Tutkimusmuistio · marraskuu 2026

Laskenta konsensuksena

Tekoäly × krypto × sirut 2026, lähtökohtana Pearl

Pearl · Hyötytyö · DePIN ja agentit · ASIC-talous · Prosessisolmut · Vaiheittaiset budjetit

Tan Shuai
tanshuai.com · i@tanshuai.com



JOHTOPÄÄTÖS

Teoreema pätee; kannustin ei

01 Pearl toimii insinöörityönä, ei vielä hyötytyönä

Noin 90 EH/s kokonaislukumatriisikertolaskua suojaa ketjua, mutta vain noin 1 % lohkoista sisältää oikeaa tekoälytyötä.

02 Maksettu kysyntä on inferenssissä, datassa ja yksityisyydessä

Bittensor noin 70 milj. dollaria vuodessa todennettavaa tuloa, Grass 17 milj. dollaria H1 2026, TEE:t tuotannossa; agenttimaksut noin 5 000–11 000 dollaria kuussa.

03 ASIC kannattaa vain suurella potilla, vakailla säännöillä ja toisella markkinalla

Sen voittokatto on R × (1 − 1/k). Nykyään mikään verkko ei tarjoa kaikkia kolmea analyysi.

≈90 EH/s

Pearl 13.11.2026: noin 122 000 H100:n kokonaislukuläpäisy

≈1 %

Pearlin lohkoista sisältää oikeaa tekoälytyötä (Blockworks)

4–11×

Bittensorin liikkeeseenlasku suhteessa todennettavaan tuloon

KOKONAISKUVA

Tekoäly × krypto kuudella sektorilla: missä maksettu kysyntä on todellista

Hyötytyöketjut 01

TODELLISTA MUTTA PIENTÄ

≈70 milj. $ / v

Bittensorin todennettava ulkoinen tulo

Signaali: liikkeeseenlasku 4–11× tulot; Pearl ≈1 % tekoälylohkoja

Mekanismit toimivat; hyöty vaatii maksajia

Hajautettu laskenta 02

TODELLISTA MUTTA PIENTÄ

2,35 milj. $ / v

Renderin ketjussa maksetut maksut, suurimmat todennettavat

Signaali: markkina-arvo ≈360× maksut

Enimmäkseen perusinferenssin jälleenmyyntiä

Koulutus ja inferenssi 03

VOITTO OSAKKEISIIN

100+ milj. $ / v

Prime Intellect, osakeyhtiö keskitetyillä GPU:illa

Signaali: Gensynin koulutus-mainnet ei käytössä

Edistys on todellista; voitto menee osakkeisiin

Todennettava tekoäly 04

VARHAINEN

398

Phalan TEE-pilven maksavaa käyttäjää, vuoden 2025 lopussa

Signaali: ei julkistettua maksettua zkML:ää

TEE:t tuotannossa; zkML varhain

Agenttimaksut 05

ENNEN KYSYNTÄÄ

5–11 t. $ / kk

x402-maksut, jotka agentit todella käynnistivät

Signaali: ≈200 milj. tapahtumaa, enimmäkseen signalointia

Raiteet tulivat ensin; kysyntä ei

Dataverkot 06

OIKEITA OSTAJIA

17 milj. $

Grassin datatulot, 1. vuosipuolisko 2026 (oma ilmoitus)

Signaali: markkina-arvo ≈10× vuositasoinen tulo

Harvoja sektoreita, joilla on oikeita ostajia

> Tuki on kylmäkäynnistyksen polttoainetta, ei liiketoimintamalli. Krypto hoitaa jakelun ja selvityksen; osakkeet vievät voitot, ainakin vuonna 2026.

Yksi kertolasku-yhteenlasku on yksi tiiviste

Teoreemasta mainnetiin

Komargodski ja Weinstein (huhtikuu 2025): hyötytyön todiste mille tahansa matriisitulolle 1 + o(1) -lisäkustannuksella. Pearlin mainnet käynnistyi 27.4.2026.

Miten se toimii

Louhijat kertovat kohinaisia matriiseja, tiivistävät kunkin ruudun akun arpalipuksi ja todistavat voittaneen ruudun alle 60 kt:n Plonky2-todisteella.

Yksikkö

1 H on yksi hyvitetty INT7 × INT7 → INT32 -kertolasku-yhteenlasku: lohkoketjun turvabudjetti tensoriläpäisyllä hinnoiteltuna.

PEARL 13.11.2026

89,77 EH/s

verkon hashrate (riippumaton täysi solmu)

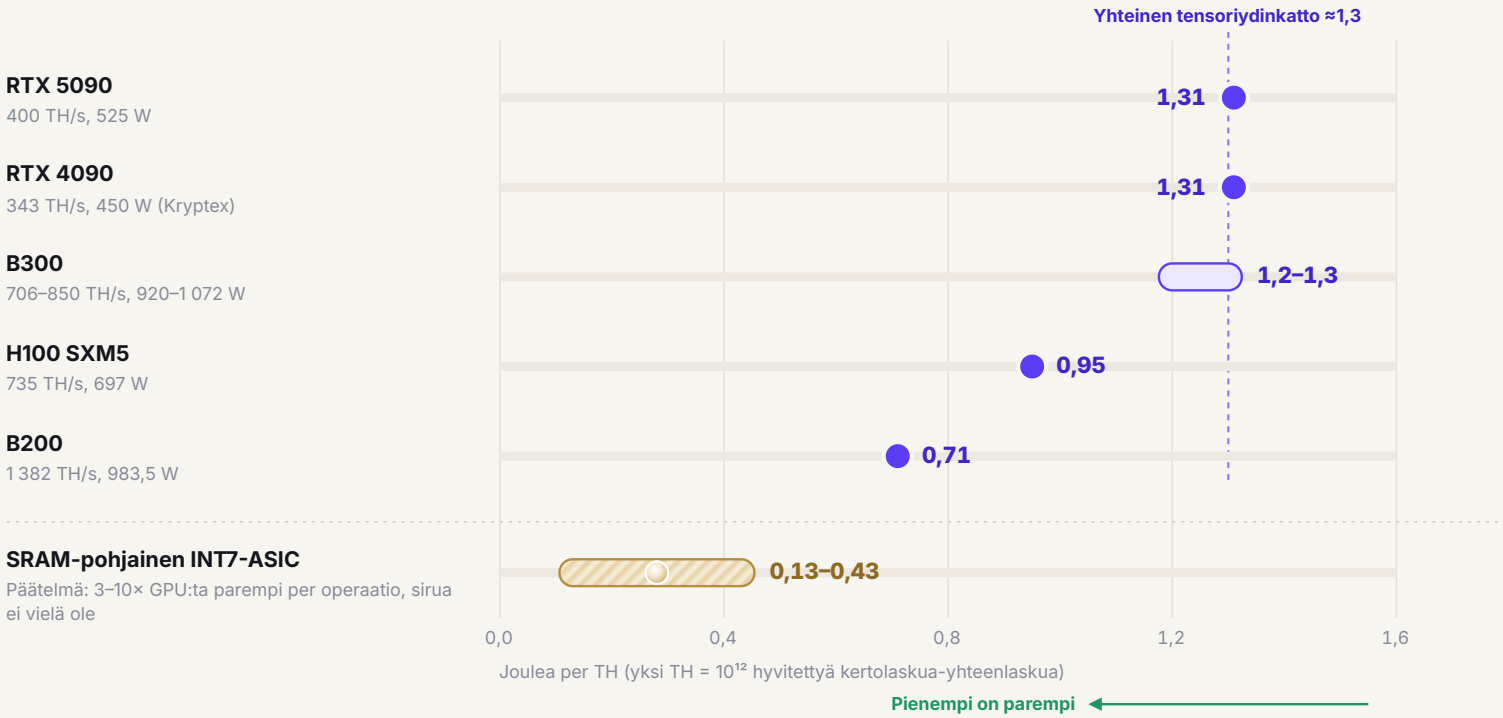
≈500 milj. $

markkina-arvo; täysin laimennettuna noin 2,8 mrd. dollaria

+78 %

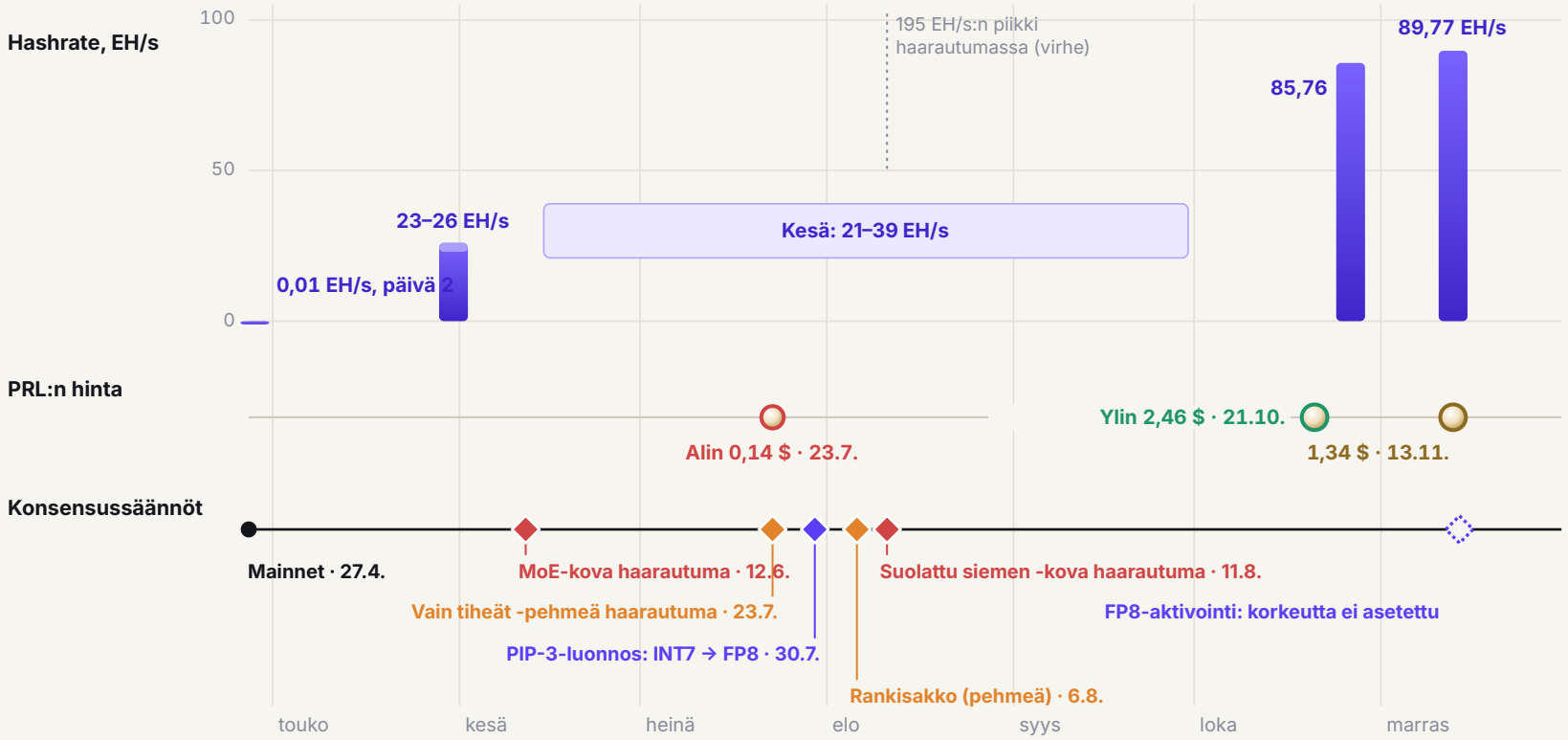
uutta tarjontaa seuraavien 12 kuukauden aikana

Pearlin kokonaislukutyössä GPU:illa on yhteinen energiakatto



> Pelikortit ja B300 kohtaavat noin 1,3 J/TH:ssa; B200:kin pääsee vain 0,71:een. Siru, joka vain kertoo 7-bittisiä kokonaislukuja SRAMista, voisi uskottavasti olla 3–10 kertaa parempi analyysi.

Hashrate seuraa hintaa; säännöt muuttuvat jatkuvasti



Noin 120 miljoonaa kolikkoa, 32 % nykyisestä tarjonnasta, louhittiin kuuden ensimmäisen päivän aikana. RTX 5090 tienaa nyt noin 5–6 dollaria päivässä; korttien vuokraaminen pelkkään louhintaan tuottaa tappiota.

Teoreema pätee; kannustin ei

MITÄ HYÖTYTYÖ MAKSAA

Inferenssipuoli: pieni lisäkustannus

Pearl raportoi 5,08 % lisäaikaa Llama 70B:lle neljällä H200:lla; riippumaton testi mittasi 9,2 % pienemmän läpäisyn yhdellä Hopper-GPU:lla.

MITÄ HYÖTYTYÖ ANSAITSEE

Louhintapuoli: liian vähän hashratea

Inferenssiä palveleva kortti louhii noin 27 % omistetun louhijan tahdista prefillissä, 5,4 % chatissa, noin 1 % kun dekoodaus hallitsee.

Rationaaliset louhijat siis kertovat satunnaisia matriiseja. Hyöty on ketjun ulkopuolinen kaupallinen ongelma: jonkun on maksettava inferenssistä.

Neljä haarautumaa kahdessa kuukaudessa, seuraavaksi FP8

12. kesäkuuta
Asiantuntijasekoitusmallien kova haarautuma (lohko 71 935)

23. heinäkuuta
Vain tiheät mallit -pehmeä haarautuma (lohko 91 630)

6. elokuuta
Rankirangaistuksen pehmeä haarautuma: osa kokoonpanoista menettää 50–87,5 % tehollisesta hashratesta

11. elokuuta
Suolatun siemenen kova haarautuma: vanhat louhijat tuottavat vain virheellisiä osuuksia

Ei asetettu
PIP-3: INT7:stä FP8:aan, vain Hopper ja Blackwell hyväksytään

2/3

hyödyllinen tekoälylle, bitilleen todennettava, laitteistoneutraali: lukuformaatti saa enintään kaksi

13 bittiä

säilyy Hopperin FP8-akkumuloinnissa katkaisulla: ei toistettavissa sukupolvien välillä

≈82 %

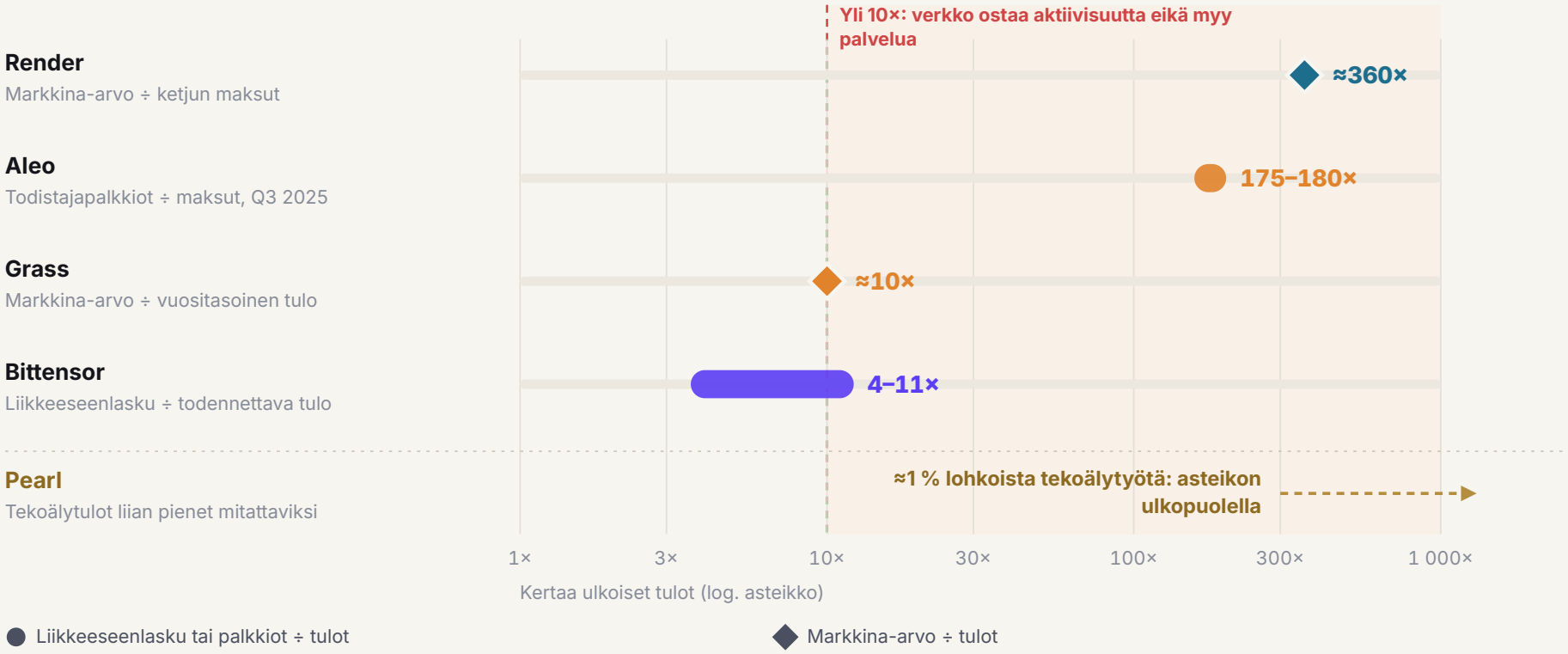
hashratesta kuluttajakorteilla, joita PIP-3 ei hyväksyisi (matalan luottamuksen malli)

Joka hallitsee työfunktiota, hallitsee laitteistosijoittajien kohtaloa analyysi.

Matriisit eivätkä nollatietotodisteet pysäytä ASICeita

Verkko	Mitä tapahtui	Mitä se opettaa
Kaspa	64 × 64 -matriisitulo tiivisteiden välissä; ASICit 16 kuukauden jälkeen, noin 1 000× GPU-tehokkuus; paras tienaa nyt 0,86 dollaria päivässä	Matriisi ei ole hyödyllinen eikä ASIC-suojattu
Aleo	Synteettinen SNARK-pulma; omistetut koneet viiden kuukauden jälkeen; todistajapalkkiot 175–180× maksut	Synteettinen työ pyörii tuella
Qubic	Väittää kouluttavansa tekoälyä; sen laskenta louhi Moneroa (väitetysti 51 %) ja nyt Dogecoinia	Yleiskäyttöinen PoW voidaan kaapata ulkopuolelta
Bittensor	Panospainotettu pisteytys; noin 70 milj. dollaria vuodessa todennettavaa tuloa vastaan yli 300 milj. dollarin liikkeeseenlasku	Ainoa, jolla on mittavaa ulkoista tuloa
Monero, Sia, Ethereum	Haarautumat tekivät ASICeista hyödyttömiä; Mergen jälkeen alle 20 % louhijoista löysi uutta työtä	Laitteisto, jolla on toinen markkina, selviää

Tukikerroin on rehellisin terveystarkastus



> Kun kerroin ylittää noin 10 kertaa ulkoiset tulot, verkko ostaa aktiivisuutta eikä myy palvelua. Pearlin tekoälytulot ovat liian pienet asteikolle sijoitettaviksi.

Todellista mutta pientä kysyntää, ja arvo siirtyy osakkeisiin

- **Laskentamarkkinat**

  Renderin ketjussa maksetut maksut noin 2,35 milj. dollaria vuodessa; Akashin H100 2,73 dollaria tunnilta voittaa AWS:n ja Googlen, ei Vast.aita tai RunPodia.

- **Koulutus**

  8–40 miljardin parametrin malleja koulutettu internetin yli; INTELLECT-3 palasi 512 H200:aan InfiniBandilla.

- **Todennettava tekoäly**

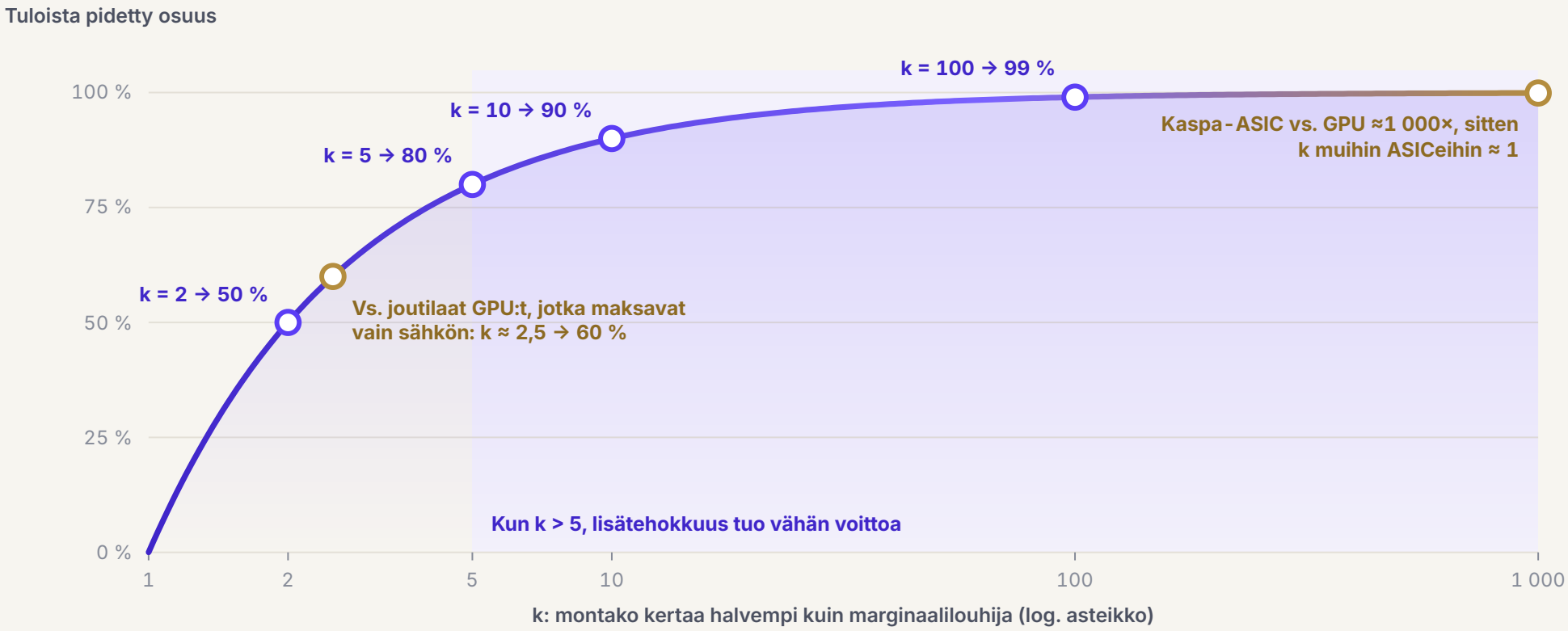
  TEE:t lisäävät alle 7 % ja ovat tuotannossa; TEE.fail murtoi attestoinnin 1 000 dollarin väliinkytkimellä; zkML todistaa GPT-2:n 174 tokenia minuutissa.

- **Agentit ja data**

  x402:n agenttien käynnistämät virrat noin 5 000–11 000 dollaria kuussa; Grass 17 milj. dollaria datatuloja H1 2026.

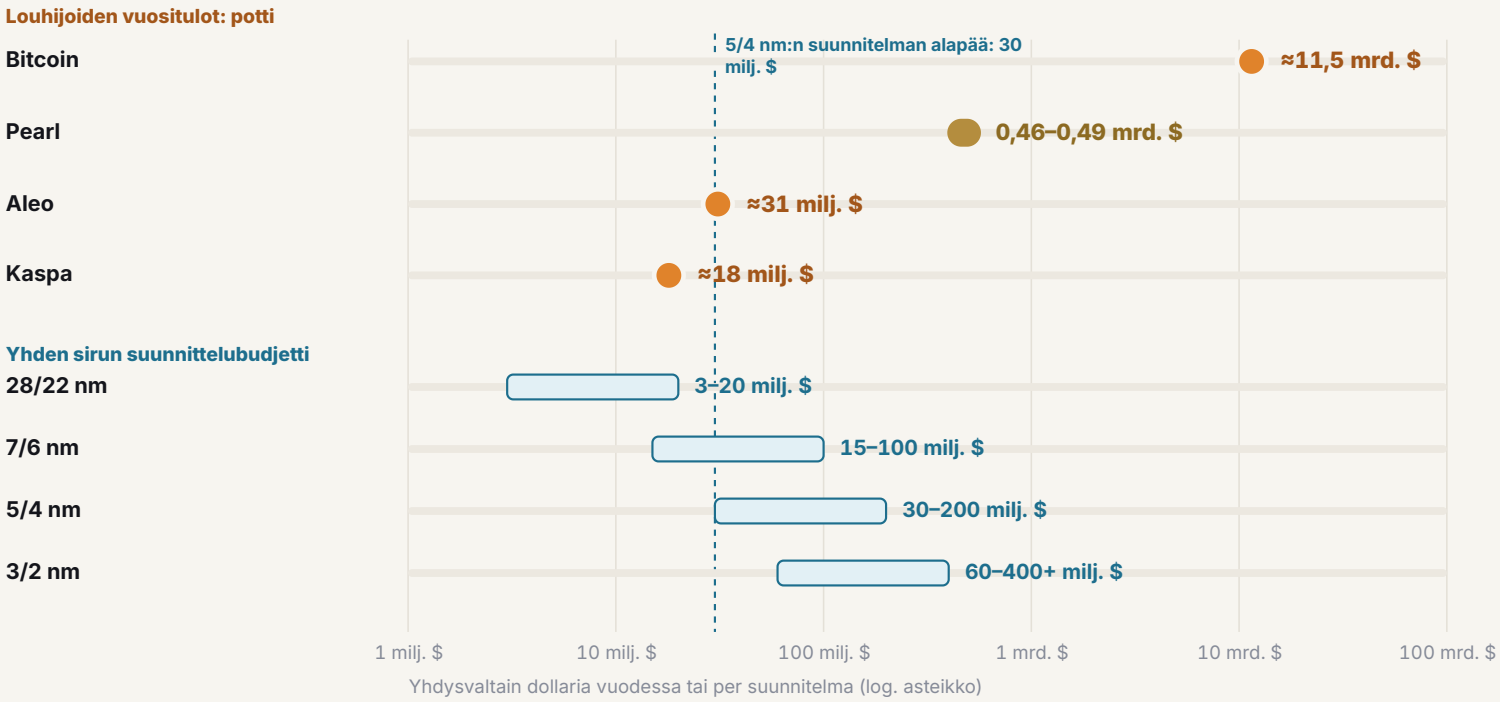
Neljä keskitetyllä infrastruktuurilla toimivaa osakeyhtiötä on arvoltaan noin 8,5 mrd. dollaria, suunnilleen yhtä paljon kuin kaikki protokolla- ja sovelluskerroksen tekoälytokenit.

Miksi tehokkuus lakkaa kannattamasta, kun k > 5



Voittokatto ≈ R × (1 − 1/k). Kun ASICeista tulee marginaalilouhijoita, k nollautuu muihin ASICeihin nähden; vain sähkön maksaviin joutilaisiin GPU:ihin nähden k on noin 2,5 arvio.

Useimmat potit ovat pienempiä kuin yhden sirun suunnittelubudjetti



Takaisinmaksun hashrate h* = NRE ÷ [R × (1 − 1/k) × T × p]. Pearlille 20 milj. dollarin NRE:llä ja k = 5: noin 4,9 EH/s vuoden ajan, jos säännöt pysyvät, 9,8 EH/s, jos niiden pysymisen todennäköisyys on puolet **arvio**.

Viisi sirutyyppiä, viisi vastausta





Pearl-tyyppinen PoUW-louhintasiru

EI NYT

k: ei HBM:ää eikä yleisyksiköitä: 3–10× per op (päätelmä)

Toinen markkina: tekoälyinferenssi, jos yleinen INT8/FP8-GEMM

Panosta inferenssi edellä -siruun, joka voi louhia, ei omaan INT7-osaan



Bitcoinin SHA-256-louhintasiru

PYSY EROSSA

k: ≤1 vakiintuneisiin nähden

Toinen markkina: lähes ei mitään

Vain omalla sähköllä, kapealla muodolla tai IP:nä



Tekoälyn koulutussiru

IP:TÄ, EI SIRUJA

k: 1,1–1,8× samalla tarkkuudella

Toinen markkina: —

Paketointi ja HBM ratkaisevat; rakenna IP:tä, chipletejä, palveluja



Tekoälyn inferenssisiru

RAKENNA

k: luovu yleisyydestä: 10–20× väitetty

Toinen markkina: se on päämarkkina

Sido asiakas, valitse sitten lukitus



ZK-todistuskiihdytin

ODOTA JA SUOJAUDU

k: 10–100× GPU:t, väitetty

Toinen markkina: rajallinen ZK:n ulkopuolella

Ohjelmoitavat MSM- ja NTT-moottorit; FPGA ensin



FHE-kiihdytin

ASEMOIDU AJOISSA

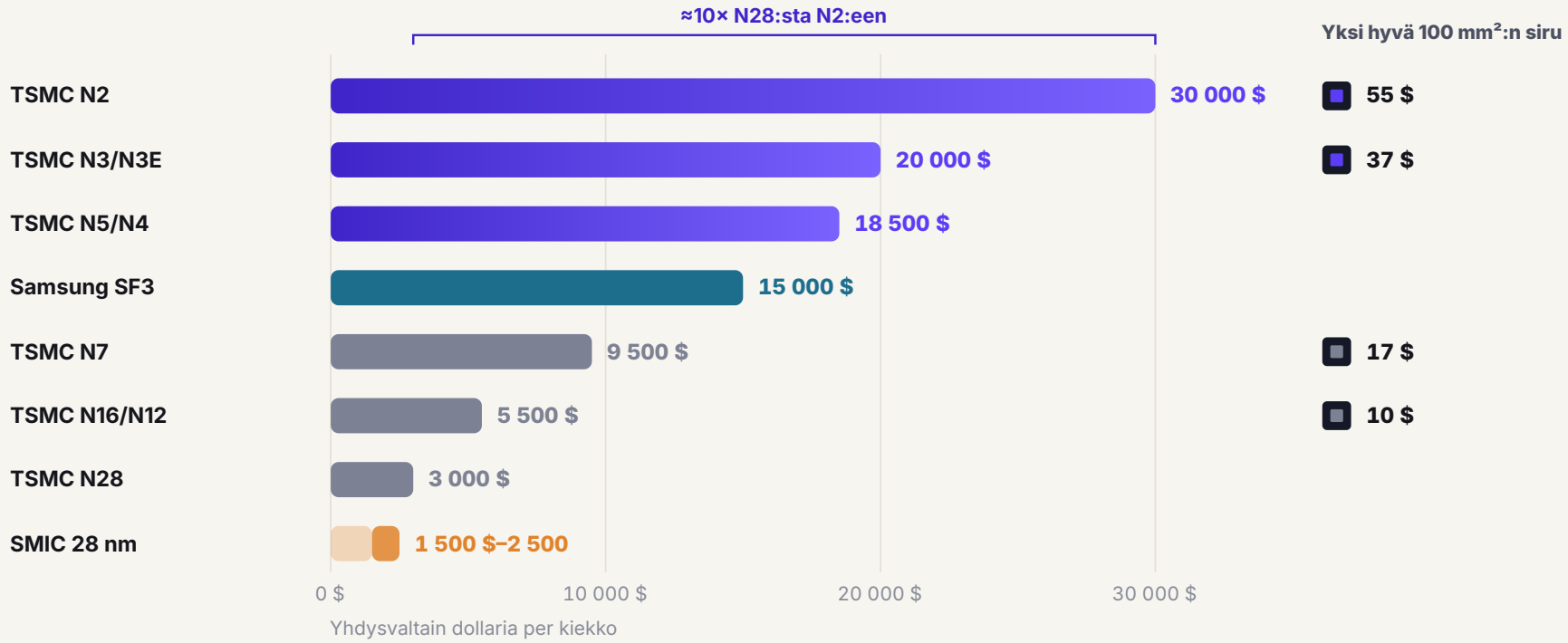
k: 1 074–5 547× Xeon (Heracles)

Toinen markkina: salattu laskenta, yksityinen tekoäly

Ikkuna 2027–2029; validoi kevyin investoinnein

> Mikään verkko ei nykyään tarjoa yhtä aikaa suurta pottia, vakaita sääntöjä ja yli 1:n k:ta: bitcoinin k kuuluu vakiintuneille, Pearlin säännöt ovat epävakaimmat, Kaspan ja Aleon potit liian pienet.

Huippusolmun kiekko maksaa kymmenen kertaa kypsän solmun kiekon



> Anna suurimman elinkaarikustannuksen ratkaista: energia ympäri vuorokauden laskeville siruille, paketointi ja HBM koulutussiruille (63 % H100:n kustannuksesta), SRAM vai HBM inferenssisiruille.

PROSESSISOLMUT

Solmu kullekin sirulle ja tiimille

Siru	Pieni tiimi	Skaalautunut yritys	Manner-Kiinan polku
PoUW-louhintasiru	28 tai 16/12 nm MPW; ensimmäinen volyymi N7/N6	N3/N3E tai Samsung SF3	SMIC N+1/N+2 toimii, noin 40–50 % enemmän per siru
SHA-256-louhintasiru	Älä tavoittele kärkeä	3 nm:n luokka	Vaikea yltää huippusolmun tehokkuuteen
Tekoälyn koulutussiru	IP, chipletit, suunnittelupalvelut	N3P, sitten N2/A16 CoWoSilla ja HBM:llä	SMIC N+2/N+3 kotimaisella HBM:llä
Tekoälyn inferenssisiru	SRAM-keskeinen N6/N7:llä tai N4/N5/SF4:llä	N3/N2 HBM:llä tai SRAM-chipletit	SMIC N+2 LPDDR:llä tai GDDR:llä
ZK- ja FHE-kiihdyttimet	Ensin FPGA tai 16/12 nm MPW	N5/N3; FHE HBM:llä	ZK toimiva; FHE:tä rajoittaa HBM

VAIHEITTAINEN BUDJETTI

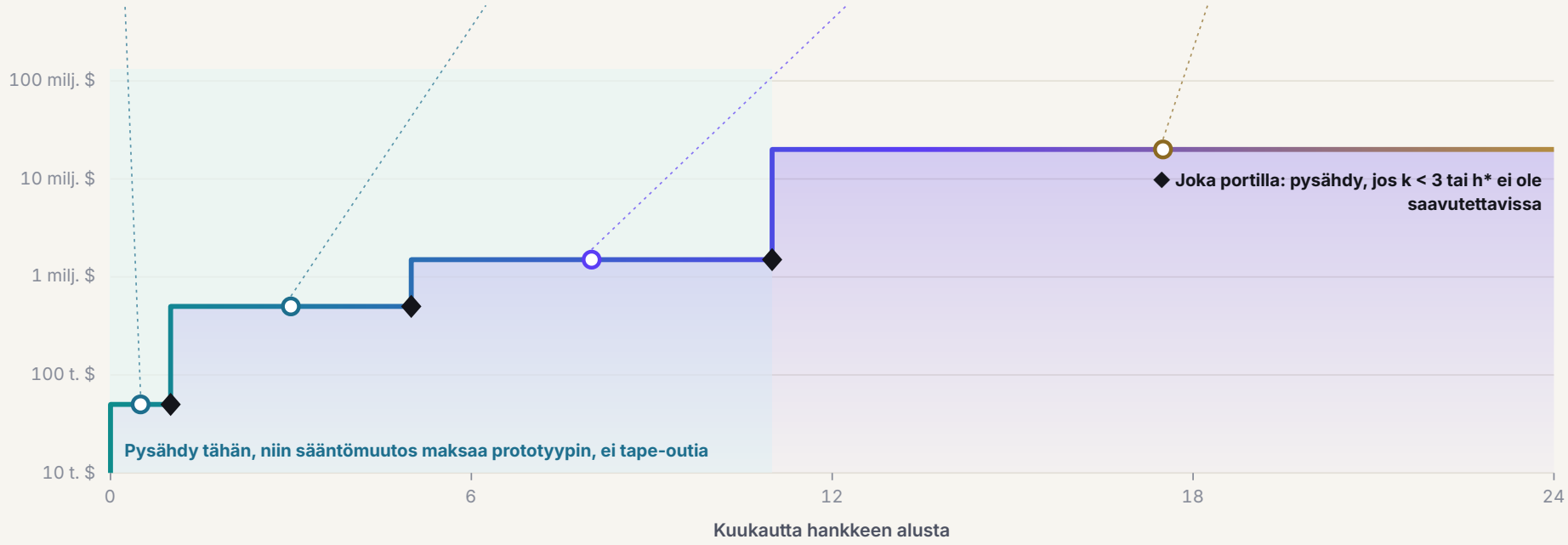
Osta näyttöä ennen maskeja

Portti 0 · Malli
≈50 t. $ · viikkoja
J/op ja $/op aritmetiikasta, SRAMista ja I/O:sta

Portti 1 · FPGA
≈0,5 milj. $ · kuukausia
Todellinen kuorma päästä päähän: osuudet tai tokenit

Portti 2 · MPW
≈1,5 milj. $ · kk 11
Mitattu pii korvaa mallin

Portti 3 · Maskit ja 1. erä
≈20 milj. $ · kk 24
N7-maskit ≈3,5 milj. $ 15–100 milj. $:n suunnittelussa



Malli, FPGA ja MPW tuottavat mitattua piitä noin 1,5 miljoonalla dollarilla yhdessätoista kuukaudessa; maskisarja ja ensimmäinen erä maksavat yli kymmenen kertaa niin paljon. Pysähdy ennen maskeja, kunnes ostaja tai protokollaversio on kiinnitetty.

MAHDOLLISUUDET

Krypto ensimmäisenä asiakkaana, tekoäly toisena markkinana

Räätälöidyt sirut

- Kysyntä on ylivoimaisesti tekoälyä: Broadcomilla noin 58 mrd. dollaria tekoälypuolijohteita tilikaudella 2026
- Louhintasiruosaaminen siirtyy: matalajänniteryhmät, kilowattiluokan virransyöttö, nopeat tape-outit
- Voita itsenäisellä markkinareitillä, ei louhintakanavilla

Tekoälykehitys

- Tunnit ovat hyödyke: 25–49 dollaria tunnilta Clutchissa
- Arvo on liitoskohdissa: kernelit räätälöidyille siruille, louhinta inferenssipalvelun sisällä
- Todennettava inferenssi: TEE:t sekä ZK-pistokokeet

Tekoäly × krypto -järjestelmät

- Kerroksellinen todennus: TEE tai otanta, sitten kiistat tai ZK-pistokokeet
- Jakelu ja likviditeetti ovat esteitä, eivät kustannukset
- Sido laskennan ostaja ennen tokenia

Kolme polkua, jokaisella pieni ensiaskel

Polku	Ensiaskel
A. Inferenssi edellä -kiihdytin, joka voi myös louhia	Neljän viikon selvitys SRAM-pohjaisen INT8/FP8-ryhmän J/op- ja $/op-arvoista vs. RTX 5090 ja H100, sitten FPGA tai kypsän solmun MPW
B. Räätälöidyn piin palvelut: ensin krypto, sitten tekoäly	Tee tämän raportin NRE- ja kannattavuusmallista maksullisia toteutettavuusselvityksiä, joissa on välitavoitteet ja kiinteä protokollaversio
C. Tekoälynatiivi verkko, jolla on ostaja ennen tokenia	Suunnittelumuistio kerroksellisesta todennuksesta ja valmistajaneutraalista kanonisesta aritmetiikasta, kirjoitettuna yhden nimetyn inferenssiostajan kanssa

Enintään kolme polkua, jokainen testattu ennen kuin rahaa sidotaan analyysi**.**

Mitä seurata ja mitä kysyä

SEURATTAVAT MERKIT

Milloin tahansa	Pearlin FP8-aktivointikorkeus ja se, jakautuuko ketju
Kuukausittain	Tekoälytyötä sisältävien lohkojen osuus Pearlissa
Neljännesvuosittain	Bittensorin todennettava tulo vs. liikkeeseenlasku; agenttien käynnistämät x402-virrat
Tammikuu 2027	TSMC:n raportoitu 3–6 %:n hinnankorotus 2 nm:lle ja 3 nm:lle
Q1 2027	FP4 Pearliin, perustajien AMA:n mukaan raportoidusti
Huhtikuu 2028	Bitcoinin seuraava puoliintuminen

KYSYTTÄVÄT KYSYMYKSET

01 Kuka hallitsee työfunktiota?

02 Mikä on tukikerroin?

03 Mitä seuraava portti maksaa, ja mikä pysäyttää sinut?

04 Mikä on takaisinmaksun hashrate, p mukaan lukien?

05 Mikä on sirun toinen markkina?

06 Kuka on ensimmäinen maksava asiakas, nimeltä?

Näitä alueita voimme tutkia yhdessä teknisen vaihdon ja teknisen yhteistyön kautta: räätälöidyt sirut, tekoälykehitys ja tekoäly × krypto -järjestelmät.

i@tanshuai.com · tanshuai.com