：https://simeononsecurity.com/articles/pearl-prl-mining-guide-2026/
- Hashrate Index，〈Pearl (PRL): Inside the AI-Compute Cryptocurrency〉，2026 年 6 月 2 日：https://hashrateindex.com/blog/pearl-prl-ai-compute-cryptocurrency/
- Tom's Hardware，〈New AI compute cryptocurrency Pearl sparks a GPU mining rush, but profitability is sliding〉：https://www.tomshardware.com/tech-industry/cryptomining/new-ai-compute-cryptocurrency-pearl-sparks-a-gpu-mining-rush-but-profitability-is-sliding
- Together AI，與 Pearl Research Labs 的合作：https://together.ai/blog/together-ai-partners-with-pearl-research-labs ；模型頁面：https://together.ai/models/gemma-4-31b-it-pearl
- Basu，Pearl 挖礦實例普查，arXiv 2606.04819：https://arxiv.org/html/2606.04819v2
- Blockworks，0xResearch 電子報，2026 年 10 月 28 日：https://blockworks.com/newsletter/0xresearch/issue/post_daf0d74a-2bf4-41e4-86d3-2a1275475a24
- Datawallet，〈Pearl Explained〉：https://www.datawallet.com/crypto/pearl-explained
- Coingabbar 關於 TheMarker 報導 Pearl Research Labs 融資：https://www.coingabbar.com/en/pearl-research-labs-funding-130m-stealth-round-themarker

有用工作鏈與歷史

- Grothe 等，Gridcoin 安全分析，USENIX WOOT 2017：https://www.usenix.org/system/files/conference/woot17/woot17-paper-grothe.pdf
- 學習證明偽造，arXiv 2208.03567：https://arxiv.org/abs/2208.03567
- hoge.gg，去中心化推論中的驗證與信任：https://hoge.gg/decentralized-inference-2026-verification-trust/ ；Bittensor 收入與國庫：https://hoge.gg/bittensor-quantum-wallet-revenue-tao-treasury-2026/
- Kaspa：kHeavyHash 矩陣程式碼：https://github.com/kaspanet/rusty-kaspa/blob/master/consensus/pow/src/matrix.rs ；啟動：https://coinranking.com/coin/V8GxkwWow+kaspa-kas/about ；IceRiver KS1/KS2 發表：https://www.iceriver.io/2023/03/14/1677644580/ ；從 GPU 到 ASIC 的歷史：https://captainmining.com/blogs/crypto-news/the-evolution-of-kaspa-mining-from-gpus-to-asic-powerhouses ；GPU 算力：https://coincalculators.io/algorithms/kheavyhash ；KS7：https://www.asicminervalue.com/miners/bitmain/antminer-ks7-40th ；網路：https://minerstat.com/coin/kas ；2024 年的 1 EH/s：https://ourcryptotalk.com/news/kaspa-reaches-1-ehs-in-hashrate ；Crescendo：https://ourcryptotalk.com/news/kaspa-crescendo-live
- Aleo：主網 FAQ：https://aleo.org/post/aleo-mainnet-faq/ ；去中心化證明：https://aleo.org/post/decentralized-proving-advantages/ ；ASIC：https://whattomine.com/coins/432-aleo-zksnark/asics ；Blockworks，〈State of Aleo Q3 2025〉：https://app.blockworks.com/report/state-of-aleo-q3-2025 ；ARC-46：https://chaincatcher.com/en/article/2144326
- Qubic：The Block 關於 Monero 重組：https://www.theblock.co/post/366535/monero-faces-chain-reorganization-fears-after-qubic-says-it-controls-51-of-hashrate ；Halborn：https://www.halborn.com/blog/post/explained-the-monero-51-percent-attack-august-2025 ；Dogecoin 挖礦：https://hackernoon.com/qubic-is-now-mining-dogecoin-on-its-ai-compute-infrastructure ；CoinGecko：https://www.coingecko.com/en/coins/qubic
- Bittensor 共識文件：https://www.bittensor.com/llms.mdx/docs/internals/consensus/content.md ；FalconX，〈State of Bittensor〉：https://www.falconx.io/newsroom/state-of-bittensor-subnet-adoption-trends-network-mechanics-and-covenants-departure

- Primecoin：https://en.wikipedia.org/wiki/Primecoin ；Blockworks，〈State of Filecoin Q3 2025〉：https://app.blockworks.com/report/state-of-filecoin-q3-2025
- Monero 與抗 ASIC 分叉：https://lbry.com/news/forking-for-asic-resistance ；Sia 分叉：https://hotfix.coindesk.com/markets/2018/11/01/sia-completes-hard-fork-as-bricked-miners-form-rival-blockchain ；Obelisk 價格：https://www.cryptoglobe.com/latest/2018/11/obelisk-hardware-skyrockets-in-selling-price-after-sia-hard-fork/ ；合併後的礦工：https://hotfix.coindesk.com/business/2022/11/11/ex-ethereum-miners-token-hop-to-stay-alive-after-the-merge

AI × 加密貨幣各領域

- DefiLlama：Render：https://defillama.com/protocol/render-network-bme ；Livepeer：https://defillama.com/protocol/livepeer
- Cointelegraph 關於 Messari 的 DePIN 收入：https://cointelegraph.com/news/depin-revenues-grow-despite-token-losses
- Aethir，2025 年回顧：https://aethir.com/blog-posts/aethirs-2025-wrap-up-decentralized-gpu-cloud-milestones
- CoinGecko，AI 類別：https://www.coingecko.com/en/categories/artificial-intelligence
- Akash，H100 租用價格：https://akash.network/the-bid/h100-rental-price-2026-cost-per-hour/ ；2026 年第一季報告：https://akash.network/blog/akash-network-q1-2026-report/
- io.net，800 萬美元交易與每日 token 量：https://lifestyle.kbew98country.com/story/271004/io-net-to-burn-up-to-12m-tokens-as-network-closes-8m-deal-and-hits-4-billion-daily-ai-tokens/
- DCD，Axe Compute 合約：https://www.datacenterdynamics.com/en/news/axe-compute-secures-15bn-compute-contract-with-unnamed-customer/
- Pluralis-8B：https://www.alphaxiv.org/abs/2607.13332.md ；Nous Research，Psyche：https://nousresearch.com/the-next-phase-of-psyche ；Implicator 關於 INTELLECT-3：https://www.implicator.ai/prime-intellects-intellect-3-open-source-ambition-meets-centralized-reality/
- SiliconANGLE，Prime Intellect 融資：https://siliconangle.com/2026/07/08/prime-intellect-raises-130m-1b-valuation-ai-training-platform/ ；The Block，Venice：https://www.theblock.co/post/406934 ；RuntimeWire，Nous 融資：https://runtimewire.com/article/nous-research-75-million-round-1-5-billion-valuation
- ownyourmind，Gensyn：https://ownyourmind.ai/projects/gensyn/ ；Phemex，Ritual（僅見於標題）：https://phemex.com/news/article/ritual-launches-ai-layer-1-mainnet-and-ritual-token-price-dives-72-from-high-101259
- 機密運算開銷，arXiv 2409.03992：https://arxiv.org/abs/2409.03992v2 ；Phala 2025 年報告：https://phala.com/posts/phala-2025-report ；TEE.fail：https://thehackernews.com/2025/10/new-teefail-side-channel-attack.html ；DeepProve，IACR ePrint 2026/1112：https://eprint.iacr.org/2026/1112
- TRM Labs，衡量 AI Agent 支付：https://www.trmlabs.com/trm-tech-blog/whos-actually-paying-measuring-ai-agent-payments-onchain ；Forkast 關於 x402 Foundation：https://forkast.news/the-x402-foundation-activated-a-27-year-old-internet-code-200-million-transactions-later-the-real-volume-is-still-tiny/ ；The Block，Tempo 主網：https://www.theblock.co/amp/post/394131/tempo-mainnet-goes-live-with-machine-payments-protocol-for-agents ；BlockEden 關於 Virtuals 的 aGDP：https://blockeden.xyz/blog/2026/04/21/agdp-agent-gdp-virtuals-protocol-ai-blockchain-valuation-primitive-tvl-displacement/ ；The Block 關於 ElizaOS：https://theblock.co/post/410774/eliza-labs-native-token-dead
- Dealroom，Grass 收入：https://dealroom.co/news/157794-grass-backed-by-multicoin-projects-75m-in-2026-data-revenue/ ；CryptoSlate，Fetch.ai 與 Ocean：https://cryptoslate.com/cryptos-flagship-ai-pact-fracture-fetch-sues-ocean-over-263m-fet-community-sales/ ；Fortune 關於 World：https://fortune.com/2026/06/01/internet-according-to-sam-altman-seeing-orb/
- Galaxy，加密貨幣創投：https://www.galaxy.com/insights/research/crypto-blockchain-venture-capital-q3 ；Crypto Briefing（僅見於標題）：https://cryptobriefing.com/crypto-vc-investment-q3-2026-galaxy/ ；Blockhead 關於 Tiger Research：https://www.blockhead.co/2026/10/14/bitcoin-rose-43-in-q3-crypto-venture-funding-did-not-follow/ ；ForkLog 關於 2025 年代幣發行：https://forklog.com/en/85-of-tokens-launched-in-2025-fell-below-initial-prices/

ASIC 經濟學與晶片類型

- Hashrate Index，2026 年 11 月 9 日綜覽：https://hashrateindex.com/blog/hashrate-index-roundup-november-9-2026/
- AnySilicon，2026 年各節點 ASIC 設計成本：https://anysilicon.com/news/how-much-does-asic-design-cost-in-2026-real-price-ranges-by-process-node/ ；Silicon Analysts，fabless 投片成本指南：https://siliconanalysts.com/analysis/fabless-startup-tapeout-cost-guide ；市場資料：https://siliconanalysts.com/market-data
- MillionMiner，比特大陸 S23 XP Hyd：https://millionminer.com/news/bitmain-wdms-2026-s23-xp-hyd-launch
- Khattak 與 Mikaitis，Tensor Core 中的 FP8 累加，arXiv 2512.07004：https://arxiv.org/html/2512.07004v2
- 嘉楠，2026 年第二季財報：https://finviz.com/news/389337/canaan-inc-reports-unaudited-second-quarter-2026-financial-results ；Bitdeer，2026 年第三季財報：https://greenstocknews.com/news/nasdaq/btdr/bitdeer-reports-unaudited-third-quarter-2026-results-record-revenue-of-us-320-7-million-adjusted-ebitda-up-173-to-us-69-6-million
- TheEnergyMag：Velaura AI：https://theenergymag.com/news/market-news/velaura-ai-series-a-bitcoin-pivot ；Core Scientific 與 Block：https://theenergymag.com/news/2026-07-29/core-scientific-exit-block-bitcoin-deal-ai ；AI 租約經濟：https://theenergymag.com/news/2026-08-06/miner-weekly-ai-pumpability-out-fuel
- Blockworks，Cipher 與 Fluidstack：https://blockworks.co/news/cipher-mining-inks-3b-ai-hosting-deal-with-fluidstack ；Cointelegraph，Core Scientific：https://cointelegraph.com/news/core-scientific-to-quit-bitcoin-mining-by-year-end-as-ai-business-surges ；ForkLog，Bitfarms：https://forklog.com/en/former-bitfarms-shuts-down-all-mining-sites-in-the-us/ ；IREN，FY27 第一季財報：https://globenewswire.com/news-release/2026/11/05/3397020/0/en/iren-reports-q1-fy27-results.html
- Spark，Bitcoin ASIC 市場集中度：https://www.spark.money/research/bitcoin-asic-manufacturer-market-concentration

- Google，TPU7x 文件：https://docs.cloud.google.com/tpu/docs/tpu7x?hl=es ；The Register，Ironwood：https://www.theregister.com/2025/04/10/googles_7thgen_ironwood_tpus_debut/ ；SemiAnalysis，B300：https://inferencex.semianalysis.com/chips/b300 ；TPU v1 論文，arXiv 1704.04760：https://arxiv.org/abs/1704.04760 ；Glenn Lockwood，MI355X：https://glennklockwood.com/garden/processors/mi355x
- Tom's Hardware，Vera Rubin：https://www.tomshardware.com/pc-components/gpus/nvidia-launches-vera-rubin-nvl72-ai-supercomputer-at-ces-promises-up-to-5x-greater-inference-performance-and-10x-lower-cost-per-token-than-blackwell-coming-2h-2026 ；TrendForce，CoWoS 定價：https://trendforce.com/news/2026/10/27/news-tsmc-reportedly-eyes-20-cowos-price-hike-skips-equipment-price-renegotiations-amid-ai-demand-surge
- Menon Lab，AI 推論加速器比較：https://themenonlab.blog/blog/ai-inference-accelerators-compared ；Introl，GPU 以外的 AI 加速器：https://introl.com/blog/ai-accelerators-beyond-gpus-tpu-trainium-gaudi-cerebras-2025
- StratNews（Reuters），國家資助資料中心使用國產 AI 晶片：https://stratnewsglobal.com/team-sng/china-orders-state-funded-data-centres-to-use-domestic-ai-chips/ ；TNW，H200 進口：https://thenextweb.com/news/nvidia-h200-chips-hong-kong-china-import-approval
- Succinct，16 張 GPU 上的即時證明：https://blog.succinct.xyz/real-time-proving-16-gpus/ ；Cysic ZK ASIC 產品：https://cysic-docs.pages.dev/hardware-products/zk-asic-products
- Tom's Hardware，Intel Heracles：https://www.tomshardware.com/tech-industry/cyber-security/intels-heracles-chip-computes-fully-encrypted-data-without-decrypting-it-chip-is-1-074-to-5-547-times-faster-than-a-24-core-intel-xeon-in-fhe-math-operations ；IEEE Spectrum：https://spectrum.ieee.org/fhe-intel ；Evertiq，Niobium 與 SemiFive：https://evertiq.com/design/2026-02-20-semifive-secures-design-win-with-niobium-for-fhe-accelerator ；The Quantum Insider，Niobium 融資：https://thequantuminsider.com/2025/12/03/niobium-23m-fhe-funding/ ；Optica OPN，Optalysys：https://www.optica-opn.org/home/industry/2026/february/optalysys_raises_us_$31_million_to_push_photonics_computing_toward_cloud_infrastructure/ ；Zama，FPGA 上的 HPU：https://www.zama.org/post/announcing-hpu-on-fpga-the-first-open-source-hardware-accelerator-for-fhe

製程節點

- Silicon Analysts，晶圓定價：https://siliconanalysts.com/data/wafer-pricing
- Tom's Hardware，台積電 A16 定價傳聞：https://www.tomshardware.com/tech-industry/semiconductors/tsmc-could-charge-up-to-usd45-000-for-1-6nm-wafers-rumors-allege-a-50-percent-increase-in-pricing-over-prior-gen-wafers ；Wccftech，中芯定價：https://wccftech.com/smic-5nm-chip-prices-up-to-50-percent-more-expensive/amp/
- EUROPRACTICE，台積電 2026 年 MPW 時程：https://europractice-ic.com/wp-content/uploads/2025/11/TSMC-Europractice-MPW-schedule-2026.pdf
- Horowitz，〈Computing's Energy Problem〉，ISSCC 2014：https://www.Gwern.net/doc/cs/hardware/2014-horowitz-2.pdf
- Tom's Hardware，華為昇騰路線圖：https://www.tomshardware.com/tech-industry/artificial-intelligence/huawei-ascend-npu-roadmap-examined-company-targets-4-zettaflops-fp4-performance-by-2028-amid-manufacturing-constraints ；The Substrate，中國 AI 晶片供應鏈：https://www.the-substrate.net/p/where-chinas-ai-chip-supply-chain ；Tom's Hardware，Trainium3：https://www.tomshardware.com/tech-industry/artificial-intelligence/amazon-launches-trainium3-ai-accelerator-competing-directly-against-blackwell-ultra-in-fp8-performance-new-trn3-gen2-ultraserver-takes-vertical-scaling-notes-from-nvidias-playbook

機會與上線經濟

- Webull（Benzinga），博通財報電話會議：https://www.webull.com/news/15511095937917952 ；Quartr，創意電子 2026 年第二季：https://quartr.com/events/global-unichip-corp-3443-q2-2026_F9×6NJQY ；Taiwan News，世芯：https://www.taiwannews.com.tw/news/6370946 ；Design & Reuse，芯原：https://www.design-reuse.com/news/202530457-surge-in-custom-chip-business-propels-verisilicon-s-q1-revenue-to-double-with-new-orders-skyrocketing-to-8-2-billion-yuan-increased-r-d-investment-leads-to-wider-net-loss-earnings-insight/ ；The Block，嘉楠的 AI 部門：https://www.theblock.co/post/359250/crypto-miner-canaan-to-shutter-non-core-ai-semiconductor-business-unit-amid-strategic-realignment
- Clutch，AI 開發定價：https://clutch.co/developers/artificial-intelligence/pricing ；PixelPlex，區塊鏈開發成本：https://pixelplex.io/blog/blockchain-development-cost/
- Hyperbolic，抽樣證明：https://hyperbolic.ai/blog/deep-dive-into-hyperbolic-proof-of-sampling ；Gensyn，Verde：https://www.gensyn.ai/research/verde-a-verification-system-for-machine-learning-over-untrusted-nodes ；分層驗證，arXiv 2512.20176：https://arxiv.org/abs/2512.20176v1
- Sherlock，2026 年稽核定價參考：https://sherlock.xyz/post/smart-contract-audit-pricing-a-market-reference-for-2026
- Blockworks，Binance 上架標準：https://blockworks.com/news/binance-listing-standards-scrutiny ；Cointelegraph，造市協議：https://cointelegraph.com/magazine/market-maker-deals-quietly-killing-crypto-projects ；Blockworks，Movement：https://blockworks.co/news/movement-rushi-manche-suspension-market-maker-web3port ；Nansen，HIP-3：https://nansen.ai/post/what-is-hip-3-hyperliquid ；The Block，Monad：https://www.theblock.co/post/380094/monad-mainnet-launches

有用工作量證明 · 加密貨幣 × 矽

算力即共識

2026 年的 AI × 加密貨幣 × 晶片，從 Pearl 的有用工作量證明談起

本報告的每個關鍵數字都附有來源與日期。作者自行推導的數字標為估算；僅由賣方公布的數字標為廠商宣稱。本報告只討論技術與商業。

譚帥

技術人與創業者 · AI 研發者

tanshuai.com · i@tanshuai.com

公開版 · 資料截至 2026 年 11 月 13 日

