Forskningsnotat · November 2026

Regnekraft som konsensus

AI × krypto × chips i 2026, med udgangspunkt i Pearl

Pearl · Nyttigt arbejde · DePIN og agenter · ASIC-økonomi · Procesnoder · Budgetter i etaper

Tan Shuai
tanshuai.com · i@tanshuai.com



KONKLUSIONEN

Teoremet holder, incitamentet gør ikke

01 Pearl virker som ingeniørarbejde, endnu ikke som nyttigt arbejde

Omkring 90 EH/s heltals-matrixmultiplikation sikrer kæden, men kun omkring 1 % af blokkene bærer reelt AI-arbejde.

02 Betalt efterspørgsel ligger i inferens, data og privatliv

Bittensor omkring $70 mio. om året i verificerbar omsætning, Grass $17 mio. i 1. halvår 2026, TEE'er i produktion; agentbetalinger omkring $5.000–11.000 om måneden.

03 En ASIC betaler sig kun med en stor pulje, stabile regler og et andet marked

Dens profitloft er R × (1 − 1/k). I dag tilbyder intet netværk alle tre analyse.

≈90 EH/s

Pearl den 13. november 2026: heltalskapaciteten i omkring 122.000 H100'ere

≈1 %

af Pearls blokke bærer reelt AI-arbejde (Blockworks)

4–11×

Bittensors udstedelse i forhold til den verificerbare omsætning

AI × krypto i seks sektorer: hvor betalt efterspørgsel er reel

Kæder med nyttigt arbejde
01

REEL, MEN LILLE

≈$70 mio. om året

Bittensors verificerbare eksterne omsætning

Signal: udstedelse 4–11× omsætning; Pearl ≈1 % AI-blokke

Mekanismerne virker; nytte kræver betalere

Decentral regnekraft
02

REEL, MEN LILLE

$2,35 mio. om året

Renders on-chain-gebyrer, de største verificerbare

Signal: markedsværdi ≈360× gebyrer

For det meste videresalg af standardinferens

Træning og inferens
03

PROFIT I EGENKAPITAL

$100+ mio. om året

Prime Intellect, et selskab på centrale GPU'er

Signal: Gensyns trænings-mainnet ikke i drift

Fremskridt er reelle; profit går til egenkapital

Verificerbar AI
04

TIDLIGT

398

betalende brugere af Phalas TEE-cloud, ultimo 2025

Signal: ingen oplyst betalt zkML

TEE'er i produktion; zkML tidligt

Agentbetalinger
05

FØR EFTERSPØRGSEL

$5–11K om måneden

x402-betalinger faktisk igangsat af agenter

Signal: ≈200 mio. transaktioner, mest signalering

Infrastrukturen kom først; efterspørgslen ikke

Datanetværk
06

REELLE KØBERE

$17 mio.

Grass' dataomsætning, første halvår 2026 (selvrapporteret)

Signal: markedsværdi ≈10× annualiseret omsætning

En af de få sektorer med reelle købere

> Subsidie er brændstof til en koldstart, ikke en forretningsmodel. Krypto står for distribution og afvikling; egenkapitalen tager overskuddet, i hvert fald i 2026.

Én multiplikation-akkumulering er én hash

Fra teorem til mainnet

Komargodski og Weinstein (april 2025): et bevis for nyttigt arbejde for ethvert matrixprodukt med 1 + o(1) overhead. Pearls mainnet startede den 27. april 2026.

Sådan virker det

Minere multiplicerer støjfyldte matricer, hasher hver flises akkumulator til en lottokupon og beviser den vindende flise med et Plonky2-bevis under 60 KB.

Enheden

1 H er én krediteret INT7 × INT7 → INT32-multiplikation-akkumulering: en blockchains sikkerhedsbudget prissat i tensorkapacitet.

PEARL DEN 13. NOVEMBER 2026

89,77 EH/s

netværkets hashrate (uafhængig fuld node)

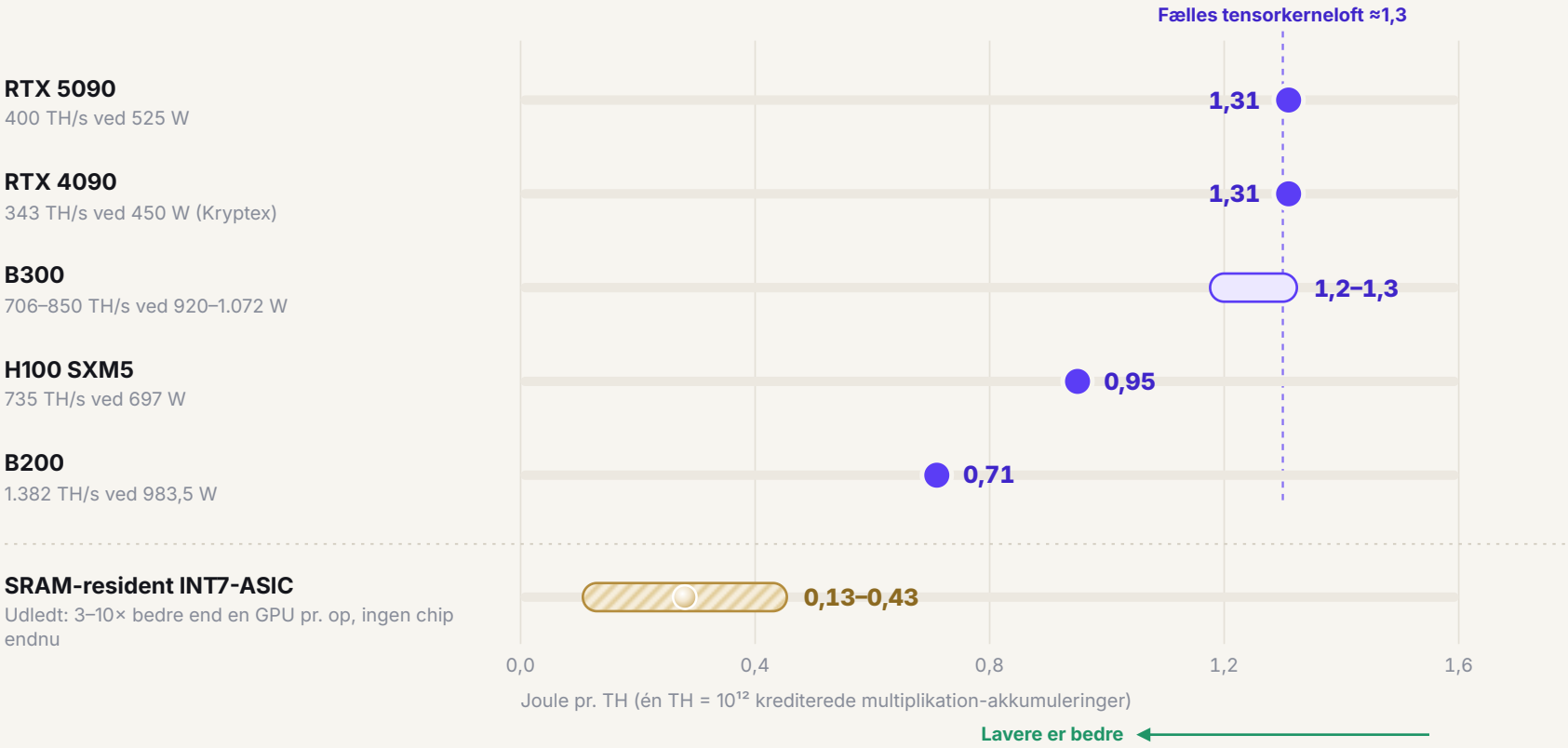
≈$500 mio.

markedsværdi; fuldt udvandet omkring $2,8 mia.

+78 %

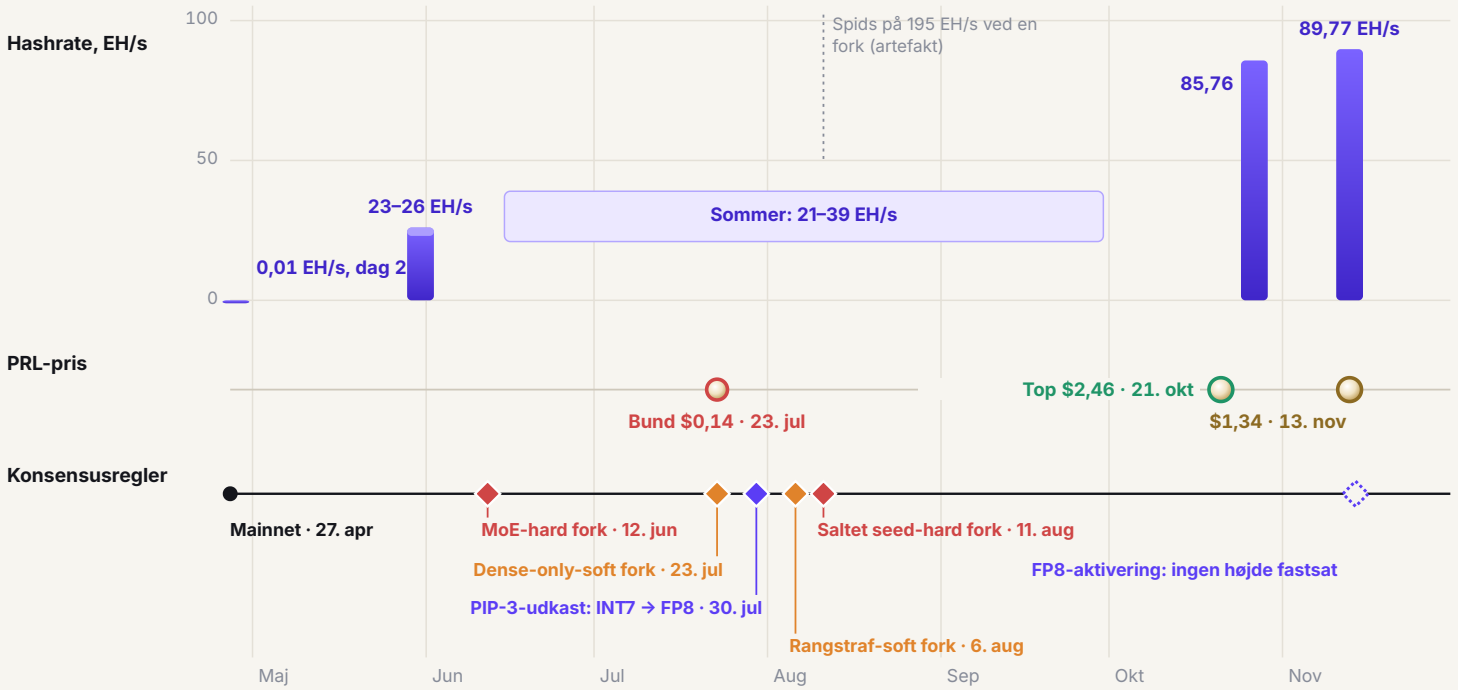
nyt udbud de næste 12 måneder

På Pearls heltalsarbejde deler GPU'er et energiloft



Gamingkort og B300 mødes ved omkring 1,3 J/TH; selv B200 når kun 0,71. En chip, der kun multiplicerer 7-bit-heltal fra SRAM, kunne plausibelt gøre det 3–10 gange bedre analyse.

Hashraten følger prisen; reglerne bliver ved med at ændre sig



> Omkring 120 mio. mønter, 32 % af det nuværende udbud, blev udvundet de første seks dage. En RTX 5090 tjener nu omkring $5–6 om dagen; at leje kort alene for at mine giver tab.

Teoremet holder, incitamentet gør ikke

HVAD NYTTIGT ARBEJDE KOSTER

Inferenssiden: lille overhead

Pearl oplyser 5,08 % mere tid for Llama 70B på fire H200'ere; en uafhængig test målte 9,2 % lavere kapacitet på én Hopper-GPU.

HVAD NYTTIGT ARBEJDE TJENER

Mining-siden: for lidt hashrate

Et kort, der betjener inferens, miner med omkring 27 % af en dedikeret miner ved prefill, 5,4 % ved chat, omkring 1 %, når decode dominerer.

Så rationelle minere multiplicerer tilfældige matricer. Nytte er et kommercielt problem uden for kæden: nogen skal betale for inferens.

Fire forks på to måneder, og FP8 som det næste

12. juni
Mixture-of-experts-hard fork (blok 71.935)

23. juli
Dense-only-soft fork (blok 91.630)

6. august
Rangstraf-soft fork: nogle opsætninger mister 50–87,5 % af den effektive hashrate

11. august
Hard fork med saltet seed: gamle minere producerer kun ugyldige shares

Ikke fastsat
PIP-3: INT7 til FP8, kun Hopper og Blackwell optages

2 af 3
nyttigt for AI, verificerbart bit for bit, hardwareneutralt: et talformat får højst to

13 bits
beholdes af Hoppers FP8-akkumulering, med trunkering: ikke reproducerbart på tværs af generationer

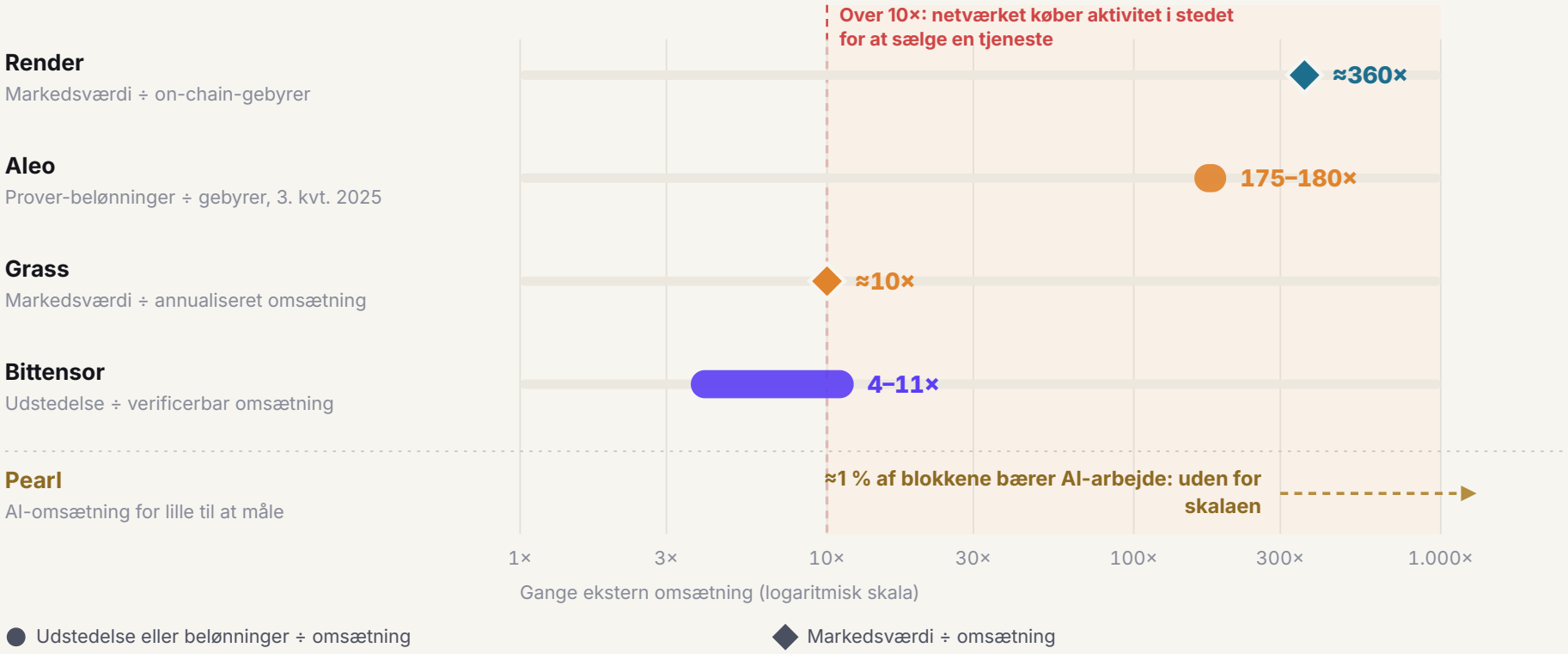
≈82 %
af hashraten på forbrugerkort, som PIP-3 ikke ville optage (model med lav sikkerhed)

Den, der kontrollerer arbejdsfunktionen, kontrollerer hardwareinvestorernes skæbne analyse.

Hverken matricer eller zero knowledge stopper ASIC'er

Netværk	Hvad der skete	Hvad det lærer os
Kaspa	Et 64 × 64-matrixprodukt mellem hashes; ASIC'er efter 16 måneder, omkring 1.000× GPU-effektiviteten; den bedste tjener nu $0,86 om dagen	En matrix er hverken nyttig eller ASIC-sikker
Aleo	En syntetisk SNARK-gåde; dedikerede maskiner efter fem måneder; prover-belønninger 175–180× gebyrerne	Syntetisk arbejde kører på subsidie
Qubic	Påstår AI-træning; regnekraften minede Monero (51 % påstået) og nu Dogecoin	Generel PoW kan erobres udefra
Bittensor	Stake-vægtet bedømmelse; omkring $70 mio. om året i verificerbar omsætning mod mere end $300 mio. i udstedelse	Den eneste med ekstern omsætning i stor skala
Monero, Sia, Ethereum	Forks gjorde ASIC'er ubrugelige; efter Merge fandt under 20 % af minerne nyt arbejde	Hardware med et andet marked overlever

Subsidiemultiplen er det mest ærlige sundhedstjek



> Over omkring 10 gange den eksterne omsætning køber et netværk aktivitet i stedet for at sælge en tjeneste. Pearls AI-omsætning er for lille til at placere på skalaen.

Reel, men lille efterspørgsel, og værdi, der flytter til egenkapital

- **Regnekraftmarkeder**

  Renders on-chain-gebyrer omkring $2,35 mio. om året; Akashs H100 til $2,73 i timen slår AWS og Google, men ikke Vast.ai eller RunPod.

- **Træning**

  8–40 mia. parametre trænet over internettet; INTELLECT-3 gik tilbage til 512 H200'ere på InfiniBand.

- **Verificerbar AI**

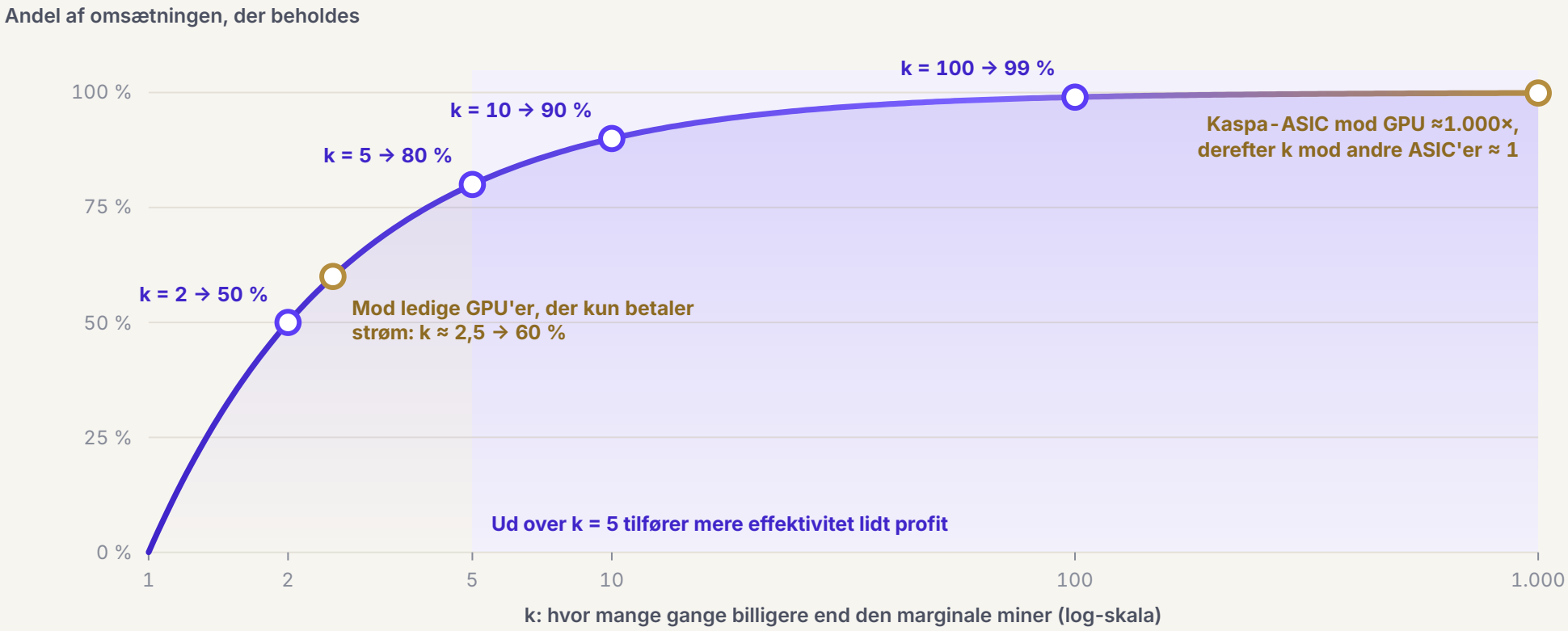
  TEE'er tilføjer under 7 % og kører i produktion; TEE.fail brød attesteringen med en interposer til $1.000; zkML beviser GPT-2 med 174 tokens i minuttet.

- **Agenter og data**

  Strømme igangsat af agenter via x402 omkring $5.000–11.000 om måneden; Grass $17 mio. i dataomsætning i 1. halvår 2026.

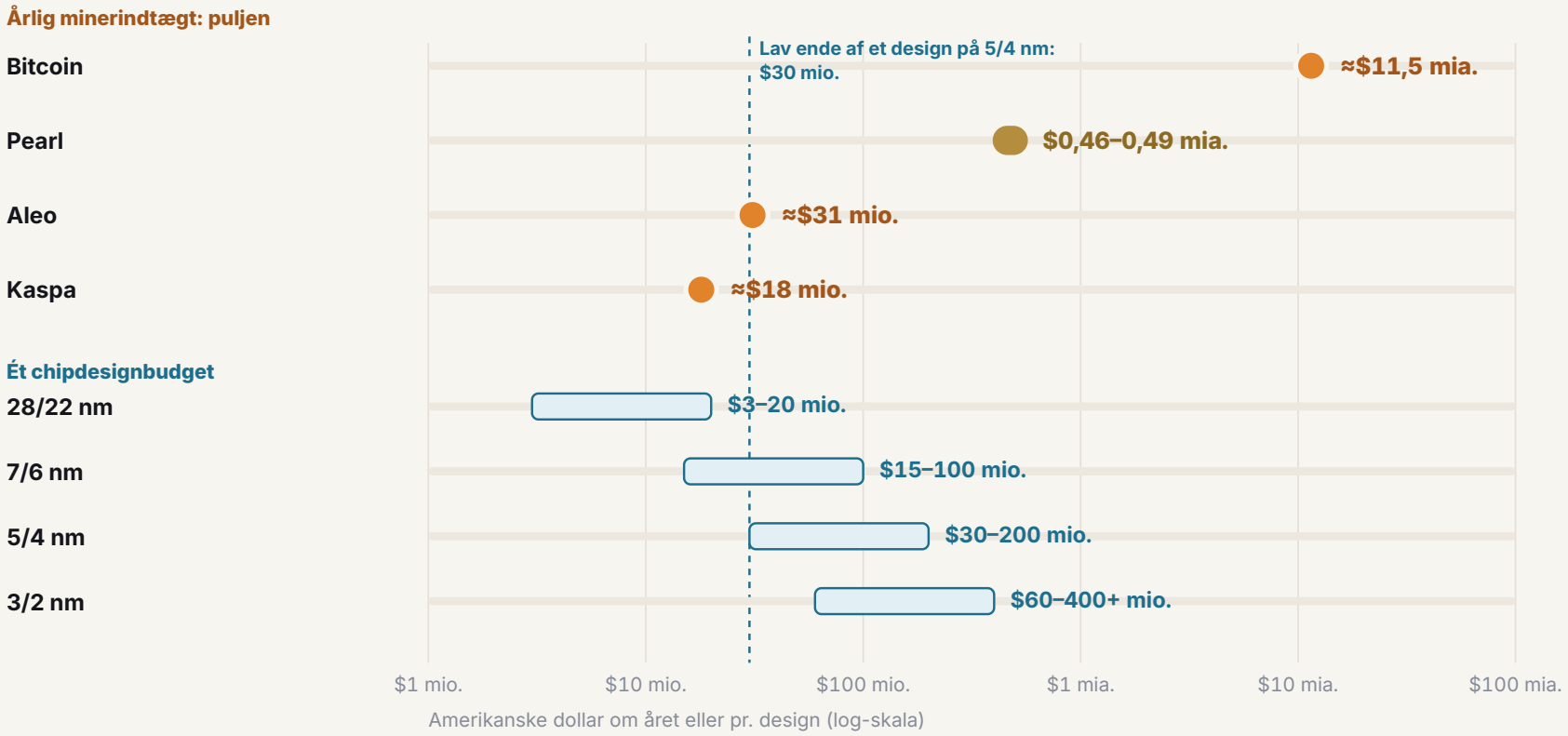
> **Fire selskaber på centraliseret infrastruktur er værd omkring $8,5 mia., omtrent lige så meget som alle AI-tokens på protokol- og applikationslaget.**

Hvorfor effektivitet holder op med at betale sig efter k = 5



Profitloft ≈ R × (1 − 1/k). Når ASIC'er bliver de marginale minere, nulstilles k mod andre ASIC'er; mod ledige GPU'er, der kun betaler for strøm, er k omkring 2,5 **estimat**.

De fleste puljer er mindre end ét chipdesignbudget



Tilbagebetalings-hashrate h* = NRE ÷ [R × (1 − 1/k) × T × p]. For Pearl ved $20 mio. i NRE og k = 5: omkring 4,9 EH/s i et år, hvis reglerne holder, 9,8 EH/s, hvis de holder med lige odds **estimat**.

Fem chiptyper, fem svar

PoUW-mining-chip i Pearl-stil

IKKE NU

k: ingen HBM eller generelle enheder: 3–10× pr. op (udledt)

Andet marked: AI-inferens, hvis generel INT8/FP8-GEMM

Sats på en inferens-først-chip, der kan mine, ikke en dedikeret INT7-del

Bitcoin-SHA-256-mining-chip

HOLD DIG UDE

k: ≤1 mod de etablerede

Andet marked: næsten intet

Kun med egen strøm, en nicheform eller som IP

AI-træningschip

IP, IKKE CHIPS

k: 1,1–1,8× ved samme præcision

Andet marked: —

Pakning og HBM afgør; byg IP, chiplets, ydelser

AI-inferenschip

BYG

k: opgiv generalitet: 10–20× påstået

Andet marked: det er hovedmarkedet

Få kunden til at skrive under, vælg så bindingen

ZK-bevisaccelerator

VENT OG AFDÆK

k: 10–100× GPU'er påstået

Andet marked: begrænset uden for ZK

Programmerbare MSM- og NTT-motorer; FPGA først

FHE-accelerator

POSITIONÉR TIDLIGT

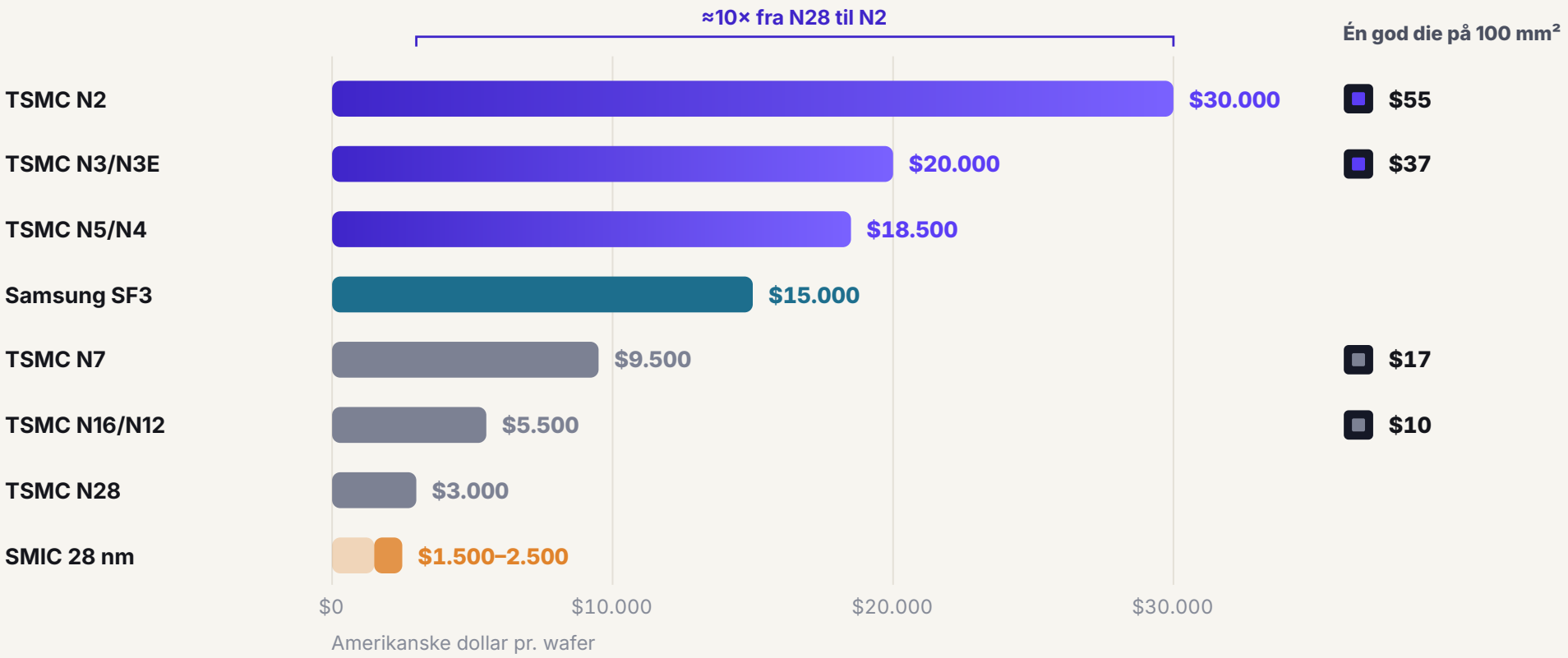
k: 1.074–5.547× en Xeon (Heracles)

Andet marked: krypteret beregning, privat AI

Et vindue 2027–2029; valider med lette aktiver

> Intet netværk tilbyder i dag en stor pulje, stabile regler og k over 1 på én gang: bitcoins k tilhører de etablerede, Pearls regler er de mindst stabile, Kaspas og Aleos puljer er for små.

En wafer på en førende node koster ti gange en moden



> Lad den største levetidsomkostning vælge: energi for compute-chips, der kører døgnet rundt, pakning og HBM for træningschips (63 % af en H100's omkostning), valget mellem SRAM og HBM for inferenschips.

PROCESNODER

En node til hver chip og hvert team

Chip	Lille team	Skaleret selskab	Vej via det kinesiske fastland
PoUW-mining-chip	MPW på 28 eller 16/12 nm; første volumen N7/N6	N3/N3E eller Samsung SF3	SMIC N+1/N+2 virker, omkring 40–50 % mere pr. die
SHA-256-mining-chip	Jag ikke fronten	3 nm-klassen	Svært at matche førende noders effektivitet
AI-træningschip	IP, chiplets, designydelser	N3P derefter N2/A16 med CoWoS og HBM	SMIC N+2/N+3 med indenlandsk HBM
AI-inferenschip	SRAM-centreret på N6/N7 eller N4/N5/SF4	N3/N2 med HBM eller SRAM-chiplets	SMIC N+2 med LPDDR eller GDDR
ZK- og FHE-acceleratorer	FPGA eller MPW på 16/12 nm først	N5/N3; FHE med HBM	ZK brugbart; FHE begrænset af HBM

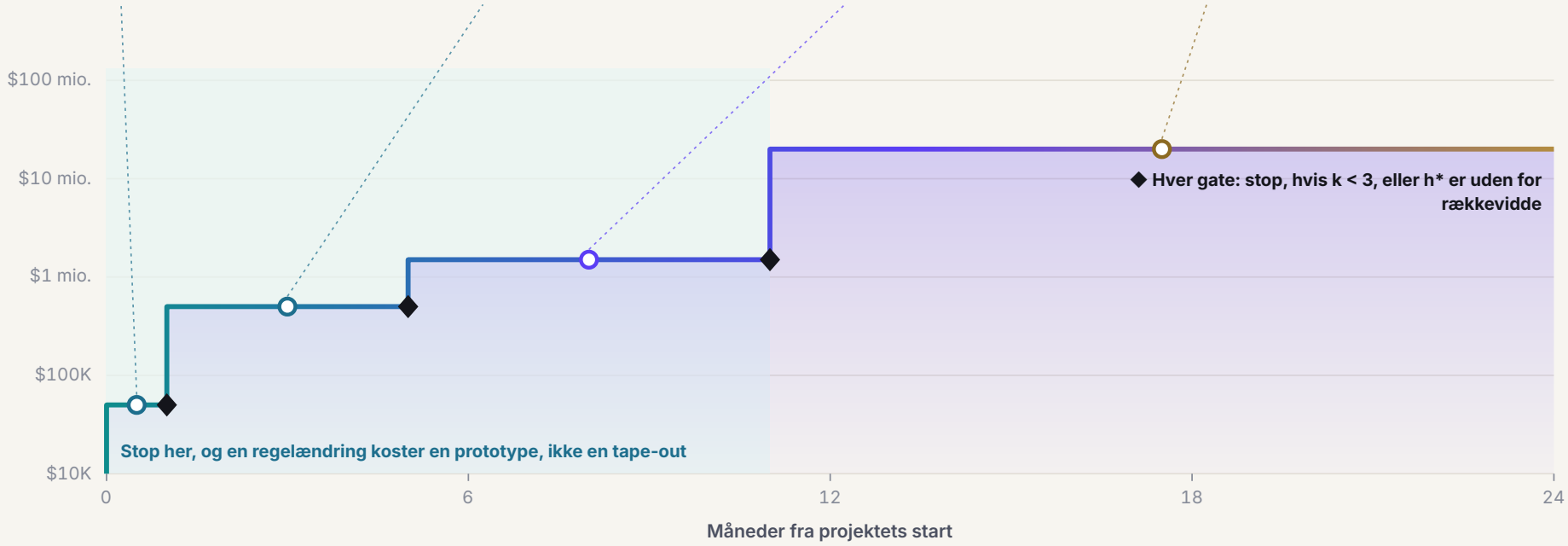
Køb evidens før masker

Gate 0 · Model
≈$50K · uger
J/op og $/op ud fra aritmetik, SRAM og I/O

Gate 1 · FPGA
≈$0,5 mio. · måneder
Den reelle arbejdsbyrde fra ende til anden: shares eller tokens

Gate 2 · MPW
≈$1,5 mio. · måned 11
Målt silicium erstatter modellen

Gate 3 · Masker og første parti
≈$20 mio. · måned 24
Masker på N7 ≈$3,5 mio. i et design til $15–100 mio.



En model, en FPGA og en MPW når frem til målt silicium for omkring $1,5 mio. på elleve måneder; maskesættet og det første parti koster mere end ti gange så meget. Stop før maskerne, indtil køberen eller protokolversionen ligger fast.

Krypto som den første kunde, AI som det andet marked

Specialchips

- Efterspørgslen er overvejende AI: Broadcom omkring $58 mia. i AI-halvledere i regnskabsåret 2026
- Mining-chip-kompetencer kan overføres: lavspændings-arrays, kilowatt-strøm, hurtige tape-outs
- Vind med en selvstændig vej til markedet, ikke via mining-kanaler

AI-udvikling

- Timer er en standardvare: $25–49 i timen på Clutch
- Værdien ligger i samlingerne: kerner til specialchips, mining inde i inferensservering
- Verificerbar inferens: TEE'er plus ZK-stikprøver

AI × krypto-systemer

- Lagdelt verifikation: TEE eller stikprøver, derefter tvister eller ZK-stikprøver
- Distribution og likviditet er barriererne, ikke omkostninger
- Få regnekraftkøberen til at skrive under før tokenet

Tre veje, hver med et lille første skridt

Vej	Første skridt
A. En inferens-først-accelerator, der også kan mine	Et fireugers studie af J/op og $/op for et SRAM-resident INT8/FP8-array mod RTX 5090 og H100, derefter FPGA eller MPW på moden node
B. Ydelser inden for specialsilicium: krypto først, AI derefter	Omsæt rapportens model for NRE og break-even til betalte forundersøgelser med milepæle og en fastlåst protokolversion
C. Et AI-nativt netværk med en køber før et token	Et designnotat om lagdelt verifikation og en leverandørneutral kanonisk aritmetik, skrevet sammen med én navngiven inferenskøber

Højst tre veje, hver testet, før der bindes penge analyse **.**

Hvad man skal holde øje med, og spørgsmål at stille

PEJLEMÆRKER

Når som helst	Pearls aktiveringshøjde for FP8, og om kæden splittes
Månedligt	Pearls andel af blokke med AI-arbejde
Kvartalsvis	Bittensors verificerbare omsætning mod udstedelsen; x402-strømme igangsat af agenter
Januar 2027	TSMC's rapporterede prisstigning på 3–6 % for 2 nm og 3 nm
1. kvartal 2027	FP4 i Pearl, som rapporteret fra grundlæggernes AMA
April 2028	Bitcoins næste halvering

SPØRGSMÅL AT STILLE

01 Hvem kontrollerer arbejdsfunktionen?

02 Hvad er subsidiemultiplen?

03 Hvad koster den næste gate, og hvad stopper dig?

04 Hvad er tilbagebetalings-hashraten, med p?

05 Hvad er chippens andet marked?

06 Hvem er den første betalende kunde, ved navn?

Det er områder, vi kan udforske sammen gennem teknisk udveksling og teknisk samarbejde: specialchips, AI-udvikling og AI × krypto-systemer.

i@tanshuai.com · tanshuai.com