Forskningsnotat · November 2026

# Beräkningskraft som konsensus

## AI × krypto × chip 2026, med Pearl som utgångspunkt

Pearl · Nyttigt arbete · DePIN och agenter · ASIC-ekonomi · Processnoder · Budgetar i steg

**Tan Shuai**
tanshuai.com · i@tanshuai.com



SLUTSATSEN

# Teoremet håller; incitamentet gör det inte

## 01 Pearl fungerar som teknik, men ännu inte som nyttigt arbete

Omkring 90 EH/s heltalsmatrismultiplikation säkrar kedjan, men bara omkring 1 % av blocken bär verkligt AI-arbete.

## 02 Betald efterfrågan finns i inferens, data och integritet

Bittensor omkring 70 miljoner dollar om året i verifierbara intäkter, Grass 17 miljoner dollar första halvåret 2026, TEE i produktion; agentbetalningar omkring 5 000–11 000 dollar i månaden.

## 03 En ASIC lönar sig bara med stor pott, stabila regler och en andra marknad

Vinsttaket är R × (1 − 1/k). I dag erbjuder inget nätverk alla tre analys.

**≈90 EH/s**

Pearl den 13 november 2026: heltalskapaciteten hos omkring 122 000 H100

**≈1 %**

av Pearls block bär verkligt AI-arbete (Blockworks)

**4–11×**

Bittensors emissioner mot dess verifierbara intäkter

# AI × krypto i sex sektorer: var betald efterfrågan är verklig

### Kedjor för nyttigt arbete — 01

VERKLIG MEN LITEN

**≈70 mn $ om året**

Bittensors verifierbara externa intäkter

**Signal:** emissioner 4–11× intäkterna; Pearl ≈1 % AI-block

**Mekanismerna fungerar; nyttan kräver betalare**

### Decentraliserad beräkning — 02

VERKLIG MEN LITEN

**2,35 mn $ om året**

Renders avgifter i kedjan, de största verifierbara

**Signal:** marknadsvärde ≈360× avgifterna

**Mest vidareförsäljning av standardinferens**

### Träning och inferens — 03

VINST I BOLAGEN

**över 100 mn $ om året**

Prime Intellect, ett aktiebolag på centraliserade GPU:er

**Signal:** Gensyns huvudnät för träning ej i drift

**Framstegen är verkliga; vinsten går till ägarna**

### Verifierbar AI — 04

TIDIGT

**398**

betalande användare av Phalas TEE-moln, slutet av 2025

**Signal:** ingen redovisad betald zkML

**TEE i produktion; zkML tidigt**

### Agentbetalningar — 05

FÖRE EFTERFRÅGAN

**5 000–11 000 $/mån**

x402-betalningar som agenter faktiskt initierat

**Signal:** ≈200 mn transaktioner, mest signalering

**Rälsen kom först; efterfrågan har inte kommit**

### Datanätverk — 06

VERKLIGA KÖPARE

**17 mn $**

Grass dataintäkter, första halvåret 2026 (egen uppgift)

**Signal:** marknadsvärde ≈10× årstakten

**En av få sektorer med verkliga köpare**

> Subventioner är bränsle för en kallstart, inte en affärsmodell. Kryptot sköter distribution och avräkning; bolagen tar vinsterna, åtminstone 2026.

# En MAC-operation är en hash

## Från teorem till huvudnät

Komargodski och Weinstein (april 2025): ett bevis på nyttigt arbete för varje matrisprodukt med 1 + o(1) i merkostnad. Pearls huvudnät startade den 27 april 2026.

## Hur det fungerar

Miners multiplicerar brusiga matriser, hashar varje rutas ackumulator till en lott och bevisar den vinnande rutan med ett Plonky2-bevis under 60 KB.

## Enheten

1 H är en krediterad INT7 × INT7 → INT32-MAC: en blockkedjas säkerhetsbudget prissatt i tensorgenomströmning.

PEARL DEN 13 NOVEMBER 2026

**89,77 EH/s**

nätverkets hashkraft (oberoende fullnod)

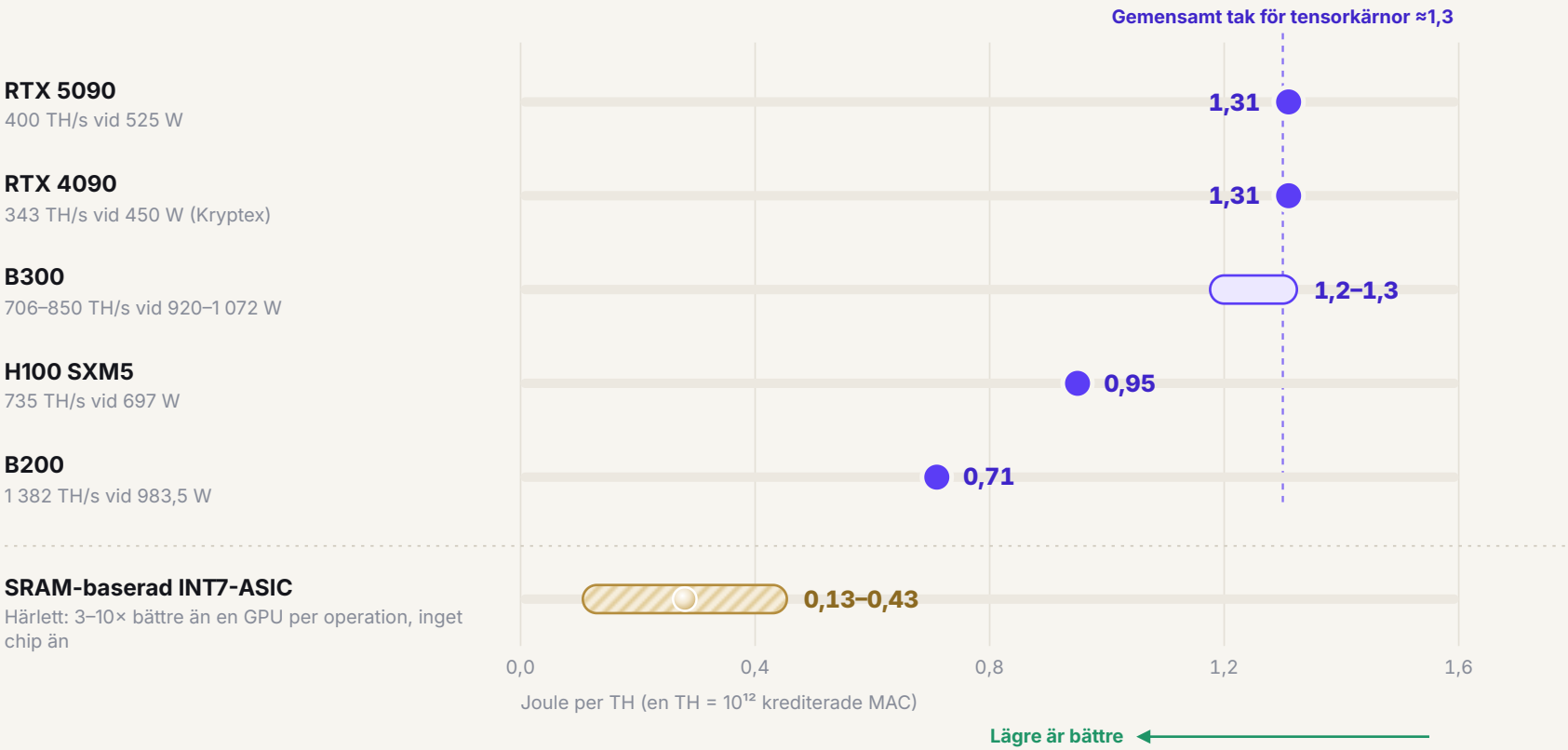
**≈500 mn $**

marknadsvärde; fullt utspätt omkring 2,8 miljarder dollar

**+78 %**

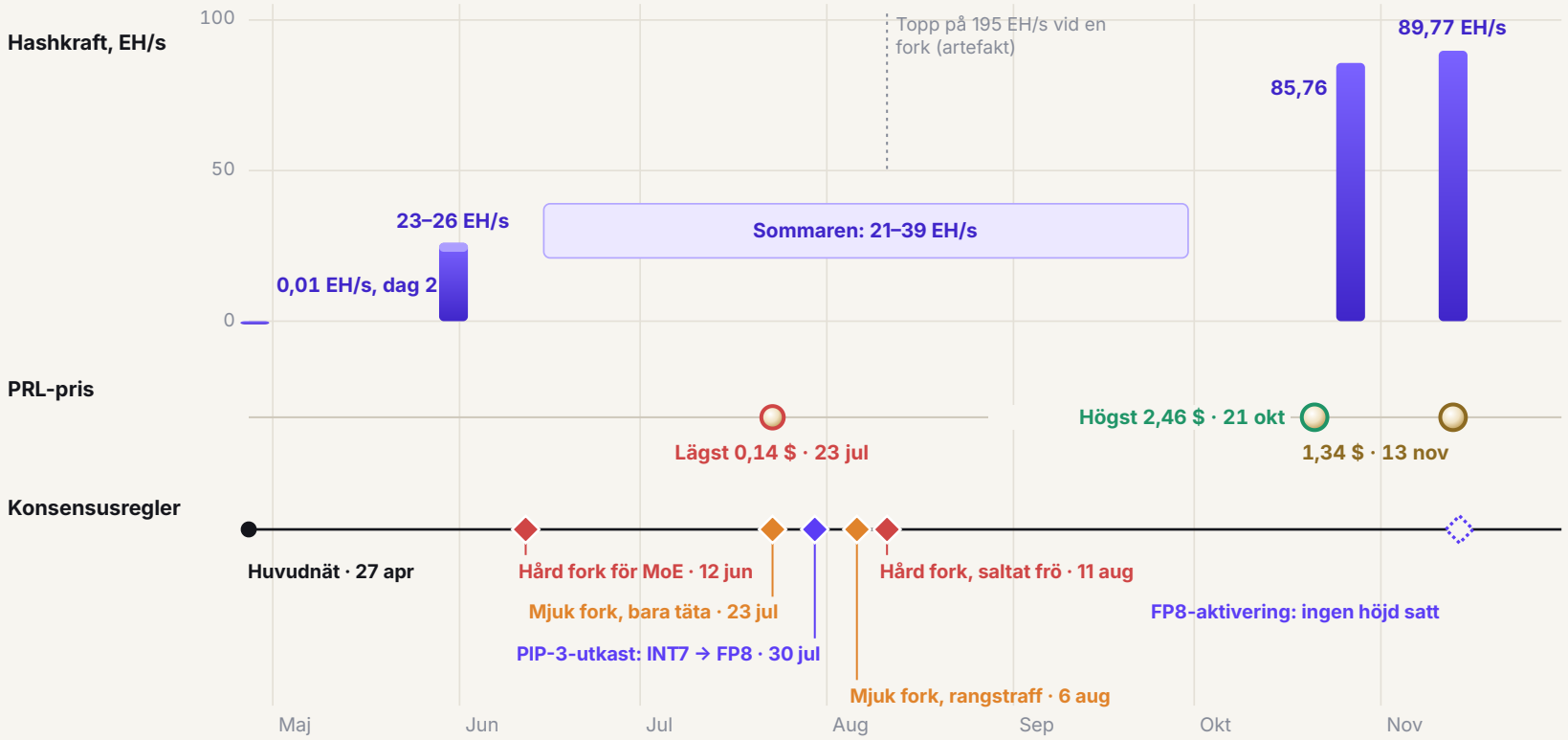
nytt utbud under de kommande 12 månaderna

# På Pearls heltalsarbete delar GPU:er samma energitak




> Spelkort och B300 möts vid omkring 1,3 J/TH; även B200 når bara 0,71. Ett chip som bara multiplicerar 7-bitars heltal ur SRAM skulle rimligen kunna bli 3–10 gånger bättre analys.

# Hashkraften följer priset; reglerna ändras hela tiden




Omkring 120 miljoner mynt, 32 % av dagens utbud, utvanns under de första sex dagarna. Ett RTX 5090 tjänar nu omkring 5–6 dollar om dagen; att hyra kort bara för att utvinna går med förlust.

# Teoremet håller; incitamentet gör det inte

VAD NYTTIGT ARBETE KOSTAR

## Inferenssidan: liten merkostnad

Pearl rapporterar 5,08 % längre tid för Llama 70B på fyra H200; ett oberoende test mätte 9,2 % lägre genomströmning på en Hopper-GPU.

VAD NYTTIGT ARBETE TJÄNAR

## Miningsidan: för lite hashkraft

Ett kort som kör inferens utvinner med omkring 27 % av en dedikerad miner vid prefill, 5,4 % vid chatt, omkring 1 % när avkodning dominerar.

**Så rationella miners multiplicerar slumpmatriser. Nyttan är ett kommersiellt problem utanför kedjan: någon måste betala för inferensen.**

# Fyra forkar på två månader, och FP8 härnäst

**12 juni**
Hård fork för mixture-of-experts (block 71 935)

**23 juli**
Mjuk fork för enbart täta modeller (block 91 630)

**6 augusti**
Mjuk fork med rangstraff: vissa uppsättningar förlorar 50–87,5 % av effektiv hashkraft

**11 augusti**
Hård fork med saltat frö: gamla miners ger bara ogiltiga andelar

**Ej satt**
PIP-3: INT7 till FP8, bara Hopper och Blackwell godkända

## 2 av 3

nyttigt för AI, verifierbart bit för bit, hårdvaruneutralt: ett talformat får högst två

## 13 bitar

behåller Hoppers FP8-ackumulering, med trunkering: inte reproducerbart mellan generationer

## ≈82 %

av hashkraften på konsumentkort som PIP-3 inte skulle godkänna (modell med låg säkerhet)

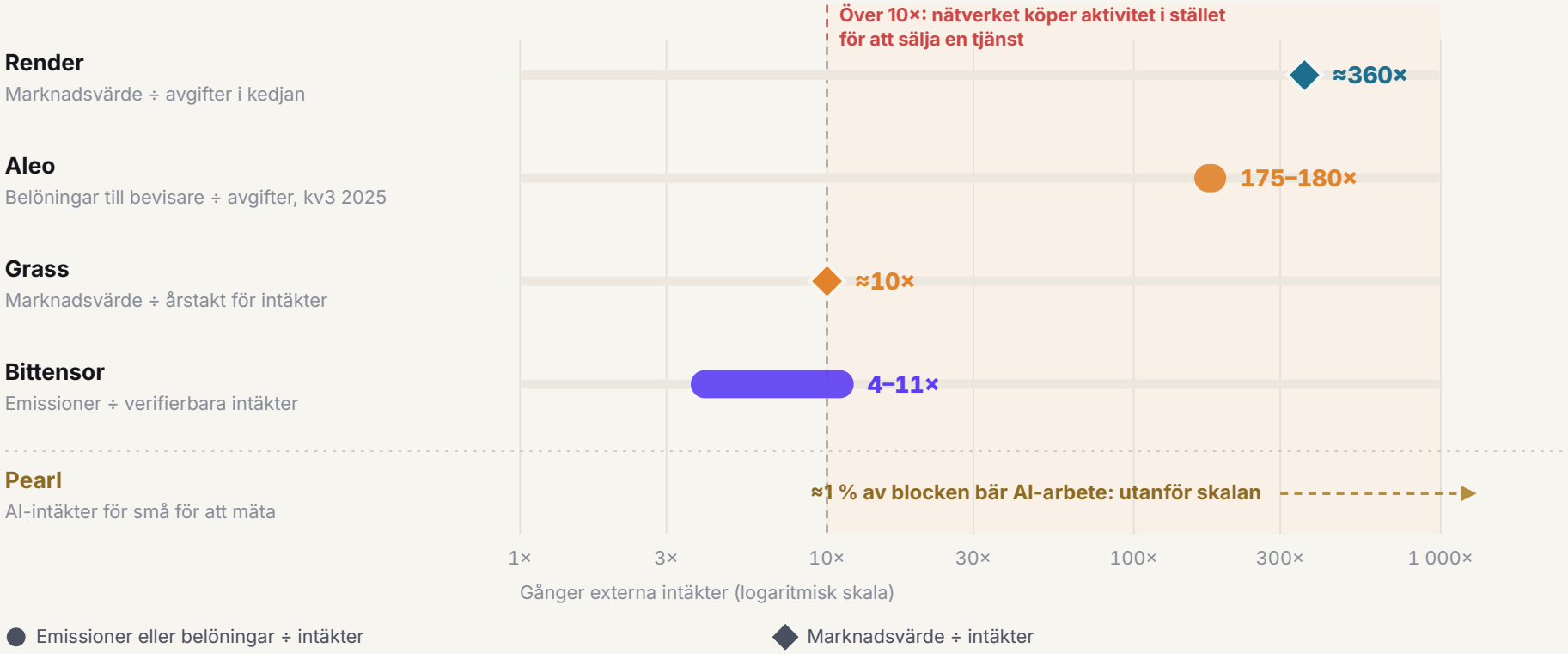
**Den som styr arbetsfunktionen styr hårdvaruinvesterarnas öde** analys.

# Varken matriser eller nollkunskap stoppar ASIC:er

| Nätverk | Vad som hände | Vad det lär oss |
|---|---|---|
| **Kaspa** | En 64 × 64-matrisprodukt mellan hashar; ASIC:er efter 16 månader, omkring 1 000× GPU-effektivitet; den bästa tjänar nu 0,86 dollar om dagen | En matris är varken nyttig eller ASIC-säker |
| **Aleo** | Ett syntetiskt SNARK-pussel; dedikerade maskiner efter fem månader; belöningar till bevisare 175–180× avgifterna | Syntetiskt arbete går på subventioner |
| **Qubic** | Uppger AI-träning; dess beräkningskraft utvann Monero (51 % enligt uppgift) och nu Dogecoin | Generell PoW kan kapas utifrån |
| **Bittensor** | Insatsviktad poängsättning; omkring 70 miljoner dollar om året i verifierbara intäkter mot mer än 300 miljoner dollar i emissioner | Den enda med externa intäkter i stor skala |
| **Monero, Sia, Ethereum** | Forkar gjorde ASIC:er obrukbara; efter the Merge hittade under 20 % av miners nytt arbete | Hårdvara med en andra marknad överlever |

SUBVENTION

# Subventionsmultipeln är det ärligaste hälsotestet




> Över omkring 10 gånger de externa intäkterna köper ett nätverk aktivitet i stället för att sälja en tjänst. Pearls AI-intäkter är för små för att placeras på skalan.

# Verklig men liten efterfrågan, och värdet flyttar till bolagen

- **Beräkningsmarknader**

  Renders avgifter i kedjan omkring 2,35 miljoner dollar om året; Akashs H100 för 2,73 dollar i timmen slår AWS och Google men inte Vast.ai eller RunPod.

- **Träning**

  8–40 miljarder parametrar tränade över internet; INTELLECT-3 gick tillbaka till 512 H200 på InfiniBand.

- **Verifierbar AI**

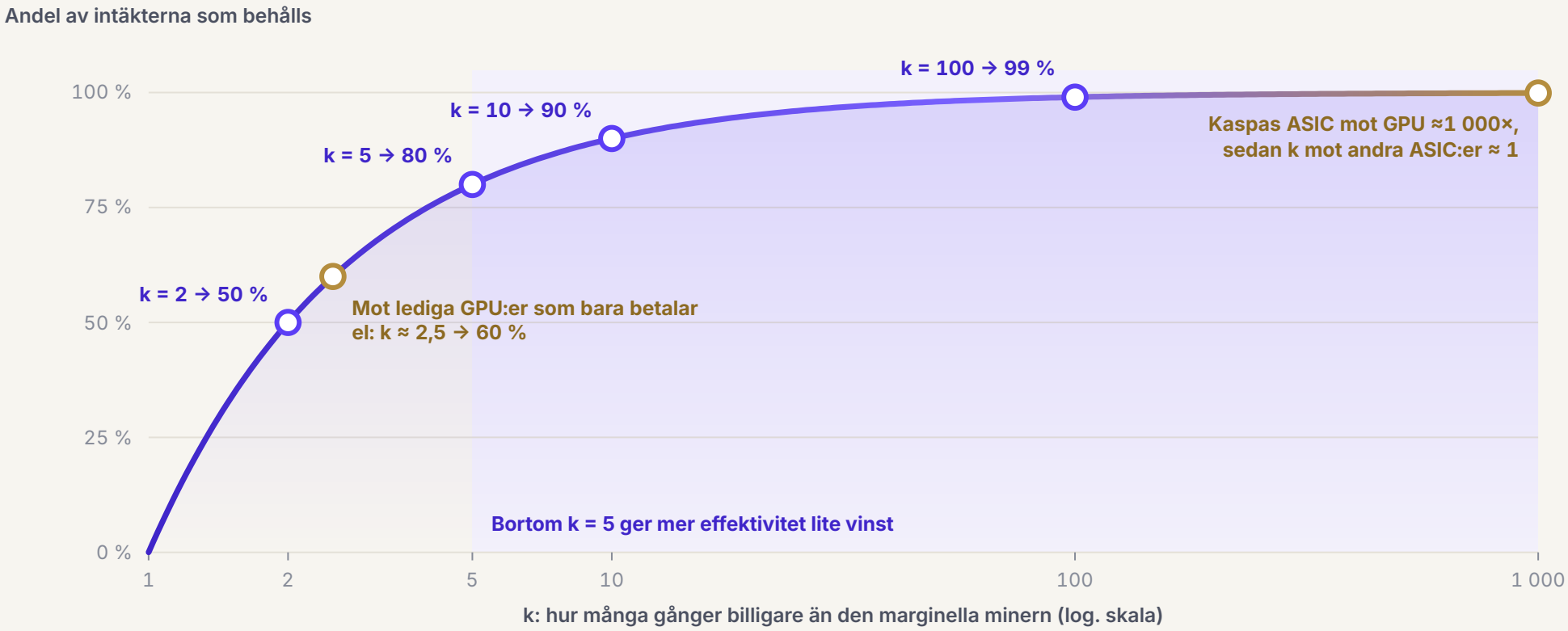
  TEE lägger till under 7 % och körs i produktion; TEE.fail bröt attesteringen med en mellanlänk för 1 000 dollar; zkML bevisar GPT-2 med 174 token i minuten.

- **Agenter och data**

  x402-flöden initierade av agenter omkring 5 000–11 000 dollar i månaden; Grass 17 miljoner dollar i dataintäkter första halvåret 2026.

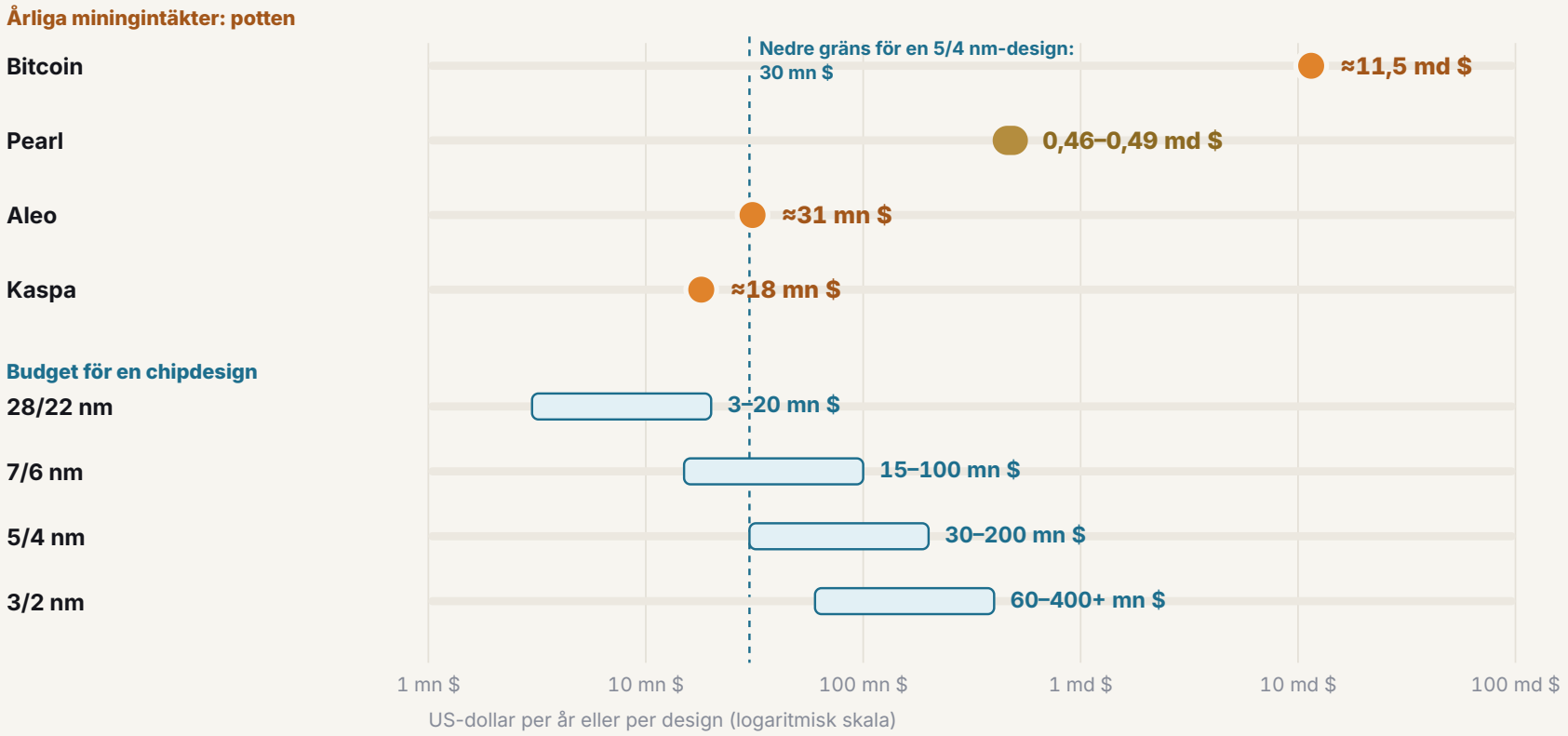
**Fyra aktiebolag på centraliserad infrastruktur är värda omkring 8,5 miljarder dollar, ungefär lika mycket som alla AI-tokens på protokoll- och applikationsnivå.**

# Varför effektivitet slutar löna sig efter k = 5




Vinsttak ≈ R × (1 − 1/k). När ASIC:er blir de marginella minerna nollställs k mot andra ASIC:er; mot lediga GPU:er som bara betalar el är k omkring 2,5 **uppskattning**.

# De flesta potter är mindre än en enda chipbudget




> Hashkraft för återbetalning h* = NRE ÷ [R × (1 − 1/k) × T × p]. För Pearl med 20 miljoner dollar i NRE och k = 5: omkring 4,9 EH/s i ett år om reglerna håller, 9,8 EH/s om de håller med lika odds **uppskattning**.

# Fem chiptyper, fem svar





### PoUW-miningchip i Pearls stil

**INTE NU**

**k:** utan HBM och generella enheter: 3–10× per operation (härlett)

**Andra marknad:** AI-inferens, om generell INT8/FP8-GEMM

**Satsa på ett inferenschip som kan utvinna, inte på en dedikerad INT7-krets**



### SHA-256-miningchip för bitcoin

**AVSTÅ**

**k:** ≤1 mot de etablerade

**Andra marknad:** nästan ingen

**Bara med egen el, en nischform eller som IP**



### AI-träningschip

**IP, INTE CHIP**

**k:** 1,1–1,8× vid samma precision

**Andra marknad:** —

**Kapsling och HBM avgör; bygg IP, chiplets, tjänster**



### AI-inferenschip

**BYGG**

**k:** avstå generalitet: 10–20× enligt uppgift

**Andra marknad:** det är huvudmarknaden

**Teckna kunden, välj sedan inlåsningen**



### Accelerator för ZK-bevis

**VÄNTA OCH GARDERA**

**k:** 10–100× GPU:er enligt uppgift

**Andra marknad:** begränsad utanför ZK

**Programmerbara MSM- och NTT-motorer; FPGA först**



### FHE-accelerator

**POSITIONERA TIDIGT**

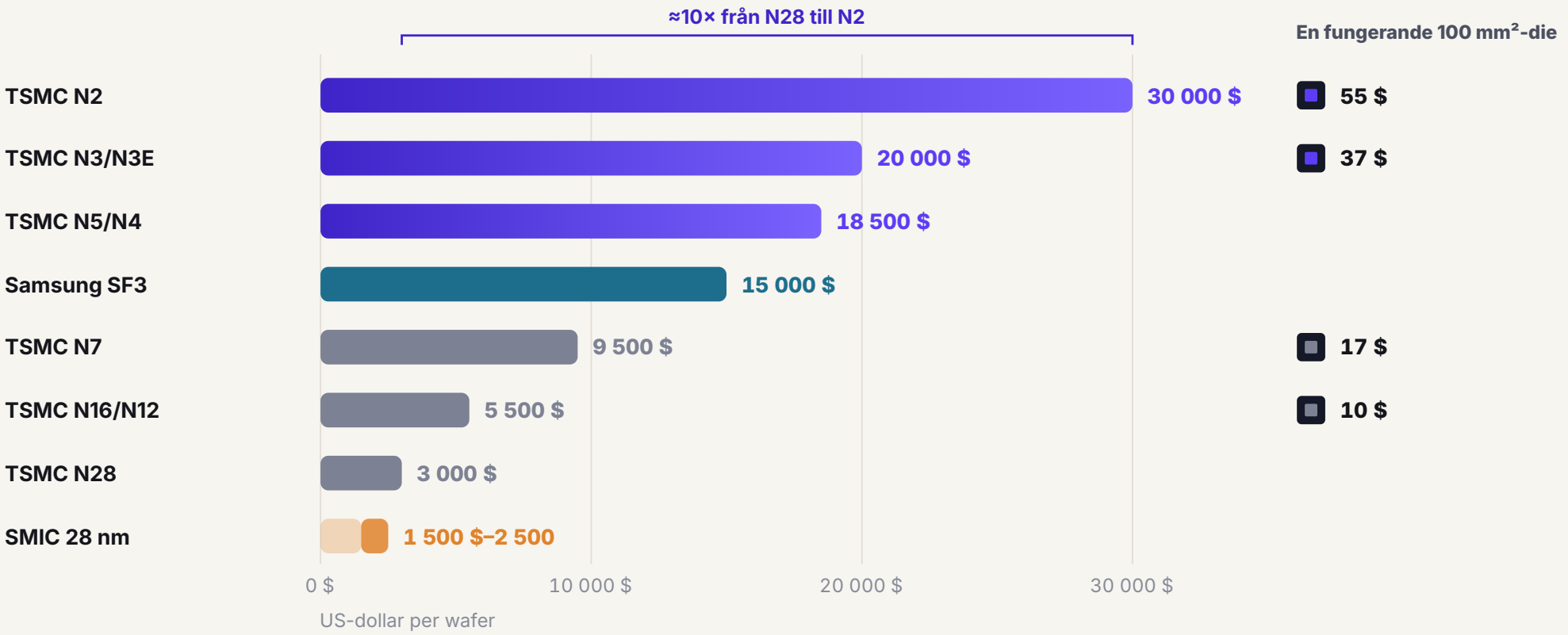
**k:** 1 074–5 547× en Xeon (Heracles)

**Andra marknad:** krypterad beräkning, privat AI

**Ett fönster 2027–2029; validera med lätta tillgångar**

> Inget nätverk erbjuder i dag stor pott, stabila regler och k över 1 samtidigt: bitcoins k tillhör de etablerade, Pearls regler är minst stabila, Kaspas och Aleos potter är för små.

# En wafer i spetsnod kostar tio gånger en mogen




> Låt den största livstidskostnaden välja: energi för beräkningschip som går dygnet runt, kapsling och HBM för träningschip (63 % av kostnaden för en H100), valet mellan SRAM och HBM för inferenschip.

PROCESSNODER

# En nod för varje chip och varje team

| Chip | Litet team | Skalat företag | Väg i Fastlandskina |
|---|---|---|---|
| **PoUW-miningchip** | 28 eller 16/12 nm MPW; första volym N7/N6 | N3/N3E eller Samsung SF3 | SMIC N+1/N+2 fungerar, omkring 40–50 % mer per die |
| **SHA-256-miningchip** | Jaga inte spetsen | 3 nm-klass | Svårt att matcha spetsnodernas effektivitet |
| **AI-träningschip** | IP, chiplets, designtjänster | N3P, sedan N2/A16 med CoWoS och HBM | SMIC N+2/N+3 med inhemsk HBM |
| **AI-inferenschip** | SRAM-centrerat på N6/N7 eller N4/N5/SF4 | N3/N2 med HBM, eller SRAM-chiplets | SMIC N+2 med LPDDR eller GDDR |
| **ZK- och FHE-acceleratorer** | FPGA eller 16/12 nm MPW först | N5/N3; FHE med HBM | ZK genomförbart; FHE begränsat av HBM |

EN BUDGET I STEG

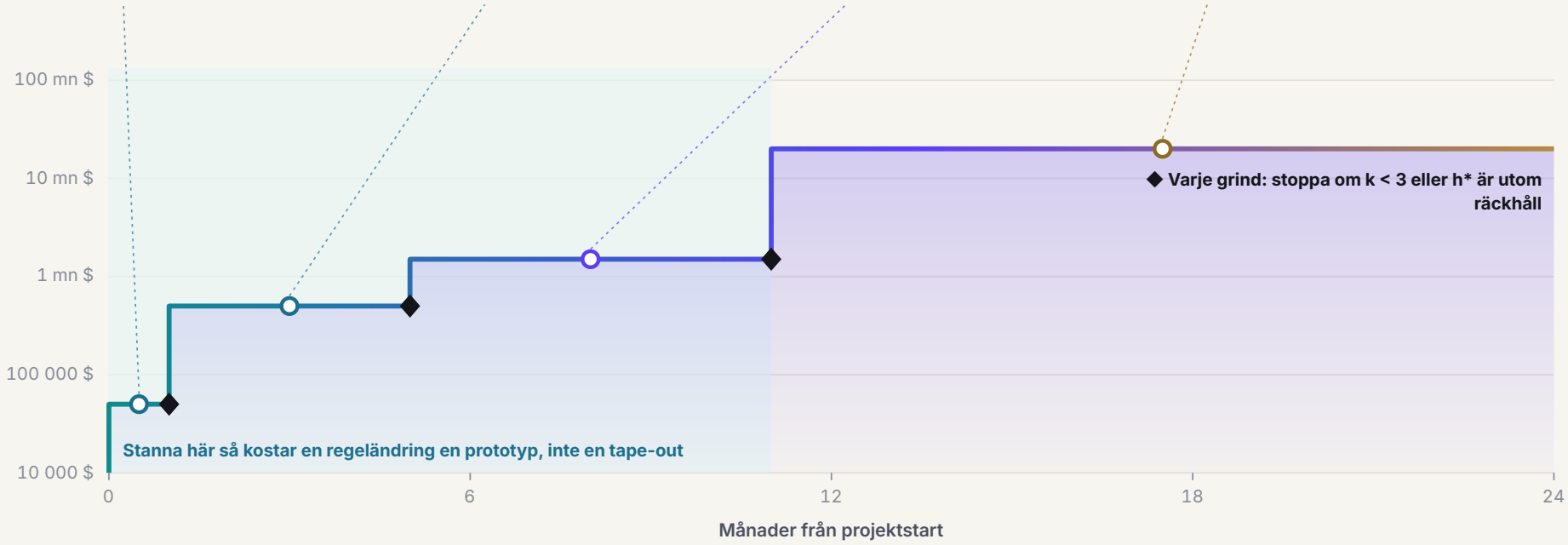
# Köp belägg före masker

**Grind 0 · Modell**
**≈50 000 $ · veckor**
J/op och $/op ur aritmetik, SRAM och I/O

**Grind 1 · FPGA**
**≈0,5 mn $ · månader**
Den verkliga lasten hela vägen: andelar eller token

**Grind 2 · MPW**
**≈1,5 mn $ · månad 11**
Uppmätt kisel ersätter modellen

**Grind 3 · Masker och första lot**
**≈20 mn $ · månad 24**
N7-masker ≈3,5 mn $ i en design på 15–100 mn $




En modell, en FPGA och en MPW når uppmätt kisel för omkring 1,5 miljoner dollar på elva månader; masksetet och den första loten kostar mer än tio gånger så mycket. Stanna före maskerna tills köparen eller protokollversionen är fastlagd.

MÖJLIGHETER

# Kryptot som första kund, AI som andra marknad

## Kundanpassade chip

- Efterfrågan är överväldigande AI: Broadcom omkring 58 miljarder dollar i AI-halvledare räkenskapsåret 2026
- Kunnandet från miningchip går att överföra: lågspänningsmatriser, kilowattmatning, snabba tape-outs
- Vinn med en egen väg till marknaden, inte via miningkanaler

## AI-utveckling

- Timmar är en handelsvara: 25–49 dollar i timmen på Clutch
- Värdet sitter i skarvarna: kärnor för kundanpassade chip, mining inuti inferenstjänster
- Verifierbar inferens: TEE plus stickprov med ZK

## System för AI × krypto

- Verifiering i lager: TEE eller stickprov, sedan tvister eller stickprov med ZK
- Distribution och likviditet är hindren, inte kostnaden
- Teckna köparen av beräkningskraft före token

VAD JAG SKULLE GÖRA

# Tre vägar, var och en med ett litet första steg

| Väg | Första steg |
|---|---|
| ***A. En inferensaccelerator som också kan utvinna*** | En fyraveckorsstudie av J/op och $/op för en SRAM-baserad INT8/FP8-matris mot RTX 5090 och H100, sedan FPGA eller MPW i mogen nod |
| ***B. Tjänster för kundanpassat kisel: krypto först, AI sedan*** | Gör rapportens modell för NRE och break-even till betalda förstudier med milstolpar och en fast protokollversion |
| ***C. Ett AI-nativt nätverk med en köpare före en token*** | Ett designnotat om verifiering i lager och en leverantörsneutral kanonisk aritmetik, skrivet med en namngiven inferensköpare |

**Högst tre vägar, var och en prövad innan pengar binds** analys **.**

ATT FÖLJA

# Vad man ska följa, och frågor att ställa

## SIGNALER ATT FÖLJA

| | |
|---|---|
| **När som helst** | Pearls aktiveringshöjd för FP8, och om kedjan delas |
| **Månadsvis** | Pearls andel block som bär AI-arbete |
| **Kvartalsvis** | Bittensors verifierbara intäkter mot emissioner; x402-flöden initierade av agenter |
| **Januari 2027** | TSMC:s rapporterade prishöjning på 3–6 % för 2 nm och 3 nm |
| **Kv1 2027** | FP4 i Pearl, enligt uppgifter från grundarnas AMA |
| **April 2028** | Bitcoins nästa halvering |

## FRÅGOR ATT STÄLLA

01 Vem styr arbetsfunktionen?

02 Hur stor är subventionsmultipeln?

03 Vad kostar nästa grind, och vad stoppar dig?

04 Hur stor är hashkraften för återbetalning, med p?

05 Vilken är chipets andra marknad?

06 Vem är den första betalande kunden, med namn?

**Det här är områden vi kan utforska tillsammans, genom tekniskt utbyte och tekniskt samarbete: kundanpassade chip, AI-utveckling och system för AI × krypto.**

i@tanshuai.com · tanshuai.com