調査ノート · 公開版

2026 · 11



有用作業証明 · 暗号資産 × シリコン

計算は合意である

2026年のAI × 暗号資産 × 半導体：Pearlの有用作業証明から

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

結論

Pearlは行列積がブロックチェーンを守れることを証明したが、その作業が有用であることはまだ証明していない。AI × 暗号資産全体で有償需要があるのは推論、データ、プライバシーであり、ASICが報われるのはパイが大きく、ルールが安定し、チップに第二の市場がある場合だけである。

タン・シュアイ

技術者・創業者 · AI研究者・開発者

tanshuai.com · i@tanshuai.com

データ基準日：2026年11月13日

金額は米ドル

目次

目次



◆ **エグゼクティブサマリー** 04
定理は成り立つが、インセンティブは成り立たない

01 **対象と方法** 07
対象、方法、四つのテスト

02 **Pearl · 仕組み** 08
Pearl：コンセンサスとしての行列積

03 **Pearl · 経済性** 10
Pearl：規模、発行、有用性ギャップ

04 **Pearl · ルール** 12
Pearl：ルールのリスク、数値形式、ガバナンス

05 **有用作業チェーン** 13
有用作業チェーン：行列もゼロ知識もASICを止められない

06 **より広い全体像** 16
AI × 暗号資産のその他の領域：本物だが小さい需要と、エクイティへ移る価値

07 **ASICの経済性** 18
ASICの問い：一つの公式、三つの物差し

08 **チップの種類ごとに** 21
五つのチップの種類、五つの答え

09 **プロセスノード** 24
プロセスノード：最大の生涯コストに選ばせる

10 **段階的予算** 27
モデルからシリコンへ：最初のチップの段階的予算

11 **機会** 29
機会はどこにあるか、そして私なら何をするか

12 **注目点** 31
注目すべきこと：2026年11月から2027年まで

13 **尋ねるべき質問** 32
尋ねなかったが、尋ねるべきだった質問

◆ **著者について** 34
タン・シュアイ

◆ **出典** 35

図表

図表



図01	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	06
図02	Pearlの整数演算では、GPUは共通のエネルギー上限を持つ	09
図03	Pearlの最初の6か月：ハッシュレートは価格に従い、ルールは変わり続ける	11
図04	補助金倍率：ネットワークは外部収益の何倍を支払っているか	15
図05	なぜ効率が報われなくなるのか：ASICが手元に残せるのは収益の最大1 − 1/k	19
図06	大半のパイはチップ1品種の設計予算より小さい	20
図07	五つのチップの種類、五つの答え	24
図08	先端ウェハは成熟ウェハの10倍のコストがかかる	25
図09	マスクの前に証拠を買う：最初のチップの段階的予算	28

本文中の表示

推計	引用したデータに基づく著者の計算または推論
ベンダー公称	製品を販売する企業が公表したもので、独立した検証はない
分析	証拠に対する著者の解釈

本書は英語版の翻訳であり、両者に相違がある場合は英語版が優先する。

データ基準日：2026年11月13日 · 金額は米ドル

エグゼクティブサマリー

定理は成り立つが、インセンティブは成り立たない

結論

Pearlは「計算は合意である」が工学として機能することを示したが、それが有用であることはまだ示していない。

≈90 EH/s
2026年11月13日のPearlのネットワーク。1 Hは1回のINT7積和演算

≈1%
実際のAI作業を含むPearlのブロック（Blockworks、2026年10月28日）

≈7,000万ドル
Bittensorの年間の検証可能な外部収益。発行は3億ドル超

175–180×
2025年第3四半期のAleoのプルーバー報酬の手数料に対する倍率

R × (1 – 1/k)
限界的なマイナーよりk倍安いASICの利益上限 推計

≈150万ドル
モデル、FPGA、MPWを経てN7で実測のシリコンに至る費用。≈350万ドルのマスクセットの前 推計

Pearl

2026年11月13日、Pearlのネットワークは約90 EH/sで稼働していた。そのコンセンサスコードでは1「ハッシュ」が1回の整数積和演算であり、ネットワークはH100約122,000基分の整数演算性能に相当する。それでも実際のAI作業を含むブロックは約1%にすぎず、唯一公開されている推論パートナーシップは、提供元のサーバーレスAPIではもう提供されていない。原因は暗号ではなく経済にある。推論を提供しながらマイニングするGPUは、専用マイナーのハッシュレートの約1%から27%しか得られないため、合理的なマイナーはランダムな行列を掛け合わせる。

有償需要

AI × 暗号資産全体で、検証可能な有償需要が現れているのは三つの場所、すなわち推論の販売、データの販売、プライバシーの販売である。Bittensorの検証可能な外部収益は年間約7,000万ドルで、その約5分の4は計算資源とインフラのサブネットから来ている。Grassは2026年上半期に1,700万ドルのデータ収益を報告している。信頼実行環境（TEE）での秘密推論は本番稼働している。対照的に、AIエージェントが実際に発起した決済は月約5,000〜11,000ドルにとどまり、zkMLと分散型学習にはまだ開示された有償需要がない。

補助金と価値

補助金倍率は最も正直な健全性チェックである。Aleoのプルーバー報酬は手数料の約175〜180倍、Bittensorの発行は検証可能な収益の約4〜11倍、Renderの時価総額はオンチェーン手数料の約360倍である。そしてPearlのマイナー収入、年間約4億6,000万ドルの大半はブロック補助金であり、有償のAI需要とはほとんど結びついていない。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。その一方で、価値はトークンからエクイティへ移りつつある。集中型インフラと暗号資産ネイティブな流通を使う4社のエクイティ企業の評価額は約85億ドルで、プロトコル層とアプリケーション層のAIトークンの合計とほぼ同じである。

ASIC

チップについて言えば、ASICの利益の上限はおおむね計算量あたり収益に (1 − 1/k) を掛けたものである。ここでkは、限界的なハードウェアに比べて何倍安いかを表す。この項は凹関数なので、k = 5–10を超える効率はほとんど利益を増やさない。結果を決めるのはパイの大きさ、ルールがどれだけ続くか、そしてチップに第二の市場があるかどうかである。チップの種類ごとの私の答えは次のとおりである。Pearl専用のINT7チップは今テープアウトせず、代わりにマイニングもできる推論優先のアクセラレータに賭ける。新規参入者としてマーチャント型ビットコインマイナー市場には入らない。小さなチームとして単体の学習チップは作らない。推論チップは顧客と契約してから作る。ZKアクセラレータはヘッジにとどめ、FHEには早めに布石を打つ。

ノードと予算

プロセスノードは、チップの生涯コストのうち最大の項目で選ぶべきである。常時稼働する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メモリ、推論チップならSRAMかHBMかの判断である。そして最初のチップは段階を踏んで買うべきである。モデル、FPGA、マルチプロジェクトウェハ、そしてその後で初めてマスクセットという順にすれば、プロトコルが変わっても失うのはテープアウトではなく試作の費用で済む。機会は分野が交差する場所にある。暗号資産を最初の顧客に、AIを第二の市場にすることである。

問い	判断	主要な数値（出典は各章）
① **Pearlは機能するか、その作業は有用か**	機能する：大規模な行列積で守られるブロックチェーンである。まだ有用ではない：マイニングのほぼすべてがランダムな行列で行われている	2026年11月13日に約90 EH/s；1 H = 1回のINT7積和演算；AI作業を含むブロックは約1%
② **AI × 暗号資産の本当の有償需要はどこにあるか**	推論、データ、プライバシー。エージェント決済、zkML、分散型学習はまだ需要以前である	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；エージェント決済は月約5,000〜11,000ドル
③ **ASICは作る価値があるか**	パイが大きく、ルールが安定し、チップに第二の市場がある場合に限る。今日、三つすべてを備えたネットワークはない	利益上限 ≈ R × (1 − 1/k)；ビットコインのマイナー収益は年間約115億ドル、Pearlは約4.6億〜4.9億ドル、Kaspaは約1,800万ドル
④ **小さなチームはどのチップを作るべきか**	マイニングもできる推論優先のアクセラレータ、契約済み顧客向けの推論チップ、早期のFHE開発。マーチャント型ビットコインマイナーや学習チップではない	KaspaのASICは1日0.86ドルを稼ぐ；3/2 nmの設計予算は6,000万〜4億ドル以上
⑤ **どのプロセスノードか**	最大の生涯コストが決める：エネルギー、パッケージングとメモリ、あるいはメモリアーキテクチャ	TSMC N2はウェハ1枚約30,000ドル、N28は約3,000ドル；HBMとCoWoSはH100のコストの約63%
⑥ **最初のチップにはいくらかかり、どう買うべきか**	四つの段階で：モデル、FPGA、マルチプロジェクトウェハ、そしてマスク。ルールか買い手が定まっていなければ、マスクの前で止める	商用MPW枠は50,000〜500,000ドル；N7のマスクは約350万ドル；7/6 nmの設計予算は1,500万〜1億ドル

図01

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

検証可能な有償需要と、補助金・評価額のシグナル（2026年11月）

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

出典: DefiLlama、SubConnect（hoge.gg経由）、TRM Labs、Phala、Dealroom、SiliconANGLE、CoinGecko、Blockworks；著者による整理。

01 対象と方法
対象、方法、四つのテスト

なぜこのレポートを、なぜ今か

2026年4月、新しいブロックチェーンPearlが、長年のアイデアを本番に持ち込んだ。マイナーにハッシュ計算の代わりに、AIが依拠する行列積を行わせてブロックを競わせるというものである。6か月のうちにネットワークは約90 EH/sに達し、トークンの時価総額は約5億ドルになった。同じ時期に、AI計算資源マーケットプレイス、分散型学習ネットワーク、エージェント決済レール、データネットワークが数十億ドルを調達し、ビットコインマイナーは電力サイトをAIデータセンターへ転換し始めた。私が知りたかったのは、このうちどれに本当の顧客がいるのか、そのどこかでカスタムシリコンが意味を持つのか、そしてチップチームが実際に使えるプロセスノードとファウンドリはどれか、ということである。

あらゆるAI × 暗号資産プロジェクトに対する四つのテスト

2017年のGridcoinに関するセキュリティ研究は、有用な計算がブロックチェーンを守れるのは、それが解くのが難しく、検証が容易で、報酬計算が容易な場合に限ると論じた。私はこれに四つ目のテストを加える。この四つで、以下の内容の大半が決まる。

01 **解くのが難しい。** 有効な証明を作る最も安い方法が誠実な計算でなければならない。近道があってはならない。

02 **検証が容易。** 作業の確認は作業そのものよりはるかに安くなければならない。さもなければネットワークは二度支払うことになる。

03 **報酬計算が容易。** プロトコルは第三者を信頼せず、証明だけから報酬を計算できなければならない。

04 **誰かが出力に支払う。** ネットワーク外の顧客が結果に支払わない限り、「有用な」作業は物語付きの補助金にすぎない。

ハッシュパズルは最初の三つのテストに合格し、四つ目に落ちる。本物のAIタスクは四つ目に合格するが、二つ目に落ちる。AIの計算をゼロ知識で証明すると計算そのものの100倍から10,000倍のコストがかかり、学習の証明（proof-of-learning）方式は安価に偽装できることが示されている。Pearlのノイズ付き行列積は、AIの計算と同じ形を保ちながら検証のテストに合格する、初めての信頼できる橋渡しである。

調査の方法

これはデスクリサーチであり、私がチップや事業計画をレビューするのと同じやり方で行った。Pearlのコード、プロトコル提案、ホワイトペーパー、独立したフルノードのチェーンデータ、企業の開示資料と決算発表、暗号学・コンピュータアーキテクチャ・機械学習の論文、ファウンドリとベンダーの価格データ、業界紙と技術系メディアを読んだ。すべての数値には日付を付けている。私自身が導いた数値はその旨を記し、推計と表示する。販売者だけが報告している数値は

ベンダー公称、証拠に対する私の解釈は 分析 と表示する。金額は米ドルである。状況は2026年11月13日時点のものである。

第02章

02 Pearl：コンセンサスとしての行列積

Pearl · 仕組み

アイデア：定理からメインネットへ

2025年4月、Ilan KomargodskiとOmri Weinsteinは「Proofs of Useful Work from Arbitrary Matrix Multiplication」を発表した。二人は任意の行列積について、素朴な乗算のわずか1 + o(1)倍のオーバーヘッドで済む有用作業証明を構成した。その安全性は、ランダムな低ランク線形方程式の束を解く困難さに依拠しており、これは証明ではなく予想である。論文はこの分野の本当の難しさを指摘している。定数倍のオーバーヘッドを持つ有用作業証明は自明だが役に立たない。難しいのは、マイナーが自分で入力を選べるときに、誠実な計算を勝つための最も安い方法に保つことである。

Pearlのメインネットは2026年4月27日09:00 UTCに始動した。マイナーはノイズ付きの積 (A + E)(B + F) を計算する。低ランクのノイズはBLAKE3のコミットメントから導かれ、その後ノイズを取り除いてA·Bを復元する。各出力タイルのアキュムレータの状態はハッシュされて宝くじの券になる。当選したタイルは開示され、60 KB未満の再帰的Plonky2ゼロ知識証明で証明される。これは上限65 KBのブロック証明書に収められる。検証は行列のサイズによらない定数サイズの小さな証明で済む。ハッシュパズルと同じくらい安く確認でき、しかも計算そのものは有用になりうる。

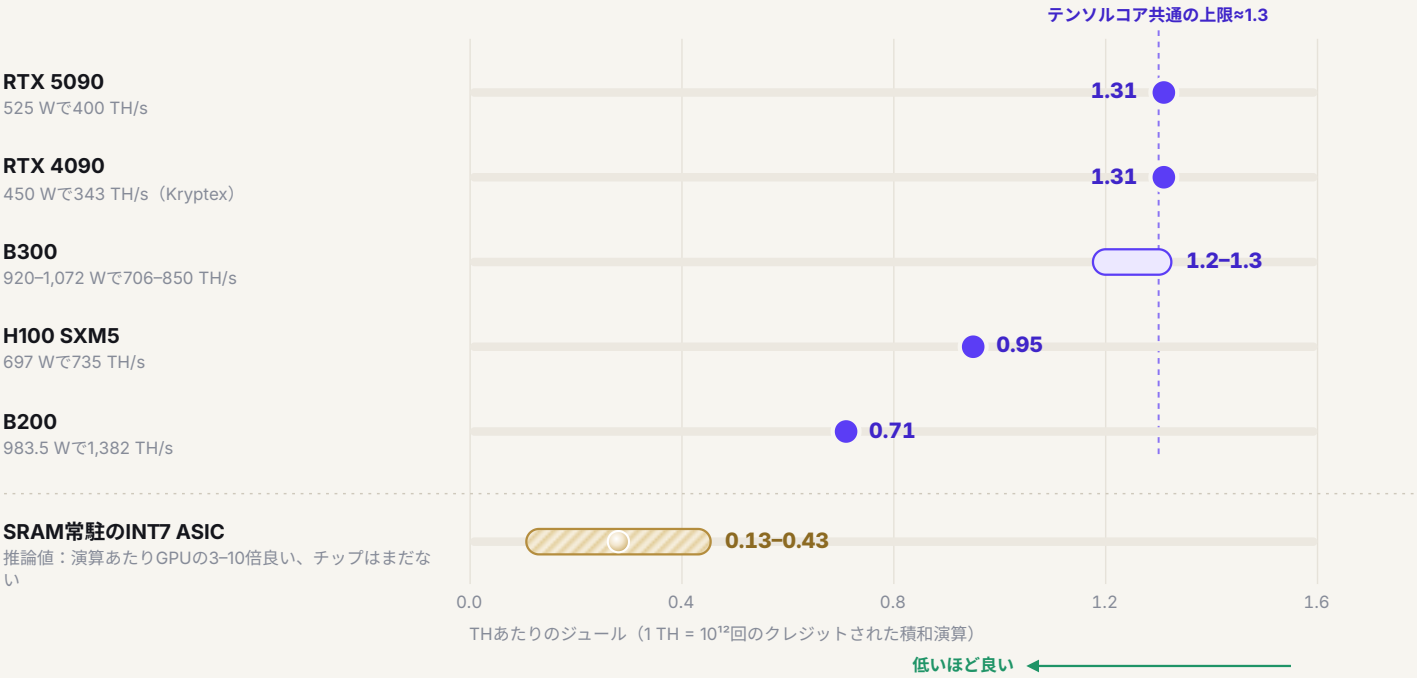
1回の積和演算が1「ハッシュ」

チップ設計者にとって最も重要な事実は単位である。Pearlのコンセンサスコードは、各試行のターゲットをタイルサイズと内積長の積でスケールするので、**1 Hはちょうど1回のクレジットされたINT7 × INT7 → INT32積和演算（MAC）である。**ブロック96,251以降はランクペナルティによりノイズのランクが128以上であることが求められるが、最小ランクでも1 Hは1 MACに等しい。したがってPearlの「EH/s」は文字どおり毎秒10^18回の整数積和演算を意味する。**ブロックチェーンのセキュリティ予算が、AIアクセラレータのテンソル演算性能で値付けされたのは初めてである。** 実測されたGPUのハッシュレートは各カードの密なINT8積和演算ピークの60%から95%に収まっており、この解釈と整合する。

ハードウェア	Pearlハッシュレート	電力	1兆MACあたりのジュール（J/TH）	出典（日付）
RTX 5090	400 TH/s	525 W	1.31 推計	Kryptex（11月12日）
RTX 4090	約305 TH/s（コミュニティの範囲は280–330）；Kryptexは343 TH/sと掲載	450 W（Kryptex）	1.31（Kryptexの数値による） 推計	prlstats（10月3日）；Kryptex
H100 SXM5	735 TH/s	697 W	0.95 推計	PeakMiner、prlstats経由（9月19日）
B200	1.382 PH/s	983.5 W	0.71 推計	PeakMiner、prlstats経由
B300	706–850 TH/s	920–1,072 W	1.2–1.3 推計	prlstats；SimeonOnSecurity

図02 **Pearlの整数演算では、GPUは共通のエネルギー上限を持つ**

実測のPearlハッシュレートでの1兆回のINT7積和演算あたりのジュール（J/TH）；低いほど良い



出典: Kryptex（2026年11月12日）；prlstats経由のPeakMinerとSRBMinerのベンチマーク；SimeonOnSecurity；ASICの範囲は著者の推論であり、実測ではない。

この表の二つの細部がチップ設計者にとって重要である。第一に、コンシューマー向けのRTX 4090と5090、そしてデータセンター向けのB300は約1.3 J/THに収束し、最良のカードであるB200でさえ約0.71 J/THにとどまる。数万ドルするデータセンターGPUが、整数積和演算1回あたりゲーミングカードとほぼ同じエネルギーを使っているということは、INT8 MACあたりのテンソルコアのエネルギーに共通の上限があることを示しており、その上限こそ専用チップが破りうるものである。第二に、B300はB200より遅い。NVIDIAはBlackwell UltraでINT8の演算性能を大幅に削ったため、このチップでは整数の作業がより遅い経路を通らざるをえない。主流のAIシリコンはINT8からFP8とFP4へ移りつつある。コンセンサスが選んだ数値形式がハードウェアの進む方向から外れると、プロトコルはルールの変更を迫られる。それがFP8フォークの根本であり、本レポート後半の私のASICに関する判断の根本でもある。

第03章

03

Pearl · 経済性

Pearl：規模、発行、有用性ギャップ

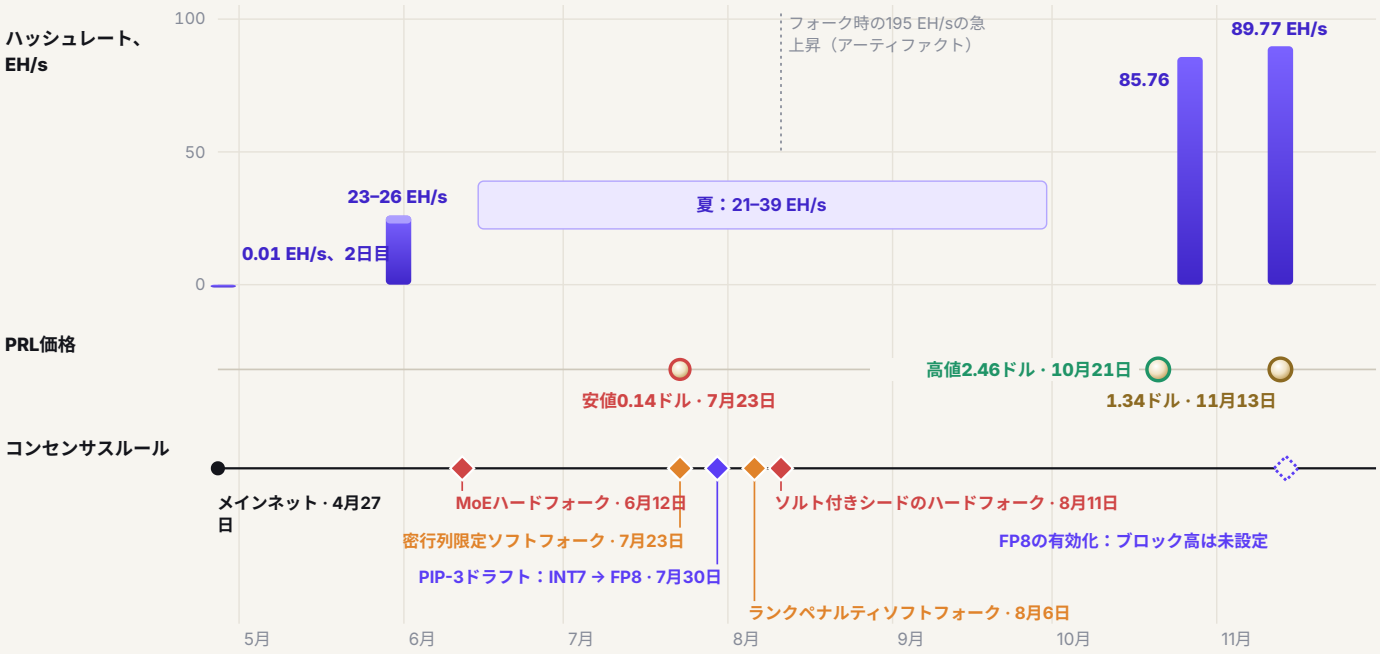
6か月で0.01から90 EH/sへ

指標	値（2026年11月13日）	根拠と出典
ネットワークハッシュレート	約90 EH/s（基準値89.77；同日の範囲88.20–93.22；11月12日の日中高値110–123）	独立フルノードprlstats；Kryptex
難易度とブロック高	58,841,982と142,530	prlstats
相当するハードウェア	H100約122,000基またはRTX 5090約225,000枚	1枚あたり735および400 TH/sとして 推計
価格、時価総額、完全希薄化後評価額	1.32–1.34ドル；約5億ドル；約28億ドル（CoinGeckoランク101位）	CoinGecko
史上最高値と最安値	2.46ドル（10月21日）と0.1399ドル（7月23日）	CoinGecko
採掘済みコイン	3億7,760万PRL、上限21億の17.98%	prlstats
ブロック補助金と1日の発行量	約2,173 PRLと約97万〜103万PRL	prlstats；Kryptex
今後12か月の新規供給	現在の供給量の約78%	prlstats
マイナー収入	1日約125万ドル（モデル）、年間約4億6,000万ドル	prlstats
ハッシュレート単位あたり収益R	1 PH/sあたり1日約14〜15ドル；RTX 5090は1日約5〜6ドルを稼ぐ	推計；Kryptex
実際のAI作業を含むブロック	約1%（10月28日の推計）	Blockworks
プールの集中度	直近24時間のブロックの46.4%をKryptexが発見；上位2プールで約62%	prlstats
保有者の集中度	アドレスのジニ係数0.969；上位100アドレスが53.0%を保有	prlstats

Pearlのハッシュレートは、価格に遅れて追随する関数に近い。ローンチの翌日、ネットワークは約0.01 EH/sで稼働していたが、5月末には23–26 EH/sに達した。夏の間、価格は5月の高値から約86%下落し、ハッシュレートは21–39 EH/sで横ばいだった。9月と10月に価格が約10倍に上昇した後、ハッシュレートは10月27日に85.76 EH/s、11月には約90 EH/sに達した。8月11日の195 EH/sへの急上昇はフォークと重なっており、推定上のアーティファクトと読むべきである。エネルギーもそれに伴って増えた。ある研究は24 EH/sの時点でネットワーク全体を約112 MWと推定し、prlstatsのモデルは現在を約190–215 MWとしている。

図03 **Pearlの最初の6か月：ハッシュレートは価格に従い、ルールは変わり続ける**

ネットワークハッシュレート、三つの価格の目印、すべてのコンセンサス変更（2026年4月27日〜11月13日）



出典: prlstatsのフルノードと系列；Kryptex；CoinGecko；Pearlのparams.goとPIP-3。8月11日の急上昇はフォーク時の推定上のアーティファクト。

発行が再帰性を増幅する

供給上限は21億コインで、半減期はない。ブロック補助金はE(t) = S·H / ((t + H)(t + H − 1))、H = 650,226として滑らかに減少する。しかし発行は時間ではなくブロックで数えられ、初期の難易度は低すぎるところから始まり、調整も遅かった。**初日に約4,406万コイン、最初の6日間で約1億2,000万コインが採掘された**。これは現在の供給量の約32%である 推計。最近のブロックは約171–183秒で、目標の194秒よりまだ速い。その結果、供給は今後12か月で約78%増える。これはマイナー、ハードウェアメーカー、保有者のすべてが向き合わなければならない希薄化である。

マイナーの経済はそこから導かれる。ネットワーク全体のマイナー収入は1日約125万ドル（モデル）である。Kryptexの1日の発行量に現在の価格を掛けると1日約135万ドルとなるので、**ハッシュレート単位あたり収益R ≈ 1 PH/sあたり1日14〜15ドル**である 推計。RTX 5090は1日約5〜6ドルを稼ぐ。H100やH200は約11ドルを稼ぐが、最も安い公開オンデマンドレンタルは1枚1時間約2.09ドル、1日約50ドルなので、マイニングのためだけにカードを借りると大きな損失になる。Rは大きく振れる。prlstatsの系列によれば、8月と9月には約10ドル、10月中旬には一時約33ドルだった 推計。ローンチから数週間のうちに、RTX 5090の推定日次収益は約33.80ドルから約17.19ドルへ半減した。クラウドGPUを借りてのマイニングが採算に乗ったのは、最初の数週間と10月の価格急騰の間だけだった。

定理は成り立つが、インセンティブは成り立たない

本当の問題は暗号ではなく需要である。Pearlの唯一の公開された商用統合は、Together AIのGemma-4-31B-it-pearlエンドポイントで、5月15日に通常価格より25%以上安く提供が始まった。その割引は発行の将来の期待価値で賄われていた。11月13日、モデルのページには**Togetherのサーバーレスapiでは提供されていない**と表示されていた。6月には、ネットワークの約21%にあたる8,012のオンラインマイニングインスタンスの調査が、ネットワークは有用なAI計算をまったく生み出していないと結論づけ（著者は証拠を決定的ではなく示唆的と評している）、純粋にランダムな行列から作られたシェアがプールに受け入れられることを示した。10月28日、Blockworksは**実際のAI作業を含むブロックは約1%にすぎない**と推計し、それがなければPearlはより小さく、安全性が低く、インフレの速いビットコインだと書いた。

理由は計算できる。推論側のオーバーヘッドは本当に小さい。Pearlは4基のH200でのLlama 70Bについてエンドツーエンドの時間が5.08%増えると報告しており、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した。マイニング側は稼ぎが少なすぎる。公式のvLLMプラグインは1,024トークン以上のプリフィルバッチでのみマイニングし、デコードステップでは決してマイニングしない。推論を提供するカードが得るのは、純粋なプリフィルのトラフィックで専用マイナーのハッシュレートの約27%、80%がデコードのチャットの組み合わせで約5.4%、デコードが支配的なトラフィックでわずか約1%である。有償の推論需要がなければ、合理的なマイナーはランダムな行列を掛け合わせる。プロトコルが検証するのは、コミットされた行列が誠実に乗算されたかどうかであって、それが有用だったかどうかではない。**定理は成り立つが、インセンティブは成り立たない。** Pearlの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。

第04章

04 Pearl · ルール
Pearl：ルールのリスク、数値形式、ガバナンス

2か月で4回のフォーク

Pearlのもう一つの顔は、ルールが変わる速さである。2026年6月から8月にかけて、ラボはハードコードされたブロック高で四つのコンセンサス変更を押し通した。Mixture-of-Expertsハードフォーク（ブロック71,935、6月12日ごろ）、密行列限定ソフトフォーク（91,630、7月23日ごろ）、ランクペナルティソフトフォーク（96,251、8月6日ごろ）、ソルト付きシードのハードフォーク（99,000、8月11日ごろ）である。ソルト付きシードのフォークの後、旧来のマイナーは無効なシェアしか作れなくなった。ランクペナルティは、高ランク構成の実効ハッシュレートを50%から87.5%削った。

次の段階はまだドラフトのPIP-3である。マイニングをINT7からFP8 × FP8 → FP32へ移し、ビット単位で一致するデバイスプロファイルを要求するもので、**対応するのはHopperとBlackwellの二つのアーキテクチャだけである**。文書はハードウェア依存を浮動小数点プロトコルの必要悪と呼び、検証に許容誤差を設ければグラインディング攻撃を招くと警告している。11月12日時点で、fp8-schemeブランチのメインネットパラメータには有効化高が設定されていなかった。現在のドラフトではRTX 40シリーズ、A100、AMDのカードは認められない。一方、信頼度の低いprlstatsのモデルは、ハッシュレートの約82%がコンシューマー向けカードによるものと推計している。フォークを強行すれば、チェーン分裂やマイナーの反発を招くおそれがある。

数値形式のトリレンマ

Pearlはトリレンマに直面している。数値形式は、AIに有用であること（FP8またはFP4）、ハードウェアをまたいでビット単位で検証可能であること、ハードウェア中立であることのうち、多くても二つしか満たせない。INT7方式は検証可能で中立だが、AIシリコンの進む方向から外れている。ホワイトリスト付きのFP8は有用で検証可能だが、コンセンサスを一つのベンダーに縛りつける。許容誤差付きのFP8は有用で中立だが、グラインディング攻撃への扉を開く。テンソルコアの浮動小数点演算は一般に数値規格に従っておらず、世代をまたいで再現できない。たとえばHopperでは、FP8の累算は小数部を13ビットしか保持せず、切り捨てを行う。チップ設計者の視点から見れば、「Hopperプロファイル」は完全に確定した演算であり、ASICはそれをビット単位で実装でき、GPUより効率的にできるかもしれない。しかしそれはプロトコルが表明する意図に反するグレーゾーンの事業であり、ガバナンスリスクが非常に高い 分析。

ガバナンス

ガバナンスは集中している。プロトコル提案はすべてラボが書いた。フォークはマイナーのシグナリングなしにハードコードされたブロック高で有効化される。二つ目のクライアント実装はない。そして10月初めの時点で、ノードやゼロ知識回路の第三者監査は公表されていなかった。イスラエルの新聞TheMarkerは、ラボがステルスラウンドで約1億2,000万〜1億3,000万ドルを調達したと報じた（約5,500万ドルのエクイティと約7,500万ドルのGPUインフラファンド）。Pearlは公式チャネルではこれを確認していない。「トークンに投資家向けの割り当てはない」ことと「ベンチャー株主のいる会社である」ことは両立しうるが、緊張は残る。AIの収益はエクイティへ流れ、希薄化はトークン保有者にかかるかもしれない。

総合すると、Pearlはこれまでで最もクリーンな「計算は合意である」の実験である。新しい仕組みで、オンチェーンで検証でき、単位がAIハードウェアに一対一で対応する。しかし有用性はまだ実現しておらず、そのセキュリティ予算、ハッシュレート、マイナーの熱意はすべて、主な需要がまだ形成されておらず、供給が12か月で約78%増えるトークンにかかっている。Blockworksが挙げる三つのシグナルは追う価値がある。アップグレードが円滑に着地するか、AI作業を含むブロックの割合が実質的に上昇するか、そして推論プロバイダーがマイニング収入を顧客に還元するかである。

第05章

05 有用作業チェーン：行列もゼロ知識もASICを止められない

有用作業チェーン

Kaspa：行列は有用でもなく、ASIC耐性もない

Kaspaは教科書的な事例である。そのkHeavyHashは、二つのハッシュの間に4ビット値の64 × 64行列ベクトル積を挟むが、その積は捨てられる。2021年11月のフェアローンチから約16か月後の2023年3月14日、IceRiverが初のKaspa用ASICを発表し、2023年末にはGPUマイニングは終わっていた。3.8 GH/s、300 WのRTX 4090と77 J/THのBitmain KS7を比べると、効率の差は約**1,000倍**になる 推計 。宴の後には圧縮が来た。11月13日、ネットワークは358.9 PH/sで稼働しており、2024年8月の1 EH/sから約64%低い。最良のKS7でも、1 kWhあたり0.10ドルの電力で**1日0.86ドル**しか稼げない。

Aleo：ゼロ知識も専用ハードウェアを止められない

Aleoのプルーバーパズルは、SNARK証明の生成作業を模倣するよう設計されている。ユーザーのトランザクションを証明するものではなく、プロジェクトはZK ASICを公然と歓迎している。2024年9月のメインネットから約5か月後には、専用マシンが出荷されていた。2025年第3四半期、プルーバーは3,120万ALEO（約780万ドル）を受け取ったが、ネットワークが集めた手数料は約43,000〜44,000ドルにすぎなかった。**補助金倍率は約175〜180倍である**。価格は取引初期の約9ドルからその四半期末には0.22ドルまで下落し、現在ではARC-46により解1件あたり10万〜250万ALEOのステークが必要となり、マイニングはステークの閾値に変わった。

QubicとBittensor

QubicはAigarthニューラルネットワークを学習させる「有用なプルーフ・オブ・ワーク」をうたっているが、2025–2026年にその計算資源の最も目立つ産出物は、他のチェーンのブロックだった。まずMoneroをマイニングし、シェアを2025年5月中旬の2%未満から7月末には25%超に引き上げ、8月には51%を主張して6ブロックの再編成を引き起こした（別の情報源は18ブロックとしている）。2026年4月1日にはASICによるDogecoinのマイニングに切り替え、その収益を買い戻しとバーンに充てている。AI学習が有用であるという独立した証拠はなく、時価総額は約2億8,000万〜3億ドルか

ら11月13日には約5,000万ドルへ下落した。Qubicは外部性も露わにした。汎用計算に支払うチェーンは、大規模で、借りることができ、協調した計算力のプールを生み出し、それはCPU向けのチェーンに向けられうる。

Bittensorはプルーフ・オブ・ワークではなく、ステーク加重の主観的スコアリングである。バリデータがマイナーを採点し、重みはステーク加重の中央値で切り詰められる。このグループで外部収益を一定の規模で持つ唯一のネットワークである。検証可能な外部顧客だけを数えるSubConnect指数は、2026年11月初めに**年間約7,000万ドル**（9月1日には約3,500万ドル）を示しており、その78%から82%は計算資源とインフラによるものである。しかし11月初めの価格で発行は年間3億ドルを超えるので、収益が賄うのは9%から23%にすぎない。収益の推計は基準によって大きく異なり、約1,700万ドル（Artemis）から、自己申告の合計を年率換算した1億7,200万ドルまで幅がある。4月には128のサブネットのうち67がインセンティブの99%超をバーンしており、主要チームCovenantがガバナンスをめぐって離脱すると、TAOは数時間で24%下落した。

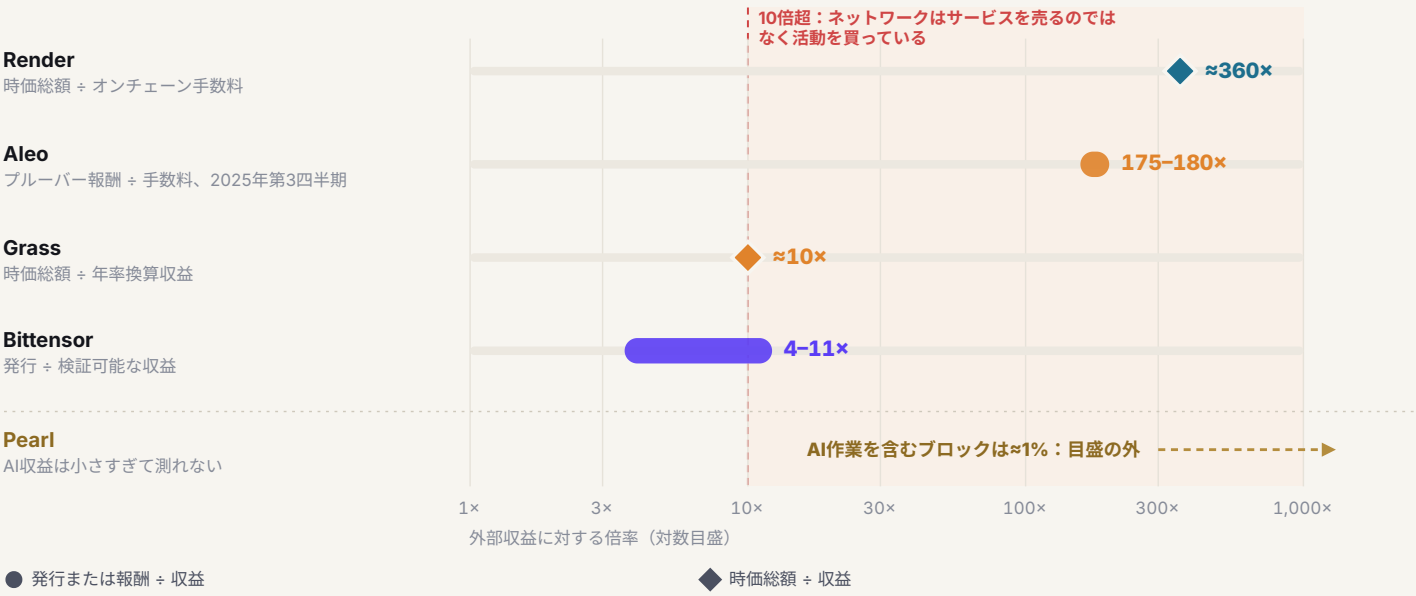
歴史も同じ答えを示す

Primecoinの素数連鎖は検証が速かったが、誰も必要としなかった。GridcoinはBOINCへの貢献を証明するのに第三者の統計サイトに依存しており、研究者は計算を一切せずにブロックを偽造した。Filecoinのストレージ証明は技術的には機能するが、2025年第3四半期の稼働率はわずか36%で、手数料793,000ドルの99.5%はペナルティであり、基本手数料はわずか4,100ドルだった。

プロジェクト	作業またはコンセンサス	時価総額（日付）	ハードウェアの経路	補助金に対する有償需要	判断
Pearl	ノイズ付き行列積（INT7 MACとZK証明書）	約5億ドル（11月13日）	GPU；FP8ドラフトはHopperとBlackwellをホワイトリスト化	AI作業を含むブロックは約1%；マイナー収入の大半は補助金	最も信頼できる仕組み；需要は未証明
Kaspa	kHeavyHash（ハッシュの間の64 × 64、4ビット行列ベクトル積）	約8億4,000万ドル（11月13日）	ローンチ約16か月後にASIC；現在はすべてASIC	有用性を主張していない；マイナー収益は年間約1,800万ドル 推計	行列は有用でもなく、ASIC耐性もない
Aleo	合成SNARKパズルとプルーフ・オブ・ステーク	約1億1,800万ドル（2025年第3四半期末）	約5か月後に専用マシン	プルーバー報酬は手数料の約175〜180倍	補助金が駆動する合成作業
Qubic	「uPoW」（Aigarthを学習させると主張）	約5,000万ドル（11月13日）	CPUとGPU；2026年4月からDogecoin用ASIC	有用性の独立した証拠なし；計算資源は外部マイニングと買い戻しに使用	AIの物語に包まれた計算資源の集約
Bittensor	Yumaコンセンサス（ステーク加重スコアリング）	約25.5億ドル（11月11日）	汎用GPU；ASICの経路なし	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；それでも4〜11倍の補助金
Filecoin（参考）	複製証明と時空間証明	約15億ドル（2025年第3四半期末）	—	稼働率36%；四半期の基本手数料4,100ドル	有用だが、需要が足りない

図04 **補助金倍率：ネットワークは外部収益の何倍を支払っているか**

発行または時価総額をネットワーク外から支払われる収益で割ったもの、対数目盛



出典: Blockworks（Aleo、2025年第3四半期）、DefiLlama（Renderの手数料）、CoinGecko、hoge.gg（Bittensor）、Dealroom（Grass）、Blockworks 0xResearch（Pearl）；著者による計算。

ハードウェアへの教訓はこうである。流動性のあるトークンで支払われる固定的で規則的な作業には、約3〜16か月でASICが現れ、しばしば既存勢力より先に挑戦者から出てくる。「有用」という主張が持ちこたえたのは、外部の顧客が出力に支払っている場合だけだった。そして座礁ハードウェアを生む主な要因は、収益に対する高い補助金と、開発者による作業関数の支配である。

第06章

より広い全体像

06 AI × 暗号資産のその他の領域：本物だが小さい需要と、エクイティへ移る価値

分散型計算資源市場

分散型計算資源には支払う顧客がいるが、需要は小さく、集中しており、大半はオープンモデル推論の再販である。オンチェーンで検証できる手数料は小さい。DefiLlamaによれば、過去1年の手数料はRenderが約235万ドル、Livepeerが約68万ドルであり、DePINセクター全体のオンチェーン収益は2025年にわずか約7,200万ドルだった。自己申告の数値はより大きいが、定義が緩い。Aethirは2025会計年度の収益を「1億2,780万ドル超」と報告しているが、それが総請求額なのかプロトコルの取り分なのかは述べていない。トークンの価値と収益は両方向に乖離している。Renderの時価総額はオンチェーン手数料の約360倍である一方、Aethirの時価総額約8,770万ドルは自己申告の収益を下回る 推計 。

70%から85%安いという主張が成り立つのは、ハイパースケーラーのオンデマンド価格と比べた場合だけである。11月3日、AkashのH100の加重平均価格は**GPU時間あたり約2.73ドル**（範囲2.04〜3.16ドル）で、AWSの約6.88ドル、Google Cloudの11.06ドルより安いが、Vast.aiの約1.73ドル、RunPodのコミュニティクラウドの1.99ドル、1年予約の約2.44ドルより高い（他のプラットフォームの価格は9月12日に確認したもの。発表元のAkashは利害関係者である）。需要の大半はOpenRouter経由で配信されるコモディティ推論で、AkashMLでは1日約17億トークン、io.netでは40億超であり、あらゆるネオクラウドと正面から競合している。「分散型計算資源」の最大の金額は再集中化しつつある。Aethirのトークンをトレジャリー資産として保有するAxe Computeは、自社の9,200基のB300クラスタを貸し出す15億ドル相当の5年契約を結んだが、2026年第1四半期の収益は35,000ドルだった。

分散型の学習と推論

インターネット越しの学習は、80億から400億パラメータで実証されている。Pluralis-8Bは主にコンシューマー向けGPUからなる330ノードで40日間学習し、集中型のH100ベースラインの効率の63%に達した。ただし論文は、この実行が分散型ではなく、Pluralis自身のノードと参加承認の権限を必要としたことを認めている。Nous ResearchのPsycheは、400億パラメータのConsilience事前学習を完了した。フロンティア規模では作業は再集中化した。Prime IntellectのINTELLECT-3は1,060億パラメータのMixture-of-Expertsモデルで、400 GbpsのInfiniBandで接続された512基のH200で2か月かけて学習された。制約は明白である。ノードには少なくとも200 Mbit/sの帯域と約100倍の通信圧縮が必要で、信頼と検証はなお運営者の特権的な役割に依存している。

資金は集中型の製品を売るエクイティ企業に流れた。Prime Intellectは年率換算で1億ドル超の収益を上げたうえで、7月に評価額10億ドルで1億3,000万ドルを調達した。プライベート推論アプリのVeniceは年率換算7,000万ドル超の収益と2026年第1四半期以降の黒字を報告しており（会社発表の数値）、評価額10億ドルで6,500万ドルを調達し、リースしたGPUで稼働している。トークンの側では、Gensynの中核である学習ネットワークはまだ「未定」で、トークンの価値は約1,720万ドルである。AIネイティブなレイヤー1であるRitualのトークンは、メインネット後に高値から72%下落した（見出しのみ）。

検証可能なAI

本番環境は信頼実行環境（TEE）を選んだ。Hopperのコンフィデンシャルコンピューティングは、典型的なLLMクエリに7%未満のオーバーヘッドを加えるだけで、大規模モデルではほとんどゼロである。Phalaの本番環境でのオーバーヘッドは約0.5%から5%だが、2025年末時点で10,004人のユーザーのうち支払っていたのは398人だった。TEEの信頼の起点はチップベンダーである。2025年10月に公表されたTEE.failは、1,000ドル未満のDDR5バスインターポーザーを使い、完全にアップデートされたIntel TDXとAMD SEV-SNPのマシンから認証鍵を取り出した。これはNVIDIAのGPUコンフィデンシャルコンピューティングも損なう。しかも両ベンダーとも、物理攻撃は脅威モデルの対象外だとしている。それはまさにノード運営者が物理的にアクセスできるDePINの環境である。zkMLは今や完全なLLMを証明できる。LagrangeのDeepProveはGPT-2を毎分約174トークン、Gemma 3を約86トークンで証明するが、本番の推論とは桁違いに離れており、開示された有償利用もない。

エージェント決済とデータ

x402は最良の教訓的な例である。TRM Labsは2025年5月以降、既知のファシリテーターが決済した約1億9,890万件の取引と5,270万ドルを数えており、その99.6%がUSDCである。自己支払い、バッチフロー、買い手が10人未満の売り手を除くと、実際にエージェントが発起した割合はわずか0.6%から7.5%、**月約5,000〜11,000ドル**である。Artemisは活動の95%超が売買ではなくプロトコルのシグナリングだと判断している。一方、レールは既存の大手によって標準化されつつある。x402 Foundationは7月14日にLinux Foundationの下に設立され、Visa、Mastercard、Stripe、Google、AWS、Cloudflare、Coinbaseが中核メンバーである。StripeとともにMachine Payments Protocolを共同で策定したTempoは、3月に評価額50億ドルでメインネットを立ち上げた。エージェントトークンのプラットフォームはいまだにローンチパッドの論理で動いている。Virtualsは4億7,900万ドルの「aGDP」を自己申告しており、ElizaOSの創業者は集団訴訟の和解後にそのトークンの終焉を宣言した。価値はステーブルコインの発行者と決済の既存大手に取り込まれる可能性が高い。ここで暗号資産が独自に果たす役割は、エージェントのアイデンティティと説明責任かもしれない。

データは、オフチェーンに本物の買い手がいる数少ないサブセクターの一つである。Grassは2025年に1,700万ドル、2026年上半期にさらに1,700万ドルのデータ収益を報告しており、通年で7,500万ドルを目標とし、黒字だとしている。GRASSの価値は約3億2,800万ドルで、上半期の年率換算収益の約10倍である 推計 。その堀は暗号資産そのものではなく、分散した家庭用回線の帯域による収集規模である。データDAOとデータマーケットプレイスには目に見える有償需要がない。Vanaの価値は約2,150万ドル、Oceanは約2,760万ドルで、OceanはFetch.aiと係争中である。人間であることの証明（proof of personhood）は、エージェントが増えるにつれて本物の統合を獲得しつつある。Worldは約1,800万人近くを認証したとしており、Zoom、Docusign、TinderがWorld IDの一部に対応している。

資本はすでに投票した

セクター	検証可能な有償需要	補助金と評価額のシグナル	判断
有用作業チェーン	Bittensorの検証可能な外部収益は年間約7,000万ドル；PearlはAI作業を含むブロックが約1%	Aleo 175〜180倍；Bittensor 4〜11倍；Pearlは大半が補助金	仕組みには価値がある；有用性には支払う顧客が必要
分散型計算資源市場	オンチェーン手数料は年間約68万〜235万ドル（Livepeer、Render）；自己申告で400万〜1億2,800万ドル	Renderの時価総額は手数料の約360倍	本物だが小さく、大半はコモディティ推論の再販
分散型の学習と推論	エクイティ企業：Prime Intellectは年間1億ドル超、Veniceは7,000万ドル超（集中型インフラ）	Gensynの学習メインネットは未稼働；Ritualのトークンは高値から−72%	技術の進歩は本物；利益はエクイティへ
検証可能なAI	TEEは本番稼働（Phalaの有料ユーザー398人）；有償のzkMLは開示なし	—	TEEは有用；zkMLは初期段階

セクター	検証可能な有償需要	補助金と評価額のシグナル	判断
エージェント決済	エージェントが発起したフローは月約5,000〜11,000ドル	約2億件の取引、大半はシグナリングと投機	レールが先、需要は後
データネットワーク	Grassは2026年上半期に1,700万ドル（自己申告）	GRASSは年率換算収益の約10倍	本物の買い手がいる数少ないセクターの一つ

六つのセクターを並べると、結論は一貫している。**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。** 11月13日、CoinGeckoのAIカテゴリーの価値は合計約186億ドルだったが、その約56%はNEARやICPのような汎用レイヤー1と、TAO、ステークされたTAO（TAOと二重計上の可能性あり）、Pearlのようなコンセンサス層のプロジェクトである。プロトコル層とアプリケーション層のAIトークンの合計は約80億ドル以下である 推計 。これはエクイティ企業4社、Tempo（50億ドル）、Nous（報道で15億ドル）、Prime Intellect（10億ドル）、Venice（10億ドル）の評価額の合計とほぼ同じである。暗号資産のベンチャー資金調達は四半期あたり約45億〜50億ドルで頭打ちとなっており、増加分はAI関連インフラから来ている。その開示額に占める割合は、2026年第3四半期に8.1%から18.2%に上昇した。そして2025年にローンチされた118のトークンの84.7%が、ローンチ価格を下回って取引されている。一言で言えば、少なくとも2026年においては、**暗号資産は流通と決済を担い、利益はエクイティが取る。**

第07章

07 ASICの経済性
ASICの問い：一つの公式、三つの物差し

一つの公式：なぜk = 5を超えると効率が報われなくなるのか

Rを計算量単位あたりの1日の収益（ネットワークのマイナー収入をネットワークのハッシュレートで割ったもの）、cを限界的なハードウェア（Pearlの場合はGPU）での計算量単位あたりの1日のコスト、kをASICがその限界的なハードウェアより何倍安いか（c_ASIC = c/k）とする。GPUが限界的なマイナーであり続ける限り、自由な参入と退出がRをcへ押しやるので、ASICは計算量単位あたりR − c/kを稼ぐ。

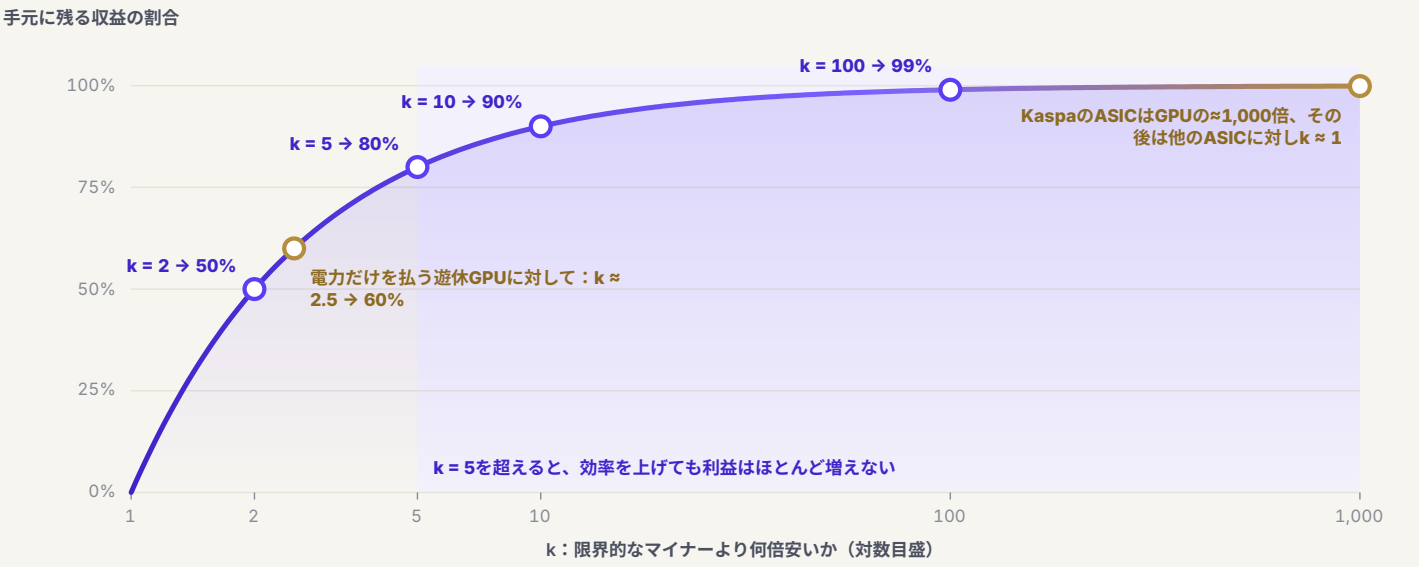
ASICの利益上限 ≈ R × (1 − 1/k)

ネットワーク全体では、ASIC群の年間粗利益の上限はおおよそネットワークのマイナー収益 × (1 − 1/k) であり、それもASICがGPUに代わって限界的なマイナーになるまでの話である。

この公式から三つの帰結が出てくる。第一に、(1 − 1/k) は凹関数である。k = 2でASICは収益の50%を手元に残し、k = 5で80%、k = 10で90%、k = 100で99%である。**k = 5–10を超えると、効率を上げてもほとんど利益は増えない。**決めるのはRとパイの大きさである。第二に、比較の基準がリセットされる。ASICが限界的なマイナーになれば、kは他のASICに対して測らなければならない。KaspaのASICはGPUに対して約1,000倍の効率優位を持っていたが、それで得られたのは短期間の棚ぼただけで、今日では最良のKS7が1日0.86ドルを稼ぐにすぎない。第三に、PearlのようなGPU向けのチェーンでは、基準はしばしばGPUの購入価格ではなく**遊休GPUの電気代**である。自前のRTX 5090は525 W、1 kWhあたり0.10ドルで1日約1.26ドルの電力を消費し、約5〜6ドルを稼ぐ 推計 。サンクコストとなったGPUに対しては、エネルギー消費が5分の1のASICでさえ、減価償却費が電気代と等しければ実効kは約2.5にすぎず、利益上限はRの約60%となる（説明のための仮定）。

図05 **なぜ効率が報われなくなるのか：ASICが手元に残せるのは収益の最大1 − 1/k**

コスト優位kに応じて、限界的なマイナーに対しASICが手元に残せる収益の割合



出典: 著者のモデル：限界的なハードウェアが価格を決めるとき、計算量あたり収益はそのコストに近づく；KaspaとRTX 5090の数値は本レポートから。

三つの物差し：パイ、回収規模、ルール

第一の物差しは**パイ**である。11月第1週のブロック報酬約2,893 BTC（約2億2,200万ドル）を年率換算すると、ビットコインマイナーは年間約115億ドルを稼ぐ 推計。Pearlのマイナーは約4.6億〜4.9億ドル（現在の価格で）、Aleoのプルーバー報酬は2025年第3四半期から年率換算して約3,100万ドル、Kaspaのマイナーはブロック報酬1.945 KAS、毎秒10ブロックで約1,800万ドルである 推計。**Kaspaのマイナー収益1年分は、5/4 nmチップ1品種の設計予算の下限（約3,000万ドル）より少ない。**

第二の物差しは**NREを回収するのに必要なハッシュレート**である。

h* = NRE ÷ [R × (1 − 1/k) × T × p]

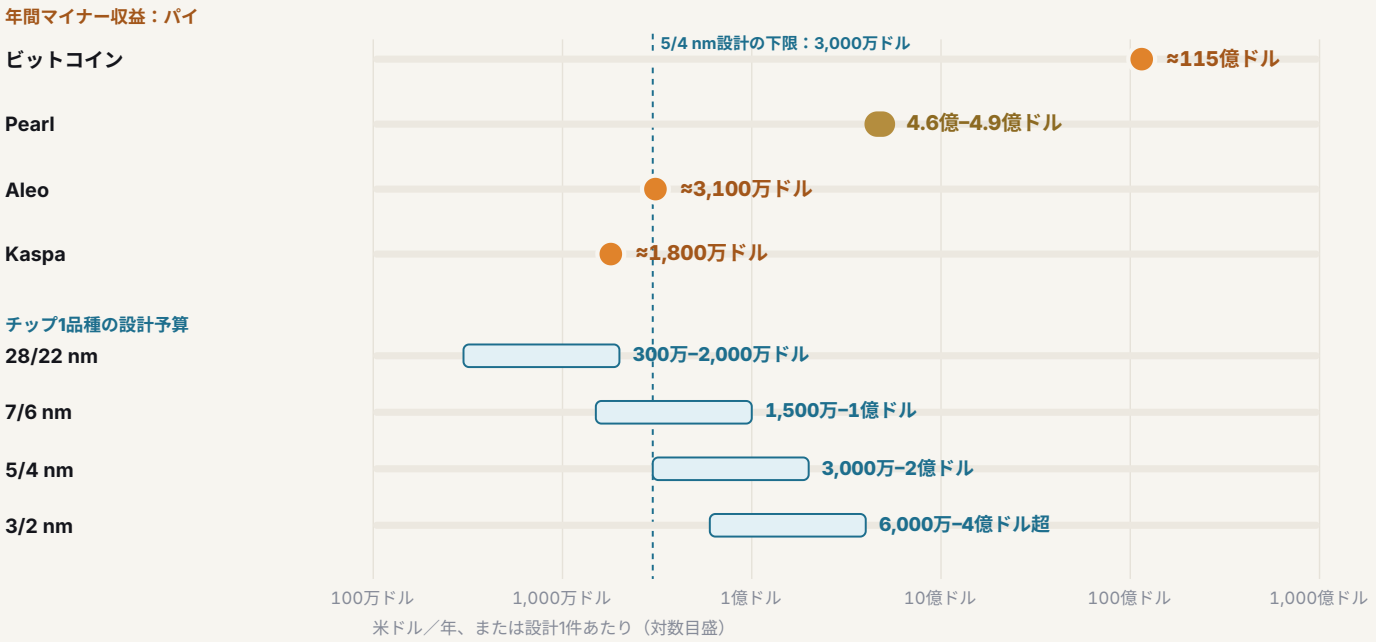
ここでTは日数で表した有効期間、pはその期間中にルールが変わらない確率である。Pearlについて、R = 1 PH/sあたり1日14ドル、k = 5、T = 365日、NRE = 2,000万ドルとする（N7/N6の繰り返しアレイのチップ。Silicon Analystsによる中位ノードの500万〜3,000万ドル、AnySiliconによる7/6 nm計算ASICの1,500万〜1億ドルという範囲の下限側をとった。マイニングチップは使うIPが少なく、構造が繰り返しだからである。これは私の仮定である）。p = 1なら、丸1年稼働する約**4.9 EH/s**、ネットワークの約5%が必要である。p = 0.5なら約**9.8 EH/s**、約11%である。そしてRが夏の水準の約10ドルに戻れば、p = 1でも約6.9 EH/sが必要になる 推計。この規模は手の届かないものではない。問題はpとTである。

第三の物差しは**ルールのリスク**であり、しばしば決定的である。2018年のMoneroの反ASICフォークはBitmainのX3を座礁させ、ネットワークは一時ハッシュレートのほぼ半分を失った。同じ年のSiaのフォークはBitmainとInnosiliconのマイナーを文鎮化させる一方、開発者とつながりのあるObeliskのマイナーの中古価格は2,499ドルから5,000ドル超へ上昇した。EthereumのMergeから1か月余りの時点で、新しい仕事を見つけた旧Ethereumマイナーは20%未満だった。**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。**そしてSiaは、「ASIC耐性」が開発者自身の堀になりうることを示している。第二の市場を持つハードウェアは生き残る。Merge後、GPUはAIとクラウドへ移ったが、単一アルゴリズムのASICはEthereum Classicに押し寄せた。期間も縮んでいる。Kaspaの最初のASICは約16か月、Aleoは約5か月かかっただけで、効率のフロンティアに最初に到達するのは、既存勢力ではなく挑戦者であることが多い。

ネットワーク	年間マイナー収益（概算）	限界的または基準となるハードウェア	ルールの安定性	新規参入者が得られるk	判断
ビットコイン	115億ドル	Bitmain S23 XP Hyd（8.9 J/TH、1 THあたり25.5ドル）	非常に高い	≤1	パイは大きいが、kは既存勢力のもの
Pearl	4.6億〜4.9億ドル（現在の価格で）	自前または遊休のGPU（限界費用 ≈ 電気代）とデータセンターGPU	非常に低い：2か月で4回のフォーク；FP8ホワイトリストが保留中	効率でおそらく3〜10倍 分析；サンクコストのGPUに対してはより低い	パイは十分大きい；ルールのリスクが拒否権を持つ
Aleo	約3,100万ドル（2025年第3四半期、年率換算）	IceRiver AE2などの専用マシン	中程度：ARC-46のステーク閾値	≈1	パイは小さく、閾値は上がっている
Kaspa	約1,800万ドル	KS7（77 J/TH）	高い	≈1	年間収益が5/4 nm設計予算1件の下限を下回る

図06 **大半のパイはチップ1品種の設計予算より小さい**

四つのネットワークの年間マイナー収益と、プロセスノード別のチップ1品種の設計コスト、対数目盛



出典: Hashrate Index（ビットコイン、2026年11月）、prlstatsとKryptex（Pearl）、Blockworks（Aleo、2025年第3四半期）、minerstat（Kaspa）、AnySilicon（設計予算、2026年）；著者による年率換算。

「パイが大きく、ルールが安定し、k > 1」という象限は今日空いている。ビットコインはパイと安定したルールを持つが、そのkは既存勢力のものである。Pearlのパイは十分大きいが、ルールは最も不安定である。KaspaとAleoのルールは十分に安定しているが、パイが小さすぎる。

第08章

08 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：専用INT7チップは作らず、推論も提供できるマイナーに賭ける

ASICを支持する論拠は本物である。今日AI作業を含むブロックは約1%しかないので、専用ASICは有用な作業をする能力を失うため稼ぎが減るというホワイトペーパーの経済的な議論は、今まさに最も弱い。GPUで最も高価な部品であるHBMとCoWoSパッケージングは、H100の製造コストの約63%を占め、ロジックダイは約9%にすぎない。7ビット整数の積和演算だけを行い、オペランドをオンチップSRAMに置き、低電圧で動くチップなら、演算あたりのエネルギーで同じノードのGPUの3〜10倍に達し、演算あたりのコストではさらに大きな優位を得ることも十分ありうる[分析；実測はまだない]。反対の論拠はより重い。先端ノードのファウンドリのリードタイムは50週を超えることがあり、新しいチームは着手から量産まで約18〜24か月を要する 推計 。チップが届くころには、PearlはFP8へ、さらにFP4へ移っているかもしれない。そしてPIP-3はデバイスのホワイトリストで認められる演算を定義するので、それが有効化されればINT7チップは単に動かなくなる。

したがって私の結論はこうである。**Pearl専用のINT7チップは今テープアウトしない。** より良い賭けが二つある。一つは、マイニングもできる推論優先のアクセラレータである。汎用のINT8/FP8 GEMMとSRAM常駐のオペランドを中心に作れば、マイニングへのアクセスが閉ざされても、価値は本物の推論市場に着地する。もう一つは、プロトコルの議論に加わり、ASICが正確に実装できるベンダー中立な正準演算を、アルゴリズムの安定性の約束とともに求めることである。それが「パイが大きく、ルールが安定し、k > 1」という象限が存在するための前提条件である。それまでは、アーキテクチャはFPGAや成熟ノードのマルチプロジェクトウェハ（MPW）で検証でき、NREのリスクを100万ドル規模に抑えられる。第10章では、これを段階的な予算に落とし込む。

ビットコイン型マイナー：kは既存勢力が握り、電力が希少な資産である

ビットコインのルールリスクは最も低いが、競争によって新規参入者のkは1を下回る。BitmainのS23 XP Hydは8.9 J/THに達し、1 THあたり25.5ドルで販売され、11月から出荷される。フラッグシップの効率は、2023年のS21の17.5 J/THから8.9 J/THへと、3年で約49%改善した。2027–2028年に量産出荷する新規参入者が勝負になるには、約8 J/TH以下が必要である 推計 。挑戦者は撤退しつつある。Canaanは2026年第2四半期の収益3,190万ドル、売上総損失2,930万ドルを報告し、第3四半期のガイダンスはわずか1,100万〜1,500万ドルだった。Bitdeerの第3四半期の自社マシンの外部販売は30万ドルに落ち、グループの粗利率は3.4%だった。AuradineはVelaura AIに社名を変えてAIチップへ転じた。そしてCore Scientificは、BlockのProto部門に発注していた約15 EH/s分の3 nmマシンをキャンセルし、4,190万ドルの損失を計上した。

需要も縮んでいる。11月9日のハッシュプライスは1 PH/sあたり1日約31.89ドルで、2027年4月までのフォワードカーブの平均は約32.7ドル、手数料はブロック報酬のわずか0.72%だった。1 kWhあたり0.045ドルなら、S23 XP Hydの回収期間は約3.1年であり 推計 、2028年ごろと見込まれる次の半減期に近い。より重要なのは電力の機会費用である。AIと高性能計算のリースは現在、契約メガワットあたり年間約167万〜190万ドルを稼ぎ、80%から85%の純営業利益率なら、メガワットあたりのマイニングの粗利益（約56万〜90万ドル）の約1.5〜2.9倍になる[推計；二つのメガワットの基準は異なる]。Core Scientificは第4四半期にマイニングをやめる。Bitfarms（現Keel）は米国のマイニングサイトをすべて閉鎖し

た。IRENはある四半期にAIクラウドで2億ドル、マイニングでわずか2,800万ドルを稼いだ。**電力とデータセンターの容量こそが資産であり、マイニングマシンは消耗品である。**

NREの計算も同じく容赦がない。フロンティアの効率には今や3 nmクラスのプロセスが必要である（二次情報によれば、MicroBTはSamsung SF3を使い、AuradineとProtoのチップは3 nmである）。マスクは約1,000万〜2,000万ドル、NRE全体では3,000万〜1億ドル以上かかる。1 THあたり20〜25ドル、粗利率30%なら、販売する1 EH/sごとに約600万〜750万ドルの粗利益が得られるので、Bitdeer規模の年間研究開発費、約1億1,000万〜1億6,000万ドルを賄うには、外部の買い手に年間約20〜25 EH/s、ネットワークの約2%を販売する必要がある 推計。結論：**新しいチームはマーチャント型ビットコインマイナー市場に参入すべきではない。** それでも意味のあるケースが三つある。自前の安価な電力との垂直統合、家庭用や暖房用マイナーのようなニッチな形態（Canaanも家庭用暖房製品を投入している）、そしてIPと設計サービスを通じた既存勢力のロードマップへの参加である。

AI学習チップ：小さなチームでは作らない

学習チップでは、kを得るのが最も難しい。同じ世代と精度では、GoogleのIronwoodがチップレベルのFP8効率でB300をリードしているのは約1.1〜1.8倍にすぎない（Ironwoodの電力は記者による推定） 推計。TPU v1の論文からよく引用される30〜80倍は、テンソルコアを持たないK80と比べて測定されたものである。本当のてこは数値形式である。FP8からFP4へ移れば、通常同じシリコンで2〜3倍の演算性能が得られ、NVIDIAはそこで最も速く動いている。同社は2026年下半期に量産されるRubinについて、NVFP4推論で50 PFを主張している。コストと供給の閾値はさらに高い。3/2 nmの設計予算は6,000万〜4億ドル以上である。2026年のCoWoSの生産能力は月約106,000〜130,000枚のウェハで、TSMCは最大20%の値上げを検討していると報じられている。HBM3Eの契約価格が1 GBあたり15.6ドルなら、288 GBのアクセラレータのHBMだけで約4,500ドルかかる 推計。この市場は、ハイパースケーラーとのBroadcom型の共同開発のものである（第11章）。結論：**小さなチームは単体の学習チップを作るべきではない。**代わりにIP、チップレット、設計サービスを作る。

AI推論チップ：汎用性をkと引き換えにすれば、報われる

推論はASICの余地が最も大きい領域である。汎用性を手放すことでkを買えるからである。Etchedは、8チップのサーバーがLlama-70Bを毎秒500,000トークン超で動かし、H100 8基の約20倍だと主張している。Taalasはモデルの重みをマスクROMに焼き込み、電力が10分の1、製造コストが20分の1だと主張している（いずれも ベンダー公称）。SRAM中心のアーキテクチャはHBMとCoWoSを避けられ、ノードも扱いやすい。TaalasはTSMCの6 nmを使い、Groqは14 nmからSamsungの4 nmへ移った。暗号資産の流通は推論チップの助けにならない。分散型計算資源ネットワークはほぼすべてNVIDIAで動いているからである。入り口はネオクラウドの調達の経済性と、中国の大きな国内推論市場である。中国では国費で建設されるデータセンターは国産AIチップを使わなければならず、H200の輸入は絞られており、北京は大手インターネット企業に国産チップで推論を行うことを求めている。結論：明確な顧客がいて、モデルとアーキテクチャへのロックインの度合いを意図的に選ぶ限り、**作る価値がある。**これはPoUWマイニングチップにとって最良の第二の市場でもある。

ZKとFHEのアクセラレータ：ZKはヘッジ、FHEには早めの布石

GPUはすでにリアルタイムのZK証明に追いついている。SuccinctのSP1 Hypercubeは、16枚のRTX 5090でEthereumのブロックの99.7%を12秒未満で証明した。CysicはそのZK C1チップがGPUプルーバーの10〜100倍の効率を持ち、2026年に出荷されると主張しているが、その需要の大部分は自社のトークン報酬から来ている ベンダー公称。AleoパズルのASICが実際のZK証明に使われているという公開された証拠は見つからなかった。ZK証明は整数演算で決定論的であり、マイニングチップの仕事と形が近いが、証明システムは速く変わる（SP1、RISC Zero、Halo2、Plonky2など）。結論：プログラマブルなMSM、NTT、ハッシュのエンジンで、まずFPGA、次にASICとして、**待ちながらヘッジする。**

FHEは最もハードウェアに縛られたプリミティブであり、上振れの余地も最も大きい。IntelのHeraclesは、Intel 3で197 mm²、176 W、48 GBのHBM3を備え、24コアのXeonの1,074〜5,547倍の速さでFHE演算を実行するが、Intelに商用化の計画はなく、プロジェクトのリーダーは2025年12月に退社した。NiobiumはSemiFiveを設計パートナーとしてSamsung 8LPUで開発を進めており（約686万ドルの開発契約）、2,300万ドル超を調達した。フォトニクス方式のOptalysysは3,100万ドルを調達し、完全な商用チップはまだ2〜3年先だとしている。そしてZamaのオープンソースFPGA設計は約200 Wで毎秒約13,000回のプログラマブルブートストラップに達しており、これがあらゆるASICが明確に上回らなければならない公開のベースラインである。結論：2027–2029年ごろの機会に向けて、**早めに布石を打ち、軽い資産で検証する**。需要は暗号資産そのものより、企業と政府向けの暗号化AIに根づく可能性が高く、FHEにはHBMが必要なので、コスト構造は学習チップに似る。

チップの種類	kの源泉	需要とパイ	NREと閾値	ルールまたはロックインのリスク	第二の市場	判断
Pearl型PoUWマイニングチップ	HBM、CoWoS、汎用ユニットを省く：J/opでおそらく3〜10倍 分析	マイナー収入は年間約4.6億〜4.9億ドル、変動が大きい	N7/N6の繰り返しアレイで約1,000万〜3,000万ドル 分析	非常に高い：プロトコルが数値形式とデバイスのホワイトリストを決める	汎用INT8/FP8 GEMMとして作ればAI推論	専用INT7チップは作らない；推論優先でマイニング可能なものを作るか、正準演算を待つ
ビットコインSHA-256マイニングチップ	Bitmainに対してk ≤ 1	年間約115億ドル、マーチャント市場は2社が握る	3 nmクラスのマスクは1,000万〜2,000万ドル；NRE全体は3,000万〜1億ドル以上	低い（アルゴリズムは安定）；競争と半減期のリスクは高い	ほぼない（単一アルゴリズム）	新規参入者はマーチャント市場に入らない；自前の電力、ニッチな形態、IPのみ
AI学習チップ	同世代のシストリックアレイは1.1〜1.8倍にすぎない；数値形式がてこ	最大（Broadcomの2026会計年度のAI半導体収益は約580億ドル）	3/2 nmの設計は6,000万〜4億ドル以上；CoWoSとHBM	NVIDIAの年次サイクル	—	小さなチームは単体チップではなく、IP、チップレット、設計サービスを作る
AI推論チップ	汎用性を手放す：10〜20倍と主張 ベンダー公称	大きく細分化；中国本土の国内市場はそれ自体で大きい	N6/N7–N4のSRAMアーキテクチャなら扱いやすい	モデルとアーキテクチャへのロックイン	それ自体が主な市場	作る価値がある：顧客と契約し、それからロックインを選ぶ
ZKアクセラレータ	GPUの10〜100倍と主張 ベンダー公称	小さく、主にトークン報酬が駆動	N7/N6、次いでN5；まずFPGA	証明システムが速く変わる	ZK以外では限定的	待ちながらヘッジ：プログラマブルなMSMとNTTのエンジン
FHEアクセラレータ	Xeonの1,074〜5,547倍（Heracles）	まだ形成されていない；企業と政府に根づく	HBMが必要；コスト構造は学習チップに近い	標準とエコシステムが未確定	暗号化計算、プライベートAI	早めに布石を打ち、軽い資産で検証する；2027–2029年の機会

図07 **五つのチップの種類、五つの答え**

コスト優位kの源泉、ルールが変わった場合にシリコンが売れる先、そして判断



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

出典: 第7章と第8章の著者による整理；ベンダーの数値は本レポートでの表示のとおり。

第09章



09 プロセスノード：最大の生涯コストに選ばせる

プロセスノード

コストの階段：先端ウェハは成熟ウェハの10倍

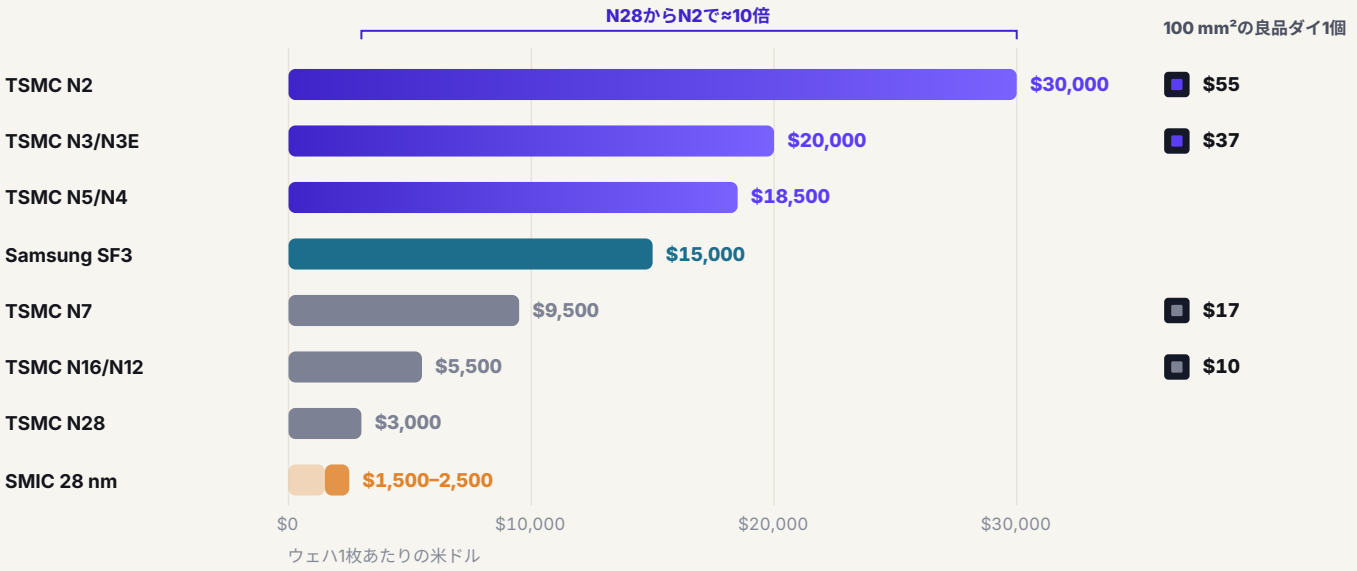
まず台帳から始める。先端ウェハは今や成熟ウェハの約10倍のコストがかかる。TSMCのN2は約30,000ドル、N3は約20,000ドル、N7は約9,500ドル、N28は約3,000ドルである。SamsungのSF3は約15,000ドルでN3より約25%安い。SMICの7 nmクラスの製造コストはTSMCより40%から50%高いと報じられている。TSMCは2027年1月からさらに3%から6%値上げすると報じられており、最も大きいのは2 nmと3 nmである。マスクと設計のコストはさらに大きく異なり、情報源によって食い違うので、表には両方を示す。

ノード	ウェハ価格（推計）	マスクセット（モデル値／ガイドの範囲）	設計予算（AnySilicon）	MPW（1プロジェクトあたり）
TSMC N2	約30,000ドル	—	3/2 nm：6,000万〜4億ドル以上	—
TSMC N3/N3E	約20,000ドル（18,000〜27,000ドル）	1,500万ドル／1,000万〜2,000万ドル	同上	—

ノード	ウェハ価格（推計）	マスクセット（モデル値／ガイドの範囲）	設計予算（AnySilicon）	MPW（1プロジェクトあたり）
Samsung SF3	約15,000ドル（13,000〜17,000ドル）	1,200万ドル	—	—
TSMC N5/N4	約18,500ドル（16,000〜21,300ドル、信頼度低）	650万ドル／1,000万〜2,000万ドル	5/4 nm：3,000万〜2億ドル	—
TSMC N7	約9,500ドル（8,100〜10,900ドル）	350万ドル／500万〜1,000万ドル	7/6 nm：1,500万〜1億ドル	商用10万〜50万ドル
TSMC N16/N12	約5,500ドル	180万ドル	16/12 nm：600万〜4,000万ドル	学術向け1 mm²あたり約35,000ドル
TSMC N28	約3,000ドル	100万ドル／100万〜300万ドル	28/22 nm：300万〜2,000万ドル	商用5万〜15万ドル；学術向け1 mm²あたり約12,000ドル
SMIC 28 nm	1,500〜2,500ドル	—	—	—
SMIC 7 nmクラス（N+2/N+3）	TSMCより40〜50%高い	—	—	—

図08 **先端ウェハは成熟ウェハの10倍のコストがかかる**

ノード別の300 mmウェハ1枚の推定価格と、歩留まり85%での100 mm²良品ダイ1個のコスト



出典: Silicon Analystsのウェハ価格（推計、N5は信頼度低）、Wccftech（SMIC）；ダイのコストは歩留まりを仮定した著者の計算。

次に物理である。Horowitzの古典的な測定によれば、プログラマブルな命令1つには約70 pJかかるのに対し、演算そのものは数ピコジュールで済む。**演算は安く、オーバーヘッドは高い**。これがシストリックアレイと専用チップが存在する理由である。加工寸法を半分にすると演算あたりのエネルギーはおおよそ半分になるが、電源電圧は0.9–1.1 V付近で止まっている。N2のウェハはN3より50%から67%高いので、密度が約1.5倍を超えて上がらない限り、トランジスタあたりのコストは下がるどころか上がる 推計 。先端ノードは効率と性能で元を取らなければならない。100 mm²のダイで歩留まり85%の場合、良品ダイ1個あたりのコストはN2で約55ドル、N3で37ドル、N5で29〜34ドル、N7で17ドル、N16で10ドルである[推計；歩留まりは仮定]。

チップの種類とチームによるノードの選択

私の原則はこうである。**チップの生涯コストのうち最大の項目にノードを選ばせる。** 常時フル稼働する計算チップ（マイニング、ZK）では電気代が生涯コストを支配するので、アルゴリズムが安定したらN5/N4やN3/SF3へ移るべきである。アルゴリズムが定まらないか資金が乏しいうちは、まず成熟ノードのMPWで検証する。学習チップのボトルネックはパッケージングとメモリであり（HBMとCoWoSはH100の部品コストの約63%）、ノードは二の次である。推論チップで最初に決めるのはメモリアーキテクチャである。SRAM中心の設計はN6/N7からN4にとどまれるが、HBMを使う設計は学習チップのコスト構造を引き継ぐ。FHEはメモリ帯域に縛られ、HBMを避けられない。

チップの種類	スタートアップまたは小さなチーム	規模の大きい企業	中国本土での道筋	要点
行列積PoUWマイニングチップ（SRAM常駐、HBMなし）	28 nmまたは16/12 nmのMPWで試作；最初の量産はN7/N6；アルゴリズムと収益が安定したらN5/N4；50–150 mm²のダイを標準的なフリップチップパッケージで	N3/N3EまたはSamsung SF3	SMIC N+1/N+2で実現可能（HBMもCoWoSも不要）、良品ダイあたり約40〜50%高い	エネルギーが支配的；プロトコルのルールが最大のリスク
SHA-256マイニングチップ	フロンティアを追わない；ニッチな形態なら成熟ノードを使える	3 nmクラス；既存勢力はTSMC 5 nmから2 nmへ、Samsung SF3から2 nmへ移行（二次情報）	先端ノードの効率に並ぶのは難しい	電力価格と半減期のサイクルが利益率を決める
AI学習チップ	単体チップは作らない：IP、チップレット、設計サービス	N3P、次いでN2/A16；2〜8個のチップレット；CoWoSとHBMを早めに確保	SMIC N+2/N+3と国産HBM（Huaweiモデル）；チップあたりのFP8はNVIDIAの約0.2〜0.5倍で、システム規模で補う	パッケージングとHBMがボトルネック
AI推論チップ	SRAM中心またはハードワイヤード、N6/N7またはN4/N5/SF4；INT8、FP8、FP4のみ	HBM付きN3/N2（長いコンテキスト、Mixture-of-Experts）、またはマルチチップレットSRAM	LPDDRまたはGDDR付きSMIC N+2；HBMクラスのメモリがチョークポイント	アーキテクチャのロックインの度合いが中心的な判断
ZKアクセラレータ	FPGAまたは16/12 nmのMPWで始める；次いでN7/N6とN5	N5/N3	SMIC N+1/N+2で実現可能	整数演算で決定論的；検証が容易
FHEアクセラレータ	FPGA（オープンソースのベースラインと比較）または16/12 nmのMPW；量産にはHBMが必要	HBM付きN5/N3	HBMへのアクセスに制約される	速度を決めるのは演算ではなくメモリ帯域

先端か成熟か、四種類のファウンドリ、そしてチップレット

選択肢	主な強み	主な弱み	最適な用途
先端ノード（N3/N2、SF3/SF2、Intel 18A）	フルノードごとに演算あたりのエネルギーがおおよそ半減；高密度SRAM	ウェハは成熟ノードの3〜10倍、マスクは5〜15倍、設計予算は10〜20倍；リードタイムは50週超；N2のトランジスタあたりコストは上がる可能性	常時稼働するアルゴリズムが安定した計算チップ；学習チップ
成熟・中位ノード（N7/N6、N16/12、N28）	マスクは100万ドル規模、安価なMPW、速い反復、多くのファウンドリ（TSMC、UMC、GlobalFoundries、SMIC）	常時フル稼働では効率で競争にならない	試作、ニッチ市場、エッジ推論
TSMC	最良の歩留まりとエコシステム	最も高い価格；N2/N3の生産能力は逼迫；CoWoSの長い待ち行列	量産のコミットメントを持ち、効率のフロンティアを追うチーム

選択肢	主な強み	主な弱み	最適な用途
Samsung Foundry	ウェハが約20〜25%安い（SF3は約15,000ドル、N3は約20,000ドル）；Groqの第2世代などが採用	ファウンドリ事業は赤字で、2027年末の損益分岐を目標としている	コストに敏感な計算チップ
Intel Foundry	HeraclesのようなIntel 3での複雑なチップで実績	18Aの外部向け価格や顧客データは公開されていない；ファウンドリ事業は赤字	エコシステムとサポートを個別に評価する
中国本土のファウンドリ（SMICなど）	大きな国内市場に近い；28 nmウェハは1,500〜2,500ドル	7 nmクラスの生産能力は月約45,000〜60,000枚で大半がHuaweiに吸収される；歩留まりはTSMCの約3分の1；コストは40〜50%高い；DUVのみ	国内市場向けの推論、マイニング、ZKチップ
チップレット	レチクルと歩留まりの限界を克服；HBMシステムでは標準（MI355X、Ironwood、Trainium3）	パッケージングコストの増加とCoWoSへの依存；良品ダイ（KGD）の試験がコストを上乗せする	学習チップと大型推論チップ；小型のマイニングチップやZKチップには不要

第10章

10

段階的予算

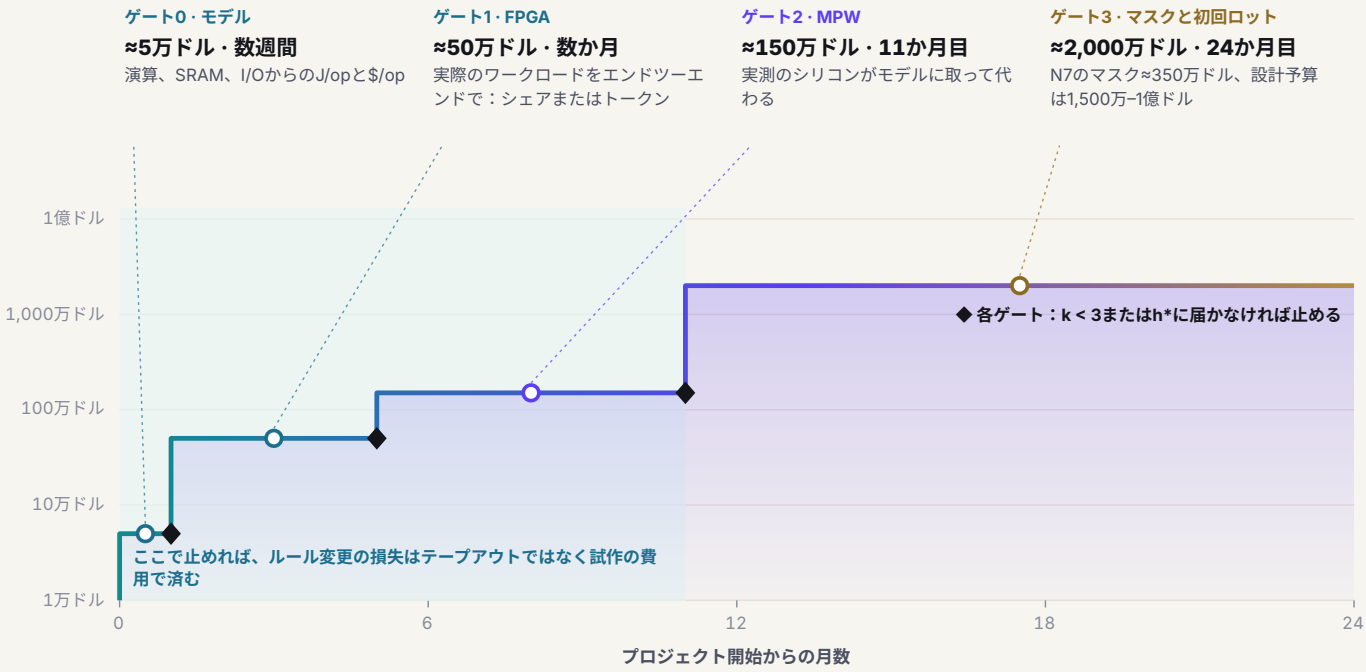
モデルからシリコンへ：最初のチップの段階的予算

マスクの前に証拠を買う

フルカスタムチップは、一つ前より大きな賭けの連続であり、その規律はマスクを買う前に証拠を買うことである。私は四つのゲートを使う 分析 。ゲート0はモデルである。演算、SRAM、I/OからJ/opと$/opを見積もり、第7章の基準となるハードウェアと比べるアーキテクチャ調査で、数週間と数万ドルかかる。ゲート1はFPGAの試作で、実際のワークロード、つまりマイニングのシェアや推論のトークンをエンドツーエンドで動かし、データパスとプロトコルとの統合を実証する。数か月と数十万ドルかかる。ゲート2はマルチプロジェクトウェハである。商用枠はN28で約50,000〜150,000ドル、N7で100,000〜500,000ドルで、実測のシリコンがモデルのエネルギー推計に取って代わる。ゲート3はフルマスクセットと最初の量産ロットである。マスクはN28で約100万ドル、N7で350万ドル、N3で1,500万ドルであり、7/6 nmでは1,500万〜1億ドルの設計予算の中に収まる。各ゲートにはプロジェクトを止める数値が必要である。たとえば限界的なハードウェアに対してkが3を下回る、あるいは期間内に届かない回収ハッシュレートh*である。

図09 **マスクの前に証拠を買う：最初のチップの段階的予算**

N7/N6プロジェクトの四つのゲートを通じた累積支出（米ドル、対数目盛）；各ゲートにはプロジェクトを止める数値がある



出典: ウェハ、MPW、マスクの価格は第9章のとおり（Silicon Analysts、AnySilicon、モデル値）；ゲートの時期と支出は著者による説明のための仮定。

この階段は急である。N7/N6のプロジェクトでは、最初の三つのゲートを合わせて約150万ドルと約11か月かかり、四つ目はその10倍以上かかる 推計。だからノードより順番のほうが重要である。プロトコルが演算方式を変えたり、買い手が去ったりしても、ゲート2で止めたチームが失うのはテープアウトではなく試作の費用である。

チップごとの費用と、成り立つための条件

プロジェクト	ゲート2（試作）	ゲート3（ノードと設計予算）	100 mm²の良品ダイ1個	回収のために成り立つべき条件
マイニングもできる推論優先のアクセラレータ	16/12 nmまたはN7のMPW、10万〜50万ドル	N6/N7、約1,500万〜3,000万ドル 推計	N7で約17ドル、パッケージングとメモリを除く	契約済みの推論顧客がNREの大半を負担する；マイニング収入は上振れ要因であり、基本シナリオではない
Pearl専用INT7マイナー（現時点では推奨しない）	28 nmのMPW、5万〜15万ドル	N7/N6、約2,000万ドル	N7で約17ドル	p = 1なら約4.9 EH/sを丸1年、p = 0.5なら9.8 EH/s（第7章）
ZKアクセラレータ	FPGA、次いで16/12 nmのMPW	N7/N6、次いでN5	N16で約10ドル、N7で17ドル	証明システムが、固定設計で対応できるMSMとNTTのカーネルに収束する
FHEアクセラレータ	オープンソースのベースラインと比較するFPGA	HBM付きN5/N3、3,000万ドル以上	HBMとパッケージングが支配的	大量の暗号化AIの買い手。まだ存在しない

ここから商業上の論点が二つ導かれる。第一に、最も安い効率はアーキテクチャから得られる。オペランドをSRAMに置き、HBMとCoWoSを省けば、ノードを選ぶ前にGPUのコストの大半（H100の部品コストの約63%）がなくなる。第二に、時間もコストである。新しいチームは着手から量産まで約18〜24か月を要し、最先端のリードタイムは50週を超える。数か月ごとに演算方式を変えるプロトコルは、ゲート3が元を取る前にチップを陳腐化させうる。

小さなチームのための三つのルール

これらの数字を合わせると、三つのルールが得られる 分析。第一に、**名前の挙がった買い手か、凍結されたプロトコルのバージョンが得られるまで、ゲート1か2にとどまる**。トークン価格もハッシュレートも、そのどちらの代わりにもならない。第二に、**kはまずアーキテクチャで、次にノードで買う**。N7上のSRAM常駐アレイは、一つのワークロードについて、マスクコストのごく一部でN3上の汎用部品を上回りうる。第三に、**テープアウトの前に、pを含めた回収に必要なハッシュレートまたは数量を書き出し**、マイルストーン払いを固定したプロトコルのバージョンに対して値付けする。そうすればルールのリスクを負うのは設計会社ではなく顧客になる。

第11章

11 機会
機会はどこにあるか、そして私なら何をするか

カスタムチップ：需要は圧倒的にAIから来る

2026年、カスタムチップの需要は圧倒的にAIから来ている。Broadcomの2026会計年度第3四半期のAI半導体収益は167億ドルで前年比221%増、通年では約580億ドルであり、その73%は6社の顧客向けのXPUによるものである（決算説明会の自動文字起こしによる）。Global Unichipの第2四半期の収益は前年比128%増で、ターンキー生産の収益は188%増、粗利率は21.5%だった。AIchipの第1四半期のノード別収益は、3/2 nmが21%、7/5 nmが63%、12 nm以上が16%だった。VeriSiliconの2026年の新規受注は4月末までに82.4億人民元（約11.6億ドル）に達し、その91.37%がAIコンピューティング向けだった。市場には三つの層がある。最上層は数十億ドル規模の複数年にわたる共同開発、中間層は7 nmから2 nmのプロジェクトでNREは数百万ドルから1億ドル超（中位ノードで500万〜3,000万ドル、最先端で3,000万〜1億ドル以上）、そしてNREが50万〜500万ドルの成熟ノードASICのロングテールである。暗号資産とマイニングの顧客は小さく循環的なニッチだが、今日計算資源に支払う、最も速く、最も許可の要らない「最初の顧客」である。

マイニングチップのチームの能力のうち最もよく移転できるもの、すなわちしきい値近傍の低電圧動作、大量に複製された計算アレイ、キロワット級の電力供給と冷却、先端ノードでの速いテープアウトは、まさに推論チップとZKおよびFHEのアクセラレータが必要とするものである。資本市場はこれを値付けしている。Velaura AI（旧Auradine）は8月に評価額10億ドル超で1億1,000万ドルを調達した。反例はCanaanのエッジAIチップ部門で、2024会計年度の収益は90万ドルでありながら営業費用の15%を消費し、2025年6月に閉鎖された。違いは、マイニングの販路を再利用するかどうかではなく、独立した市場への道筋にある。

AI開発：時間はコモディティであり、価値は継ぎ目にある

ローエンドでは、AI開発サービスはコモディティ化している。Clutchでの典型的な料金は1時間25〜49ドル、米国やカナダなどの市場では50〜99ドルである。ブロックチェーン開発チームは月約15,000ドルから90,000ドル超かかる。時間を売ることに堀はない。価値は分野の継ぎ目にある。カスタムチップ向けのカーネルとコンパイラ、推論サービングに組み込まれたマイニング（PearlのvLLMプラグインがその一例）、TEEとZKのスポットチェックを組み合わせた検証可能な推論、そしてエージェントのための決済とアイデンティティである。

AI × 暗号資産システム：トークンの前に計算資源の買い手と契約する

AIネイティブなチェーンや計算資源ネットワークを設計する人にとって、2026年の検証の道具箱は形になっている。作業単位あたりのコストが低い順に、統計的サンプリング（Hyperbolicのproof of sampling）、審判付き委任（Gensynの

Verde。誠実な検証者が1人いればよいが、ビット単位で一致する実行を必要とする）、TEE（ネイティブに近い速度だが、チップベンダーを信頼する）、完全な冗長化、そして汎用のzkMLである。実用的な設計は階層型である。低レイテンシにはTEEまたはサンプリング、ファイナリティには異議申し立てゲームまたはZKのスポットチェックを使う。2025年12月の論文は、H100のコンフィデンシャルコンピューティングに不正証明とランダムなZKスポットチェックを組み合わせ、集中型の99%のスループットと1クエリあたり0.07ドルの限界費用をシミュレーションした。ハードウェアの思想がセキュリティと分散性を決める。GPUネイティブのPoUWは当初、借りることのできるクラウドGPUによって守られるので、攻撃コストはレンタル価格に結びつく。そしてQubicは、汎用ハードウェア上のプルーフ・オブ・ワークが外部のインセンティブによって丸ごと乗っ取られうることを示している。

コストと時間は障壁ではない。Pearlは論文（2025年4月）からメインネットまで約12か月で到達した。btcdからフォークし、ローンチ時にはフルノード、ウォレット、ライトクライアント、マイナーを揃えていた。DeFiの監査の大半は25,000〜100,000ドル、企業向けやマルチチェーンの監査は150,000〜250,000ドル以上、ZK回路は80%から120%増しであり、実際に価値がリスクにさらされるプロジェクトはセキュリティに年間150,000〜500,000ドルの予算を組む。本当の障壁は流通と流動性である。創業者たちの報告によれば、Binanceは上場のためにトークン供給量の0%から3.5%、さらに8%とも言われる割合を求めた（Binanceは上場で利益を得ていることを否定している）。Cointelegraphが調べた、「トークン貸与とコールオプション」型のマーケットメイク契約を使った6プロジェクトはすべて下落し、Movementのマーケットメーカーは上場当日に約3,800万ドルのトークンを売却した。代替手段は、Binanceに上場せずに時価総額100億ドルを超え、HIP-3無期限先物市場の建玉が6月に32億ドルを超えたHyperliquidのようなオンチェーンの流動性と、MonadがCoinbaseを通じて2億6,900万ドルを調達したような、大手取引所を通じたパブリックセールである。完全希薄化後評価額が高く流通量が少ないことが、2025–2026年のローンチ後の下落を最も明確に予測する指標だった。

トークン設計はシステム設計の一部である。発行は有償需要を先導するのではなく、それに従うべきである。本レポートのネットワークのうち補助金倍率が最も健全なものは、外部の買い手が支払う作業に報酬を結びつけており、最悪のものは裏付けのないハッシュレートやステークに支払っている。実用的なルールは、ローンチ前にネットワークが1年目、2年目、3年目に目指す補助金倍率を公表し、達成できなければ発行を削減することである 分析 。

方向性	誰が買うか、支払意思	時期	主要な能力	主なリスク
マイニングもできる推論優先のアクセラレータ	ネオクラウド、プライベート導入、PoUWネットワーク	2027–2028年（FP8とFP4のフォーク次第）	INT8、FP8、FP4のGEMM；SRAMアーキテクチャ；プロトコルとの統合	プロトコルへの受け入れ、アーキテクチャのロックイン
SRAMまたはハードワイヤードの推論チップ	ネオクラウド、中国本土のデータセンター、エッジ	今	コンパイラとモデルの適応；N6–N4の設計	モデルの変化が速すぎる
マイニングチップ（ニッチまたは垂直統合）	自前の電力を持つマイナー；家庭用と暖房用のマイナー	今。半減期とハッシュプライスが制約	低電圧アレイ、効率、量産のサプライチェーン	既存勢力による価格戦争、電力価格
ZK証明の高速化	プルーバーネットワーク、ロールアップ	証明システムが収束するまで待つ	プログラマブルなMSMとNTT	需要がトークン報酬に依存
FHEの高速化	企業と政府向けの暗号化AI；プライバシーチェーン	2027–2029年	NTT、HBMシステム、暗号エンジニアリング	需要がまだ形成されていない；長い販売サイクル
TEEの強化と検証可能な推論	秘密推論ネットワーク、DePIN	今	完全性付きのメモリ暗号化、独立した認証の起点、ZKのスポットチェック	ベンダーのエコシステムへの依存

方向性	誰が買うか、支払意思	時期	主要な能力	主なリスク
AIネイティブなチェーンまたは計算資源ネットワーク	推論の買い手、マイナー、開発者	今	検証の設計、発行の設計、流通	ローンチ後の下落、トークンの流動性

私が選ぶ三つの道、それぞれの最初の一歩

選ぶとすれば、私は多くても三つの道をとり、それぞれ資金を投じる前に検証する小さな最初の一歩を置く 分析 。

- **道A：マイニングもできる推論優先のアクセラレータ。** 最初の一歩：SRAM常駐のINT8/FP8 GEMMアレイについて、Pearlの作業とTransformerの推論の両方で、RTX 5090およびH100に対するJ/opと$/opをモデル化する4週間のアーキテクチャ調査。続いて、NREを100万ドル規模に抑えたFPGAまたは成熟ノードMPWでの検証。
- **道B：暗号資産を最初の顧客、AIを第二の市場とするカスタムシリコンサービス。** 最初の一歩：本レポートのNREと損益分岐のモデルを、計算チップのプロジェクト向けの有償の実現可能性調査に仕立てる。マイルストーン払いとし、固定したプロトコルのバージョンに対して検収する。
- **道C：トークンより先に計算資源の買い手と契約するAIネイティブなネットワーク。** 最初の一歩：階層型の検証（TEE、サンプリング、ZKスポットチェック）とベンダー中立な正準演算についての設計ノートを、トークンの設計に入る前に、名前の挙がった1社の推論の買い手とともに書く。

第12章

12 注目点 注目すべきこと：2026年11月から2027年まで

時期	注目すべきこと	なぜ重要か
随時	PearlのFP8有効化高	整数ハードウェアとNVIDIA以外のカードが引き続き認められるか、そしてチェーンが分裂するかを決める
毎月	PearlでAI作業を含むブロックの割合	「有用」が現実になりつつあるかを測る唯一最良のテスト
毎月	推論プロバイダーがマイニング収入を顧客に還元するか	有償需要と発行の出会い：Pearlが必要とするモデル
四半期ごと	Bittensorの検証可能な収益と発行の比較	最大の有用作業ネットワークが補助金のギャップを縮めているか
四半期ごと	実際にエージェントが発起したx402フローの割合	エージェント決済がシグナリングから商取引へ移るか
2027年1月	報じられたTSMCの3%から6%の値上げ、最も大きいのは2 nmと3 nm	先端ノードのテープアウトのコスト
2027年第1四半期	創業者のAMAで報じられたPearlのFP4	作業がNVIDIAの最新形式へさらに移る
2027年末	Samsung Foundryの損益分岐の目標	より安い第二の供給源が健全であり続けるか
2028年4月	ビットコインの次の半減期	SHA-256マイナーのパイが半分になる

第13章

13 尋ねるべき質問

尋ねなかったが、尋ねるべきだった質問

以下は、AI × 暗号資産のどのプロジェクトであれ、資金やシリコンを投じる前に私が尋ねる質問である。

作業関数を支配しているのは誰か。 小さなチームがハードコードされたブロック高で演算を変えられるなら、あなたのハードウェアの寿命は彼らの決定次第である。書面による安定性の約束を求めるか、第二の市場を持つハードウェアを設計すること。

補助金倍率はいくつか。 発行（または時価総額）をネットワーク外から支払われる収益で割る。倍率が10を超えるなら、そのネットワークはサービスを売っているのではなく、活動を買っている。

次のゲートの費用はいくらで、何の数値で止めるか。 マルチプロジェクトウェハは数万〜数十万ドル、マスクセットは数百万ドルかかる。支出する前に止める数値を決めること。

pを含めた回収に必要なハッシュレートはいくつか。 NREを R × (1 − 1/k) × T × p で割る。答えがネットワークの大きな割合になるなら、そのチップはシリコンではなくルールへの賭けである。

チップの第二の市場は何か。 プロトコルがフォークしたりトークンが下落したりしたら、そのシリコンは他に何に売れるのか。GPUがEthereumのMergeを生き延びたのは第二の市場があったからであり、単一アルゴリズムのASICにはそれがなかった。

価値はトークンに着地するのか、エクイティに着地するのか。 2026年に利益を上げているAI × 暗号資産の企業は、大半が暗号資産の流通を持つエクイティ企業である。資金を調達する前に、二つのうちどちらを作るのかを決めること。

最初に支払う顧客は誰か、名前で言えるか。 GrassからBittensorの計算資源サブネットまで、本レポートの持続的な事例はすべて、ネットワーク外の名前のある買い手から始まった。

これらは、技術交流と技術協力を通じて、他の方々とともに探求したい領域である。マイニング、AIの学習と推論のためのカスタムチップとアクセラレータ、AI開発、そしてチェーンからノード、チップまでのAI × 暗号資産システムである。連絡先はi@tanshuai.comである。

本レポートの限界

これは2026年11月13日までの公開文書に基づくデスクリサーチである。この版のために一次インタビューも独自の測定も行っていない。Aethirの収益、Grassの収益、EtchedとTaalasの性能、Cysicの効率など、いくつかの主要な数値は企業やベンダーの主張であり、その旨を表示している。Pearlのチェーン指標は独立したフルノードとプールから得たもので、時間単位で変わる。11月13日07:13 UTC前後の値を使い、同日の範囲を示した。ウェハ、マスク、設計のコストは互いに

食い違う第三者の推計とモデル値であり、範囲で示した。私のASICの損益分岐の計算と段階的予算は説明のための仮定（k、T、p、NRE、ゲートの費用）を用いており、読者は自分の値に置き換えるべきである。

著者について

タン・シュアイは技術者・創業者であり、チップ、ハードウェア、システムソフトウェアにわたる20年以上の経験と、20件の登録特許を持つ。ファブレスのチップ研究開発とマネジメントに長年携わり、暗号資産マイニングチップとマルチメディアカメラチップのフルカスタムASICデータパス設計も手がけてきた。それが本レポートの視点である。演算あたりのエネルギー、ウェハあたりのコスト、プロトコルがシリコンに何を固定させてくれるか、そして誰が支払うか。その仕事はシリコンバレー、ニューヨーク、シカゴ、台湾、粤港澳大湾区（深圳と香港）、ベトナム、マレーシアに及ぶ。現在はAI研究者・開発者として活動している。

技術的な議論：i@tanshuai.com · tanshuai.com

注記と免責事項

本レポートは、2026年11月13日までに入手可能な公開文書に基づく独立したデスクリサーチである。情報提供と学習のみを目的としており、投資やエンジニアリングに関する助言ではない。扱うのは技術とビジネスのみである。価格、チェーン指標、プロトコルのルールは変わる。依拠するものはすべて一次情報源で確認してほしい。 ベンダー公称 、 推計 、 分析 と表示された数値は、そのようなものとして読むべきである。暗号資産の価格は非常に変動が大きい。

© 2026 タン・シュアイ。出典を明記すれば、本レポートを改変せずに共有してよい。

出典

すべて2026年11月10日から11月13日の間に閲覧した。章ごとにまとめている。

Pearl：プロトコル、コード、チェーンデータ

- Komargodski and Weinstein、「Proofs of Useful Work from Arbitrary Matrix Multiplication」、arXiv 2504.09971： https://arxiv.org/abs/2504.09971
- Pearl Research Labs、INTホワイトペーパー： https://pearlresearch.ai/research/int-whitepaper
- Pearlのソースコード：ジェネシスブロック： https://github.com/pearl-research-labs/pearl/blob/main/node/chaincfg/genesis.go ; コンセンサスパラメータとフォーク高： https://github.com/pearl-research-labs/pearl/blob/main/node/chaincfg/params.go ; ハッシュレートの算定： https://github.com/pearl-research-labs/pearl/blob/main/zk-pow/src/api/sanity_checks.rs ; ソルト付きシードのフォークのアップグレードガイド： https://github.com/pearl-research-labs/pearl/blob/main/docs/salted-seed-fork-upgrade-guide.md ; fp8-schemeブランチのパラメータ： https://github.com/pearl-research-labs/pearl/blob/fp8-scheme/node/chaincfg/params.go
- Pearl Improvement Proposals： https://github.com/pearl-research-labs/pips ; PIP-3、浮動小数点マイニング： https://github.com/pearl-research-labs/pips/blob/main/PIPS/pip-0003.md
- prlstats（独立フルノード）：ネットワーク： https://prlstats.com/api/network ; 系列： https://prlstats.com/api/series ; ホームとマイナー収入モデル： https://prlstats.com/api/home ; 採掘済み供給量： https://prlstats.com/api/mined ; プール： https://prlstats.com/api/pools ; 保有者： https://prlstats.com/api/holders ; ハードウェアとオーバーヘッドの前提： https://prlstats.com/api/assumptions
- Kryptex Pool：Pearlネットワーク： https://pool.kryptex.com/prl/about-coin ; ハッシュレート： 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 ; 価格履歴： https://api.coingecko.com/api/v3/coins/pearl-2/market_chart?vs_currency=usd&days=365&interval=daily ; 「Perle」ティッカー検索： 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、Pearl Research Labsとの提携： https://together.ai/blog/together-ai-partners-with-pearl-research-labs ; モデルのページ： https://together.ai/models/gemma-4-31b-it-pearl
- Basu、Pearlのマイニングインスタンスの調査、 arXiv 2606.04819： https://arxiv.org/html/2606.04819v2
- Blockworks、0xResearchニュースレター、 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、Pearl Research Labsの資金調達に関するTheMarkerの報道について： https://www.coingabbar.com/en/pearl-research-labs-funding-130m-stealth-round-themarker

有用作業チェーンと歴史

- Grotheら、Gridcoinのセキュリティ分析、 USENIX WOOT 2017： https://www.usenix.org/system/files/conference/woot17/woot17-paper-grothe.pdf
- 学習の証明（proof-of-learning）の偽装、 arXiv 2208.03567： https://arxiv.org/abs/2208.03567
- hoge.gg、分散型推論における検証と信頼： https://hoge.gg/decentralized-inference-2026-verification-trust/ ; Bittensorの収益とトレジャリー： https://hoge.gg/bittensor-quantum-wallet-revenue-tao-treasury-2026/
- Kaspa：kHeavyHashの行列コード： https://github.com/kaspanet/rusty-kaspa/blob/master/consensus/pow/src/matrix.rs ; ローンチ： https://coinranking.com/coin/V8GxkwWow+kaspa-kas/about ; IceRiver KS1/KS2の発表： https://www.iceriver.io/2023/03/14/1677644580/ ; GPUからASICへの歴史： https://captainmining.com/blogs/crypto-news/the-evolution-of-kaspa-mining-from-gpus-to-asic-powerhouses ; GPUのハッシュレート： https://coincalculators.io/algorithms/kheavyhash ; KS7： https://www.asicminervalue.com/miners/bitmain/antminer-ks7-40th ; ネットワーク： https://minerstat.com/coin/kas ; 2024年の1 EH/s： https://ourcryptotalk.com/news/kaspa-reaches-1-ehs-in-hashrate ; Crescendo： https://ourcryptotalk.com/news/kaspa-crescendo-live
- Aleo：メインネットFAQ： https://aleo.org/post/aleo-mainnet-faq/ ; 分散型の証明： 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：Moneroの再編成に関するThe Blockの記事： 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のマイニング： https://hackernoon.com/qubic-is-now-mining-dogecoin-on-its-ai-compute-infrastructure ; CoinGecko： https://www.coingecko.com/en/coins/qubic

- Bittensorのコンセンサスに関するドキュメント： 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とASIC耐性のためのフォーク： https://lbry.com/news/forking-for-asic-resistance ; Siaのフォーク： https://hotfix.coindesk.com/markets/2018/11/01/sia-completes-hard-fork-as-bricked-miners-form-rival-blockchain ; Obeliskの価格： https://www.cryptoglobe.com/latest/2018/11/obelisk-hardware-skyrockets-in-selling-price-after-sia-hard-fork/ ; Merge後のマイナー： https://hotfix.coindesk.com/business/2022/11/11/ex-ethereum-miners-token-hop-to-stay-alive-after-the-merge

AI × 暗号資産の各セクター

- DefiLlama：Render： https://defillama.com/protocol/render-network-bme ; Livepeer： https://defillama.com/protocol/livepeer
- Cointelegraph、MessariによるDePINの収益について： https://cointelegraph.com/news/depin-revenues-grow-despite-token-losses
- Aethir、2025年のまとめ： https://aethir.com/blog-posts/aethirs-2025-wrap-up-decentralized-gpu-cloud-milestones
- CoinGecko、AIカテゴリー： https://www.coingecko.com/en/categories/artificial-intelligence
- Akash、H100のレンタル価格： https://akash.network/the-bid/h100-rental-price-2026-cost-per-hour/ ; 2026年第1四半期レポート： https://akash.network/blog/akash-network-q1-2026-report/
- io.net、800万ドルの契約と1日のトークン数： 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の契約： 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、INTELLECT-3について： https://www.implicator.ai/prime-intellects-intellect-3-open-source-ambition-meets-centralized-reality/
- SiliconANGLE、Prime Intellectの資金調達： 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の資金調達： https://runtimewire.com/article/nous-research-75-million-round-1-5-billion-valuation
- ownyourmind、Gensyn： https://ownyourmind.ai/projects/gensyn/ ; Phemex、Ritual（見出しのみ）： https://phemex.com/news/article/ritual-launches-ai-layer-1-mainnet-and-ritual-token-price-dives-72-from-high-101259
- コンフィデンシャルコンピューティングのオーバーヘッド、 arXiv 2409.03992： https://arxiv.org/abs/2409.03992v2 ; Phala 2025年レポート： 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、AIエージェント決済の測定： https://www.trmlabs.com/trm-tech-blog/whos-actually-paying-measuring-ai-agent-payments-onchain ; Forkast、x402 Foundationについて： 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のメインネット： https://www.theblock.co/amp/post/394131/tempo-mainnet-goes-live-with-machine-payments-protocol-for-agents ; BlockEden、VirtualsのaGDPについて： https://blockeden.xyz/blog/2026/04/21/agdp-agent-gdp-virtuals-protocol-ai-blockchain-valuation-primitive-tvl-displacement/ ; The Block、ElizaOSについて： https://theblock.co/post/410774/eliza-labs-native-token-dead
- Dealroom、Grassの収益： https://dealroom.co/news/157794-grass-backed-by-multicoin-projects-75m-in-2026-data-revenue/ ; CryptoSlate、Fetch.aiとOcean： https://cryptoslate.com/cryptos-flagship-ai-pact-fracture-fetch-sues-ocean-over-263m-fet-community-sales/ ; Fortune、Worldについて： https://fortune.com/2026/06/01/internet-according-to-sam-altman-seeing-orb/
- Galaxy、暗号資産のベンチャーキャピタル： https://www.galaxy.com/insights/research/crypto-blockchain-venture-capital-q3 ; Crypto Briefing（見出しのみ）： https://cryptobriefing.com/crypto-vc-investment-q3-2026-galaxy/ ; Blockhead、Tiger Researchについて： https://www.blockhead.co/2026/10/14/bitcoin-rose-43-in-q3-crypto-venture-funding-did-not-follow/ ; ForkLog、2025年のトークンローンチについて： https://forklog.com/en/85-of-tokens-launched-in-2025-fell-below-initial-prices/

ASICの経済性とチップの種類

- Hashrate Index、2026年11月9日のまとめ： https://hashrateindex.com/blog/hashrate-index-roundup-november-9-2026/
- AnySilicon、2026年のノード別ASIC設計コスト： https://anysilicon.com/news/how-much-does-asic-design-cost-in-2026-real-price-ranges-by-process-node/ ; Silicon Analysts、ファブレスのテープアウトコストガイド： https://siliconanalysts.com/analysis/fabless-startup-tapeout-cost-guide ; 市場データ： https://siliconanalysts.com/market-data
- MillionMiner、Bitmain S23 XP Hyd： https://millionminer.com/news/bitmain-wdms-2026-s23-xp-hyd-launch
- KhattakとMikaitis、テンソルコアにおけるFP8の累算、 arXiv 2512.07004： https://arxiv.org/html/2512.07004v2
- Canaan、2026年第2四半期決算： https://finviz.com/news/389337/canaan-inc-reports-unaudited-second-quarter-2026-financial-results ; Bitdeer、2026年第3四半期決算： 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とBlock： https://theenergymag.com/news/2026-07-29/core-scientific-exit-block-bitcoin-deal-ai ; AIリースの経済性： https://theenergymag.com/news/2026-08-06/miner-weekly-ai-pumpability-out-fuel
- Blockworks、Cipherと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、2027会計年度第1四半期決算： https://globenewswire.com/news-release/2026/11/05/3397020/0/en/iren-reports-q1-fy27-results.html

- Spark、ビットコインASIC市場の集中度： https://www.spark.money/research/bitcoin-asic-manufacturer-market-concentration
- Google、TPU7xのドキュメント： 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の論文、 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の価格： 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推論アクセラレータの比較： https://themenonlab.blog/blog/ai-inference-accelerators-compared ; Introl、GPU以外のAIアクセラレータ： https://introl.com/blog/ai-accelerators-beyond-gpus-tpu-trainium-gaudi-cerebras-2025
- StratNews（Reuters）、国費で建設されるデータセンターの国産AIチップ： https://stratnewsglobal.com/team-sng/china-orders-state-funded-data-centres-to-use-domestic-ai-chips/ ; TNW、H200の輸入： https://thenextweb.com/news/nvidia-h200-chips-hong-kong-china-import-approval
- Succinct、16基のGPUでのリアルタイム証明： https://blog.succinct.xyz/real-time-proving-16-gpus/ ; CysicのZK ASIC製品： 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とSemiFive： https://evertiq.com/design/2026-02-20-semifive-secures-design-win-with-niobium-for-fhe-accelerator ; The Quantum Insider、Niobiumの資金調達： 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上のHPU： https://www.zama.org/post/announcing-hpu-on-fpga-the-first-open-source-hardware-accelerator-for-fhe

プロセスノード

- Silicon Analysts、ウェハ価格： https://siliconanalysts.com/data/wafer-pricing
- Tom's Hardware、TSMC A16の価格に関する噂： 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、SMICの価格： https://wccftech.com/smic-5nm-chip-prices-up-to-50-percent-more-expensive/amp/
- EUROPRACTICE、TSMC MPWスケジュール2026： 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、Huawei Ascendのロードマップ： 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、中国のAIチップのサプライチェーン： 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

機会とローンチの経済性

- Webull（Benzinga）、Broadcomの決算説明会： https://www.webull.com/news/15511095937917952 ; Quartr、Global Unichip 2026年第2四半期： https://quartr.com/events/global-unichip-corp-3443-q2-2026_F9×6NJQY ; Taiwan News、AIchip： https://www.taiwannews.com.tw/news/6370946 ; Design & Reuse、VeriSilicon： 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、Canaanの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開発の料金： https://clutch.co/developers/artificial-intelligence/pricing ; PixelPlex、ブロックチェーン開発のコスト： https://pixelplex.io/blog/blockchain-development-cost/
- Hyperbolic、proof of sampling： 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 ; 階層型の検証、 arXiv 2512.20176： https://arxiv.org/abs/2512.20176v1
- Sherlock、2026年の監査価格の参考： https://sherlock.xyz/post/smart-contract-audit-pricing-a-market-reference-for-2026
- Blockworks、Binanceの上場基準： https://blockworks.com/news/binance-listing-standards-scrutiny ; Cointelegraph、マーケットメイク契約： 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

有用作業証明 · 暗号資産 × シリコン

計算は合意である

2026年のAI × 暗号資産 × 半導体：Pearlの有用作業証明から

本レポートの主要な数値にはすべて出典と日付を付けている。著者が導いた数値は推計として、販売者だけが報告している数値はベンダー公称として表示している。本レポートが扱うのは技術とビジネスのみである。

タン・シュアイ

技術者・創業者・AI研究者・開発者

tanshuai.com · i@tanshuai.com

公開版 · データ基準日：2026年11月13日

