調査ノート · 2026年11月

計算は合意である

2026年のAI × 暗号資産 × 半導体：Pearlから

Pearl · 有用な作業 · DePINとエージェント · ASICの経済性 · プロセスノード · 段階的予算

タン・シュアイ
tanshuai.com · i@tanshuai.com



定理は成り立つが、インセンティブは成り立たない

01 Pearlは工学として機能するが、まだ有用な作業ではない

約90 EH/sの整数行列積がチェーンを守っているが、実際のAI作業を含むブロックは約1%にすぎない。

02 有償需要は推論、データ、プライバシーにある

Bittensorの検証可能な収益は年間約7,000万ドル、Grassは2026年上半期に1,700万ドル、TEEは本番稼働；エージェント決済は月約5,000〜11,000ドル。

03 ASICが報われるのは、大きなパイ、安定したルール、第二の市場があるときだけ

利益上限はR × (1 − 1/k)。今日、三つすべてを備えたネットワークはない 分析 。

≈90 EH/s

2026年11月13日のPearl：H100約122,000基分の整数演算性能

≈1%

実際のAI作業を含むPearlのブロック（Blockworks）

4–11×

Bittensorの発行の、検証可能な収益に対する倍率

六つのセクターで見るAI × 暗号資産：有償需要はどこにあるか

有用作業チェーン 01

本物だが小さい

年間≈7,000万ドル

Bittensorの検証可能な外部収益

シグナル： 発行は収益の4–11倍；PearlのAIブロック≈1%

仕組みは機能する；有用性には支払い手が必要

分散型計算資源 02

本物だが小さい

年間235万ドル

Renderのオンチェーン手数料、検証可能な中で最大

シグナル： 時価総額は手数料の≈360倍

大半はコモディティ推論の再販

学習と推論 03

利益はエクイティへ

年間1億ドル超

Prime Intellect、集中型GPU上のエクイティ企業

シグナル： Gensynの学習メインネットは未稼働

進歩は本物；利益はエクイティへ

検証可能なAI 04

初期段階

398

PhalaのTEEクラウドの有料ユーザー（2025年末）

シグナル： 有償のzkMLは開示なし

TEEは本番稼働；zkMLは初期段階

エージェント決済 05

需要以前

月5,000–11,000ドル

実際にエージェントが発起したx402決済

シグナル： ≈2億件の取引、大半はシグナリング

レールが先に来て、需要はまだ

データネットワーク 06

本物の買い手

1,700万ドル

Grassのデータ収益、2026年上半期（自己申告）

シグナル： 時価総額は年率換算収益の≈10倍

本物の買い手がいる数少ないセクター

> 補助金はコールドスタートの燃料であり、ビジネスモデルではない。暗号資産は流通と決済を担い、利益はエクイティが取る。少なくとも2026年においては。

1回の積和演算が1ハッシュ

定理からメインネットへ

KomargodskiとWeinstein（2025年4月）：任意の行列積に対する、オーバーヘッド1 + o(1)の有用作業証明。Pearlのメインネットは2026年4月27日に始動。

仕組み

マイナーはノイズ付き行列を掛け合わせ、各タイルのアキュムレータをハッシュして宝くじの券にし、当選タイルを60 KB未満のPlonky2証明で証明する。

単位

1 Hは1回のクレジットされたINT7 × INT7 → INT32積和演算：ブロックチェーンのセキュリティ予算がテンソル演算性能で値付けされる。

2026年11月13日のPearl

89.77 EH/s

ネットワークハッシュレート（独立フルノード）

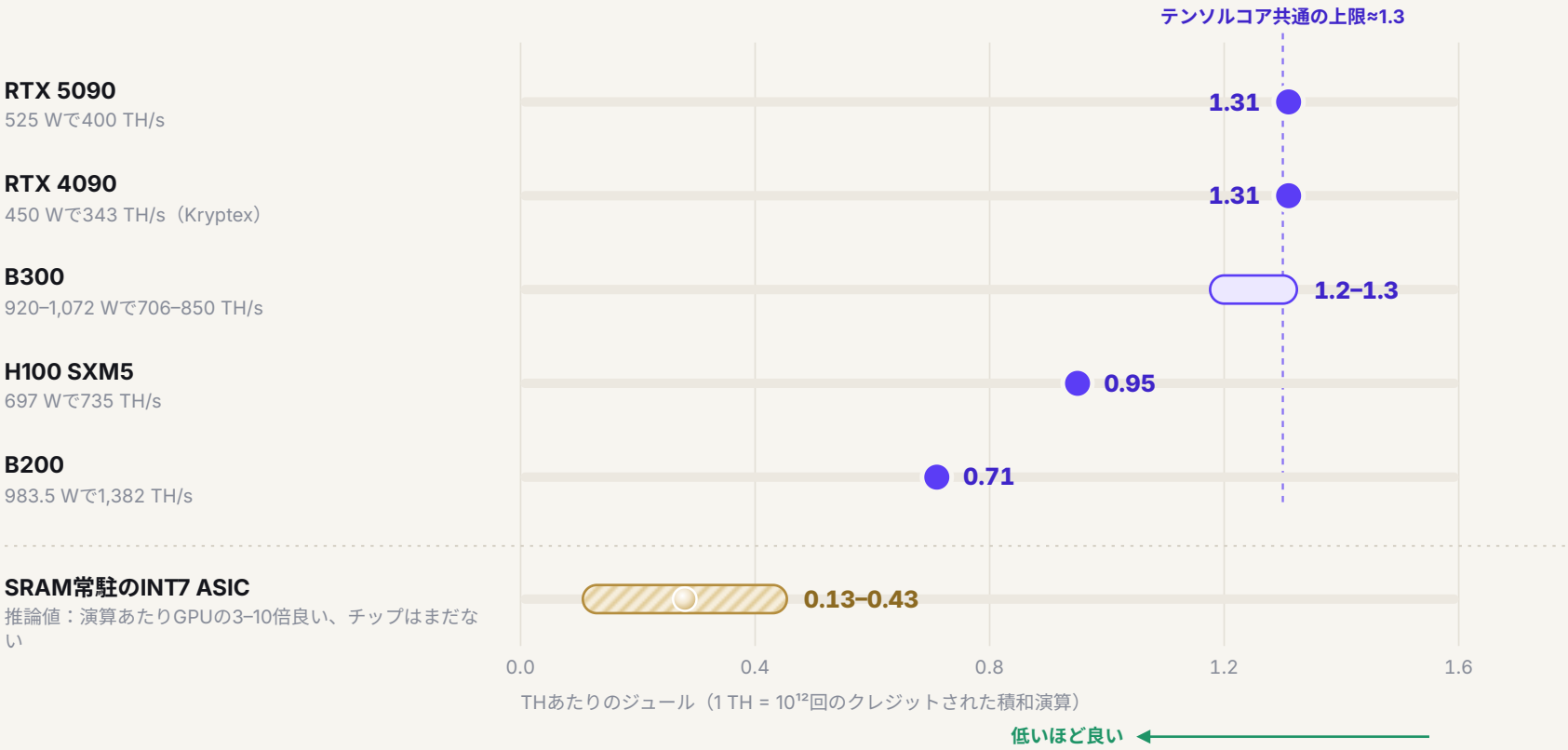
≈5億ドル

時価総額；完全希薄化後は約28億ドル

+78%

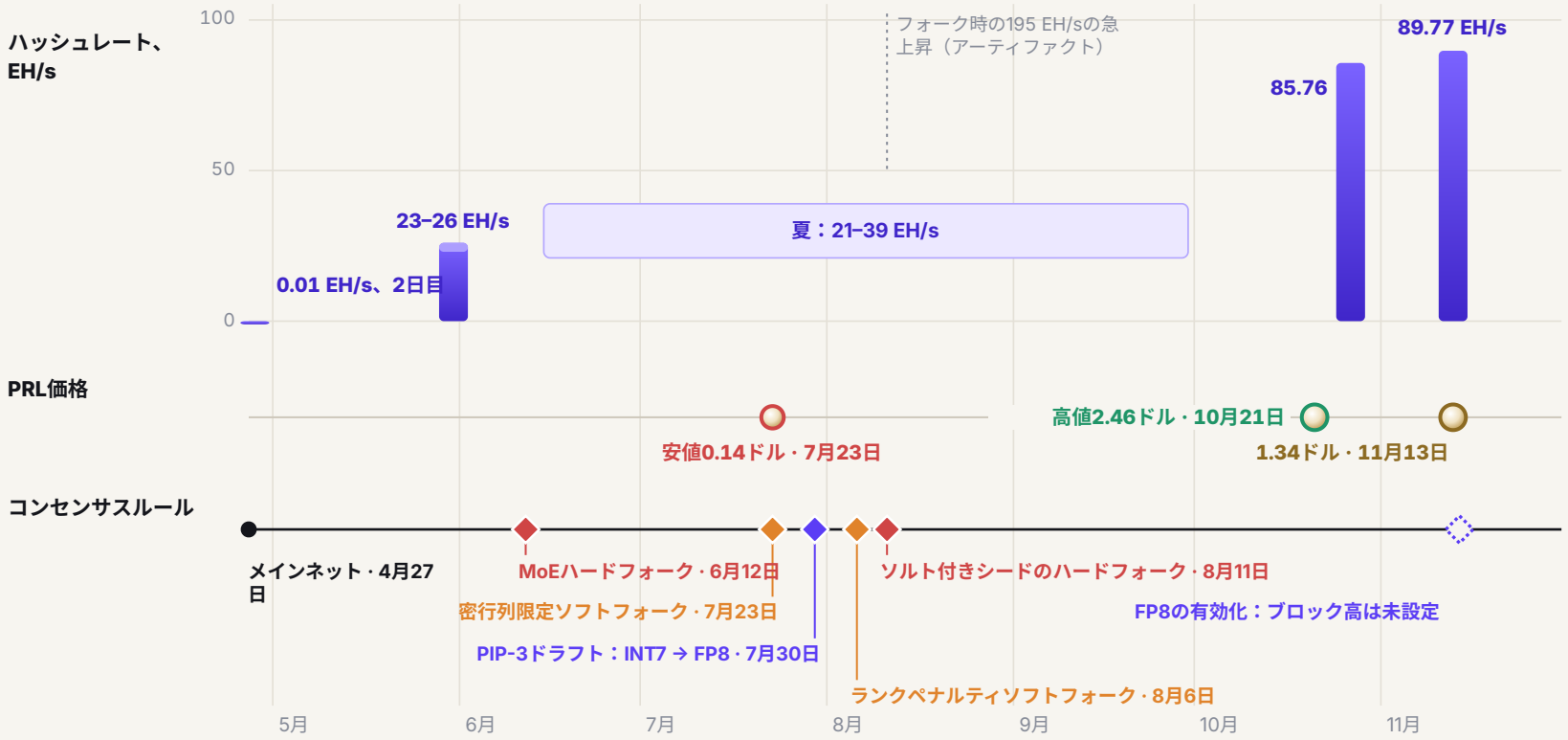
今後12か月の新規供給

Pearlの整数演算では、GPUは共通のエネルギー上限を持つ



> ゲーミングカードとB300は約1.3 J/THで並び、B200でさえ0.71にとどまる。SRAMから7ビット整数を掛けるだけのチップなら、3〜10倍良くなることも十分ありうる 分析 。

ハッシュレートは価格に従い、ルールは変わり続ける



現在の供給量の32%にあたる約1億2,000万コインが最初の6日間で採掘された。RTX 5090は現在1日約5〜6ドルを稼ぐ。マイニングのためだけにカードを借りると損をする。

定理は成り立つが、インセンティブは成り立たない

有用な作業のコスト

推論側：オーバーヘッドは小さい

Pearlは4基のH200でのLlama 70Bで時間が5.08%増えると報告；独立したテストは1基のHopper GPUで9.2%のスループット低下を測定。

有用な作業の稼ぎ

マイニング側：ハッシュレートが少なすぎる

推論を提供するカードのマイニングは専用マイナー比で、プリフィルで約27%、チャットで5.4%、デコード中心では約1%。

だから合理的なマイナーはランダムな行列を掛ける。有用性はオフチェーンの商業的な問題であり、誰かが推論に支払わなければならない。

2か月で4回のフォーク、次はFP8

6月12日
Mixture-of-Expertsハードフォーク（ブロック71,935）

7月23日
密行列限定ソフトフォーク（ブロック91,630）

8月6日
ランクペナルティソフトフォーク：一部の構成は実効ハッシュレートの50–87.5%を失う

8月11日
ソルト付きシードのハードフォーク：旧来のマイナーは無効なシェアしか作れない

未定
PIP-3：INT7からFP8へ、HopperとBlackwellのみ認める

3つ中2つ
AIに有用、ビット単位で検証可能、ハードウェア中立：数値形式が満たせるのは多くても二つ

13ビット
HopperのFP8累算が切り捨てで保持するビット数：世代をまたいで再現できない

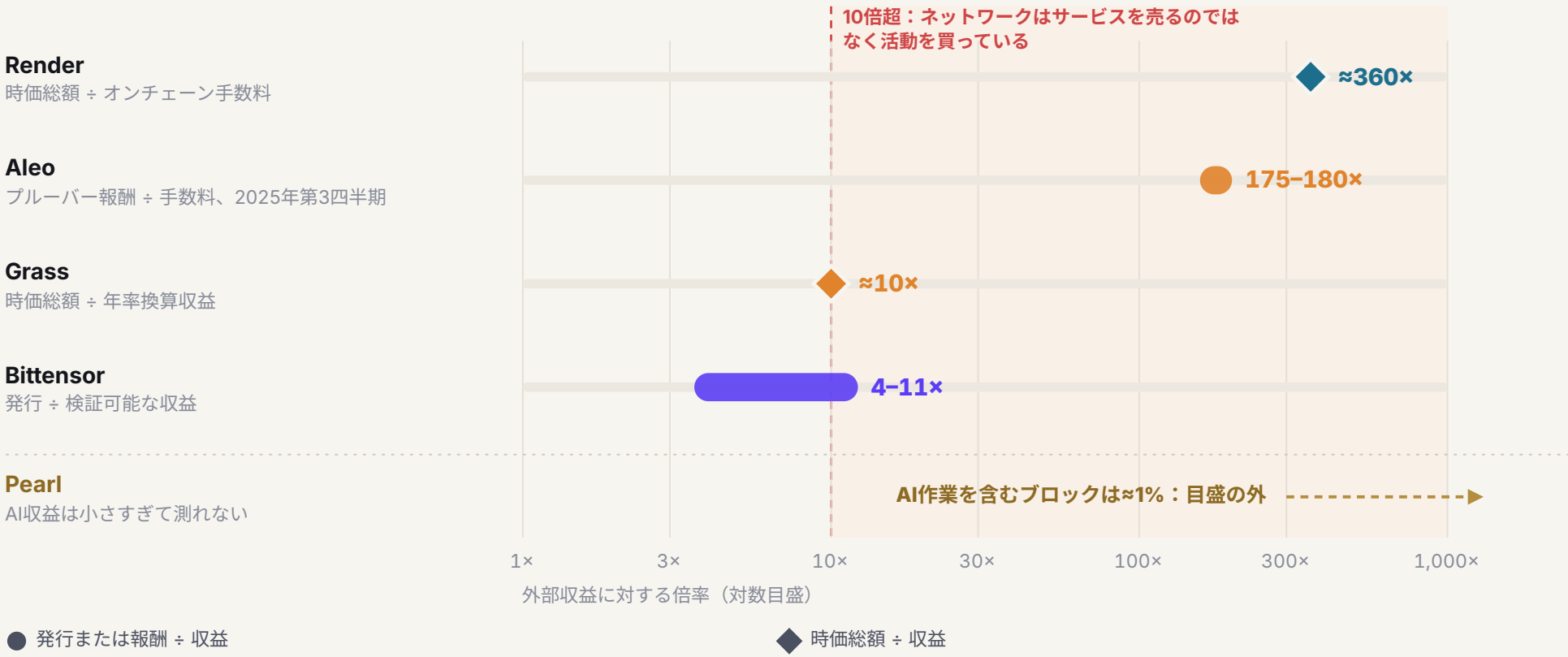
≈82%
PIP-3が認めないコンシューマー向けカードのハッシュレート比率（信頼度の低いモデル）

> **作業関数を支配する者が、ハードウェア投資家の運命を支配する** 分析 **。**

行列もゼロ知識もASICを止められない

ネットワーク	何が起きたか	何を教えるか
Kaspa	ハッシュの間に64 × 64の行列積；16か月後にASIC、GPUの約1,000倍の効率；最良機でも今は1日0.86ドル	行列は有用でもなく、ASIC耐性もない
Aleo	合成SNARKパズル；5か月後に専用マシン；プルーバー報酬は手数料の175–180倍	合成作業は補助金で動く
Qubic	AI学習をうたう；その計算資源はMonero（51%を主張）を、現在はDogecoinをマイニング	汎用PoWは外部から乗っ取られうる
Bittensor	ステーク加重スコアリング；年間約7,000万ドルの検証可能な収益に対し3億ドル超の発行	一定規模の外部収益を持つ唯一の例
Monero、Sia、Ethereum	フォークでASICが文鎮化；Merge後に新しい仕事を見つけたマイナーは20%未満	第二の市場を持つハードウェアは生き残る

補助金倍率は最も正直な健全性チェック



外部収益の約10倍を超えると、ネットワークはサービスを売るのではなく活動を買っている。PearlのAI収益は小さすぎて目盛に載せられない。

本物だが小さい需要と、エクイティへ移る価値

- **計算資源市場**

  Renderのオンチェーン手数料は年間約235万ドル；AkashのH100は1時間2.73ドルでAWSとGoogleより安いが、Vast.aiやRunPodには及ばない。

- **学習**

  インターネット越しに80億〜400億パラメータを学習；INTELLECT-3はInfiniBand接続の512基のH200に戻った。

- **検証可能なAI**

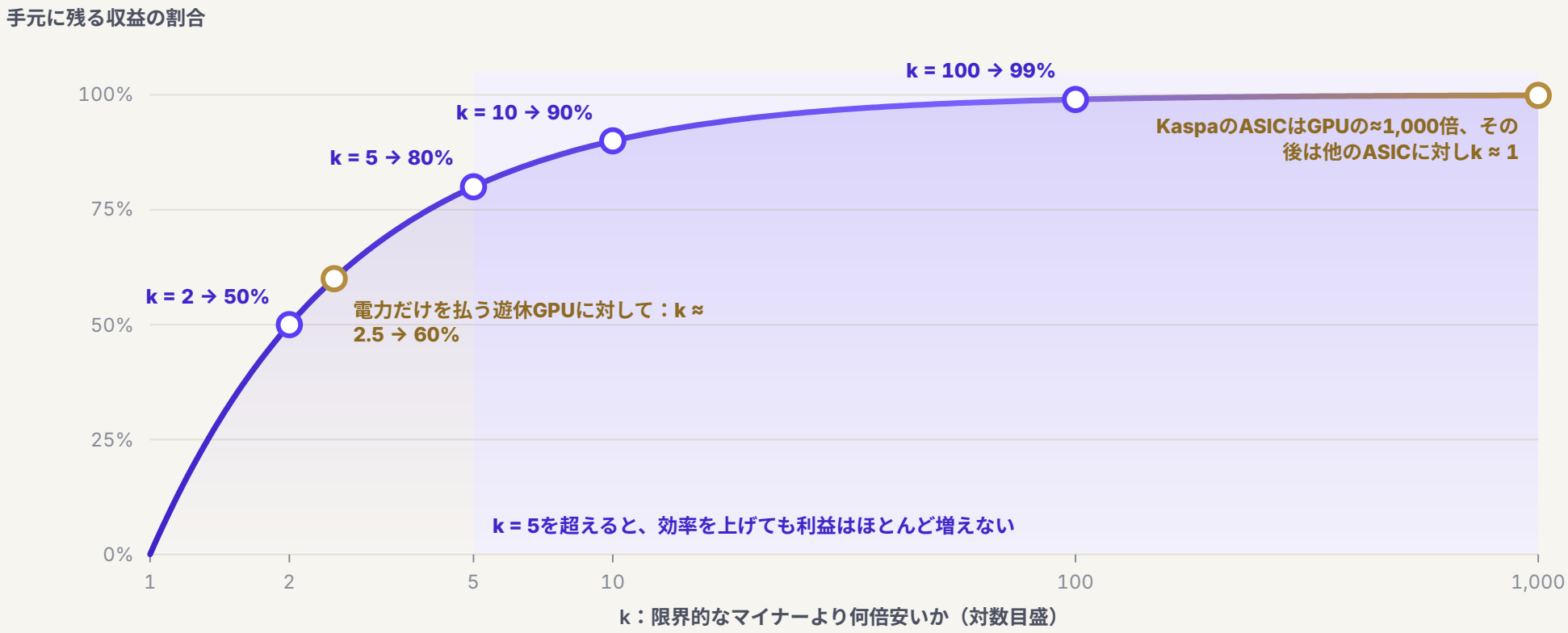
  TEEの追加負荷は7%未満で本番稼働；TEE.failは1,000ドルのインターポーザーで認証を破った；zkMLはGPT-2を毎分174トークンで証明。

- **エージェントとデータ**

  x402のエージェント発起フローは月約5,000〜11,000ドル；Grassは2026年上半期に1,700万ドルのデータ収益。

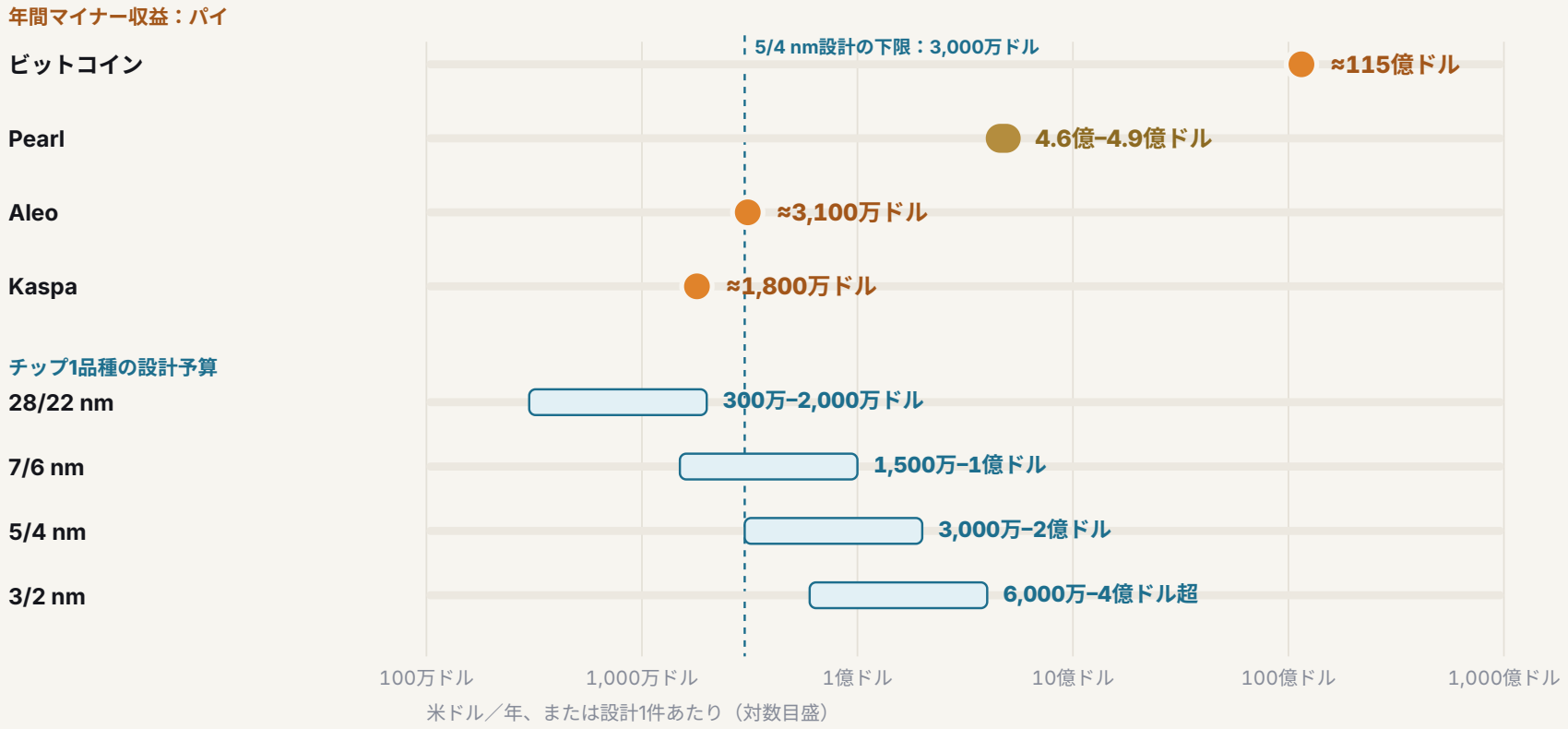
> **集中型インフラ上のエクイティ企業4社の価値は約85億ドルで、プロトコル層とアプリケーション層のAIトークン全体とほぼ同じである。**

なぜk = 5を超えると効率が報われなくなるのか



利益上限 ≈ R × (1 − 1/k)。ASICが限界的なマイナーになると、kは他のASICに対してリセットされる。電力だけを払う遊休GPUに対しては、kは約2.5である 推計 。

大半のパイはチップ1品種の設計予算より小さい



回収に必要なハッシュレートh* = NRE ÷ [R × (1 − 1/k) × T × p]。PearlでNRE 2,000万ドル、k = 5なら、ルールが維持されれば約4.9 EH/sを1年、維持の確率が五分五分なら9.8 EH/s 推計 。

チップの種類ごとに

五つのチップの種類、五つの答え



Pearl型PoUWマイニングチップ

今ではない

k： HBMも汎用ユニットもなし：演算あたり3–10倍（推論値）

第二の市場： 汎用INT8/FP8 GEMMならAI推論

専用INT7チップではなく、マイニングもできる推論優先チップに賭ける



ビットコインSHA-256マイニングチップ

参入しない

k： 既存勢力に対して≤1

第二の市場： ほぼない

自前の電力、ニッチな形態、またはIPとしてのみ



AI学習チップ

チップではなくIP

k： 同じ精度で1.1–1.8倍

第二の市場： —

パッケージングとHBMが決める；IP、チップレット、サービスを作る



AI推論チップ

作る

k： 汎用性を手放す：10–20倍と主張

第二の市場： それ自体が主な市場

顧客と契約し、それからロックインを選ぶ



ZK証明アクセラレータ

待ってヘッジ

k： GPUの10–100倍と主張

第二の市場： ZK以外では限定的

プログラマブルなMSMとNTTのエンジン；まずFPGA



FHEアクセラレータ

早めに布石

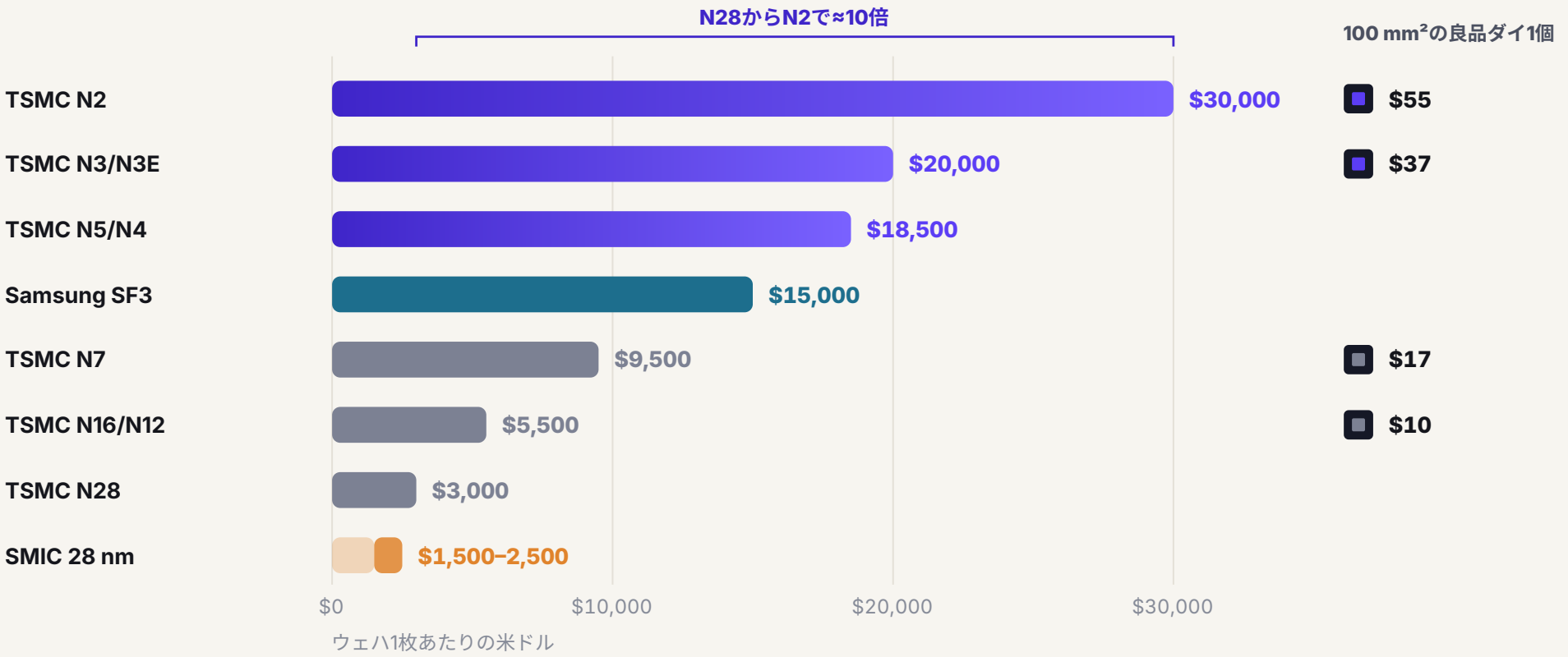
k： Xeonの1,074–5,547倍（Heracles）

第二の市場： 暗号化計算、プライベートAI

2027–2029年の機会；軽い資産で検証

> 大きなパイ、安定したルール、1を超えるkを同時に備えたネットワークは今日ない。ビットコインのkは既存勢力のもの、Pearlのルールは最も不安定、KaspaとAleoのパイは小さすぎる。

先端ウェハは成熟ウェハの10倍のコストがかかる



最大の生涯コストに選ばせる。常時稼働の計算チップならエネルギー、学習チップならパッケージングとHBM（H100のコストの63%）、推論チップならSRAMかHBMかの選択。

チップとチームごとのノード

チップ	小さなチーム	規模の大きい企業	中国本土での道筋
PoUWマイニングチップ	28または16/12 nmのMPW；最初の量産はN7/N6	N3/N3EまたはSamsung SF3	SMIC N+1/N+2で実現可能、ダイあたり約40–50%高い
SHA-256マイニングチップ	フロンティアを追わない	3 nmクラス	先端ノードの効率に並ぶのは難しい
AI学習チップ	IP、チップレット、設計サービス	N3P、次いでCoWoSとHBM付きのN2/A16	SMIC N+2/N+3と国産HBM
AI推論チップ	N6/N7またはN4/N5/SF4のSRAM中心	HBM付きN3/N2、またはSRAMチップレット	LPDDRまたはGDDR付きSMIC N+2
ZKとFHEのアクセラレータ	まずFPGAまたは16/12 nmのMPW	N5/N3；FHEはHBM付き	ZKは実現可能；FHEはHBMが制約

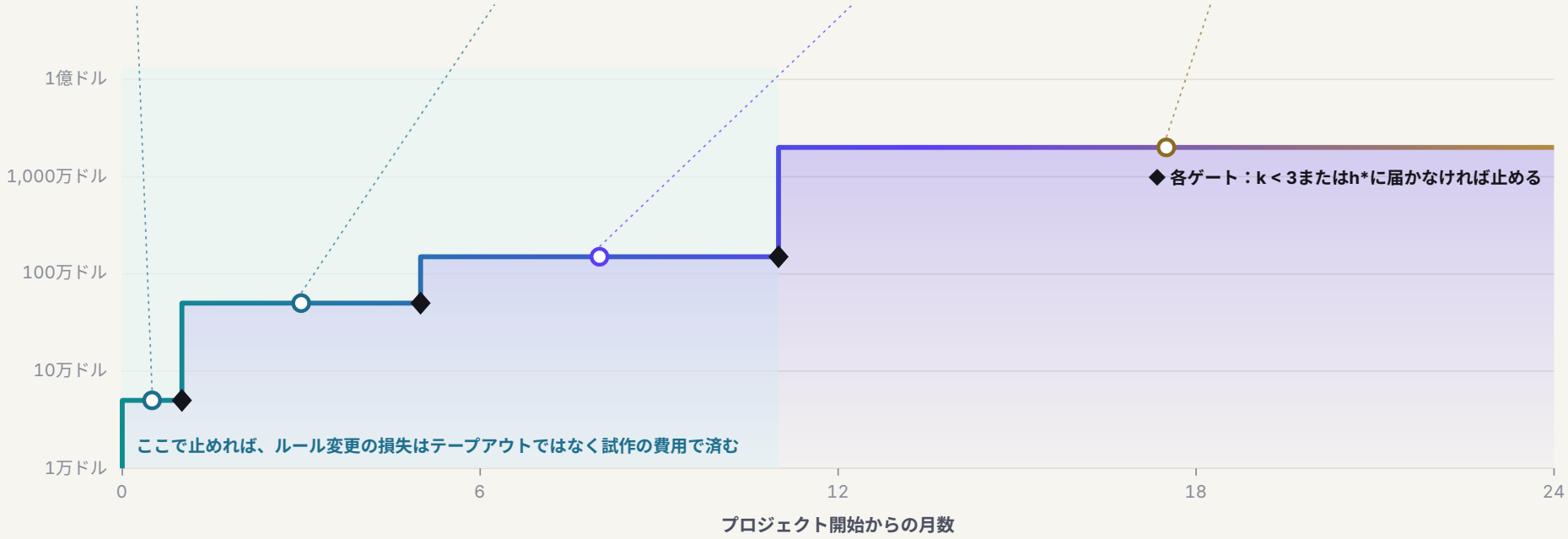
マスクの前に証拠を買う

ゲート0 · モデル
≈5万ドル・数週間
演算、SRAM、I/OからのJ/opと$/op

ゲート1 · FPGA
≈50万ドル・数か月
実際のワークロードをエンドツーエンドで：シェアまたはトークン

ゲート2 · MPW
≈150万ドル・11か月目
実測のシリコンがモデルに取って代わる

ゲート3 · マスクと初回ロット
≈2,000万ドル・24か月目
N7のマスク≈350万ドル、設計予算は1,500万–1億ドル



モデル、FPGA、MPWで、11か月・約150万ドルで実測のシリコンに至る。マスクセットと初回ロットはその10倍以上かかる。買い手かプロトコルのバージョンが固まるまで、マスクの前で止める。

暗号資産を最初の顧客に、AIを第二の市場に

カスタムチップ

- 需要は圧倒的にAI：Broadcomの2026会計年度のAI半導体は約580億ドル
- マイニングチップの技術は移転できる：低電圧アレイ、キロワット級電力、速いテープアウト
- 勝つにはマイニングの販路ではなく、独立した市場への道筋

AI開発

- 時間はコモディティ：Clutchで1時間25〜49ドル
- 価値は継ぎ目にある：カスタムチップ向けカーネル、推論サービング内のマイニング
- 検証可能な推論：TEEとZKのスポットチェック

AI × 暗号資産システム

- 階層型の検証：TEEまたはサンプリング、次に異議申し立てまたはZKスポットチェック
- 障壁はコストではなく、流通と流動性
- トークンの前に計算資源の買い手と契約する

私なら何をするか

三つの道、それぞれに小さな最初の一歩

道	最初の一歩
A. マイニングもできる推論優先のアクセラレータ	SRAM常駐のINT8/FP8アレイのJ/opと$/opを、RTX 5090とH100に対して評価する4週間の調査。次にFPGAまたは成熟ノードのMPW
B. カスタムシリコンサービス：暗号資産が先、AIが次	本レポートのNREと損益分岐のモデルを、マイルストーンと固定したプロトコルバージョン付きの有償の実現可能性調査にする
C. トークンより先に買い手がいるAIネイティブなネットワーク	階層型の検証とベンダー中立な正準演算についての設計ノートを、名前の挙がった推論の買い手1社とともに書く

> **道は多くても三つ、それぞれ資金を投じる前に検証する 分析 。**

注目すべきこと、そして尋ねるべき質問

注目点	
随時	PearlのFP8有効化高と、チェーンが分裂するかどうか
毎月	PearlでAI作業を含むブロックの割合
四半期ごと	Bittensorの検証可能な収益と発行の比較；エージェント発起のx402フロー
2027年1月	報じられたTSMCの2 nmと3 nmの3–6%値上げ
2027年第1四半期	創業者のAMAで報じられたPearlのFP4
2028年4月	ビットコインの次の半減期

尋ねるべき質問

01 作業関数を支配しているのは誰か？

02 補助金倍率はいくつか？

03 次のゲートの費用は、そして何で止めるか？

04 pを含めた回収に必要なハッシュレートは？

05 チップの第二の市場は何か？

06 最初に支払う顧客は誰か、名前で言えるか？

これらは技術交流と技術協力を通じてともに探求できる領域である：カスタムチップ、AI開発、AI × 暗号資産システム。

i@tanshuai.com · tanshuai.com