THE VERIFIER - REPORTS

REPORT NO. 02

The Proving Economy

"Proof is a commodity now - real-time, market-priced, and cheap enough to disappear."

CLAIM UNDER TEST

JULY 2026

FREE TO READ - NEVER SPONSORED

SHA-256 2b79c565557e819f3d54229bb1319539
7c845d1547e7331c6a7c9df4dede9fb8

FINGERPRINT OF THE CANONICAL TEXT - RECIPE IN APPENDIX B

CONTENTS

PROLOGUE

How to read this report

This is a Verifier report, and it obeys the house rules: one question, stated on the cover as a claim; every material claim inside logged in the ledger at Appendix A with a status and a source; a SHA-256 fingerprint of the canonical text printed here and recomputable by any reader using the recipe in Appendix B; a section that names what would change our verdicts; and a corrections log on the public record. It is the second report in this series and a deliberate companion to the first: Report No. 01 asked what proof can buy - which claims about AI a proof can actually settle. This report asks what proof costs, who sells it, and whether the thing being sold is yet the thing being advertised.

This report is not sponsored; Verifier reports never are. And the conflict disclosure here is broader than the first report's, because the subject sits closer to home: The Verifier's founder holds commercial roles at companies building zero-knowledge virtual machines, proving infrastructure and agent-accountability systems. Those companies and their products are excluded from this report's coverage, comparisons, benchmarks and rankings throughout, which means among other things that the survey of proving systems in these pages is deliberately non-exhaustive. Readers deserve to know both that the conflict exists and what its handling costs the report: completeness, traded for cleanliness.

One reading instruction, carried over from Report No. 01 and even more necessary here. This is a field that measures itself in multipliers, and a multiplier is a fact about a baseline as much as a fact about a product. Costs "fell 45-fold" against what starting point, on whose hardware, proving which workload, at which security setting? Where this report quotes a number, the ledger records who measured it and against what; where two credible parties dispute a number, the dispute is the finding and is reported as one. The desk's standing manual for reading proving benchmarks applies to every figure in this document, including ours.

THE FINGERPRINT

SHA-256 `2b79c565557e819f3d54229bb13195397c845d1547e7331c6a7c9df4dede9fb8`

Recompute it: take report-02-canonical.txt, decode entities, remove all whitespace, lower-case, hash. Full recipe in Appendix B.

PART ONE

The Question

CHAPTER 01

The claim under test

Two years ago, cryptographic proof of general computation was a bespoke service: slow, artisanal, priced by negotiation, and delivered by the handful of teams who could build it. The claim under test is that this has ended - that proof has become a commodity: generated in real time, priced by open markets, produced by interchangeable suppliers, and cheap enough that the applications built on it can stop mentioning it. The industry making the claim assembled the evidence for it at remarkable speed through 2025 and into this year: a public benchmark declaring real-time proving of the largest smart-contract network achieved, two open marketplaces auctioning proof generation to anyone with capable hardware, and per-proof prices quoted in cents. This report tests the claim against the record as of July 2026, and the finding, in one sentence, is that proving has commoditised its speed and has not yet commoditised its trust - and that the gap between those two, which the market spent 2025 ignoring, is now the story the field's own governing institutions are telling about themselves.

THE SCOREBOARD - SIX SEGMENTS, ONE STANDARD

SEGMENT	WHAT THE RECORD SHOWS	STATUS
Real-time base-layer proving	99% of blocks proven inside ten seconds - on curated benchmark hardware, off-chain	VERIFIED as benchmark, TRACKING as deployment
The zkVM layer	General programs in ordinary languages, proven in production at scale	VERIFIED
Proving marketplaces	Two live networks, opposite auction designs, prices near zero under token subsidy	EARLY
Hardware	GPU proving dominant; the bottleneck named; specialised silicon still a thesis	TRACKING
Soundness	Foundational conjectures disproven; advertised security levels cut; a common ruler imposed	CONTESTED
The price trend	Order-of-magnitude cost collapse, corroborated across independent parties	VERIFIED

Three numbers frame what follows. The first is sixteen - the seconds it now takes to prove an Ethereum block that took sixteen minutes a year earlier, a sixtyfold collapse the ecosystem's public benchmark corroborates and this publication has tracked as a standing beat. The second is two cents - the most aggressive per-proof price claimed by any prover this year, a vendor figure for a closed-source system that we ledger accordingly, but which sits within sight of open-market auction results that regularly clear near zero. The third is eighty - the bits of security that a system advertising one hundred may actually possess, by the governing foundation's own December accounting, after researchers disproved conjectures the advertised numbers rested on. The first two numbers are why the commodity claim exists. The third is why it fails, for now: a commodity requires a quality grade someone enforces, and the proving economy discovered in December that its grades were self-reported.

> The market learned to price the proof before anyone finished pricing the risk. That ordering, not the latency chart, is the state of the proving economy.

CHAPTER 02

The Commodity Test

"Commodity" is doing heavy work in the industry's self-description, so this report grades it against what the word actually requires. A functioning commodity market has five properties, and each maps cleanly onto proving. First, a standard unit: buyers must know what one of the thing is. Second, a posted price: discovered in the open, not negotiated in private. Third, interchangeable suppliers: any qualified producer's output settles the same contract. Fourth, an enforced quality grade: an assay everyone accepts, run by someone other than the seller. Fifth, a delivery guarantee: late or missing product carries a penalty the market itself enforces.

THE COMMODITY TEST - PROOF AGAINST THE FIVE PROPERTIES

PROPERTY	WHERE PROVING STANDS, JULY 2026	STATUS
Standard unit	Cycles, blocks and gas all in use; the public benchmark normalises per block, markets meter per cycle	EARLY
Posted price	Open auctions exist and clear publicly - at prices token incentives currently hold near zero	CONTESTED
Interchangeable suppliers	Two networks, incompatible designs; proofs verify universally, supply does not yet interchange	TRACKING
Enforced quality grade	Self-reported security until December; a common ruler now mandated, first deadlines just passed	CONTESTED
Delivery guarantee	Deadlines, staking and slashing live on both marketplaces	TRACKING

The test does two jobs. It converts a marketing word into a checklist, which is this publication's basic move. And it locates the interesting failure precisely: the proving economy's weakest property is not price or speed, where the progress is real and independently corroborated, but the assay - the fourth property - where 2025's self-graded security met 2026's mathematics and lost bits. The chapters of Part Two walk the supply chain from benchmark to marketplace to silicon to soundness; the test above is the rubric they are graded against, and the verdict chapter returns to it.

CHAPTER 03

The year the speed debate ended

Every commodity market begins with someone publishing a standard, and the proving economy's standard arrived in July 2025 as a north-star definition from the Ethereum Foundation: real-time proving would mean proving at least 99% of mainnet blocks within ten seconds - inside the network's twelve-second slot, minus roughly a second and a half of propagation - on hardware costing no more than about one hundred thousand dollars, drawing no more than ten kilowatts, with fully open source code, proofs at or below three hundred kilobytes, and 128-bit security. That single sentence quietly created the field's first complete specification of the product: latency, capital cost, energy, openness, size and grade, all in one buyable description.

Nine months later the foundation declared the performance half of it met. Its December accounting, drawn from the EthProofs public benchmark this desk checks as routinely as a markets page, recorded proving latency for an Ethereum block falling from sixteen minutes to sixteen seconds across the year, costs collapsing forty-five-fold, and participating zkVMs proving 99% of mainnet blocks in under ten seconds on target hardware. The sprint was corroborated in the open: EthProofs aggregates per-block

proofs from competing teams with cost, latency and size attached, downloadable and comparable, which makes the speed story one of the better-evidenced performance claims this publication covers in any field. The same December post then did something rarer than declaring victory - it changed the subject, to security, in terms Part Two returns to at length.

Two boundary conditions belong in permanent ink before the celebration is quoted anywhere. The benchmark is off-chain: the numbers come from curated hardware running curated workloads, and there is, in the foundation's own framing, a real distance between that and thousands of independent operators proving at home - the "home prover" the specification's cost and power ceilings were written for. And the specification's grade line - 128-bit security - is the one line the December accounting could not yet tick, which is precisely why the sprint's finish line became the security race's starting gun. The speed debate is over because the referee said so and published the tape. What the referee said next is the reason this report exists.

One consequence of the specification deserves its own sentence, because it is the quiet strategic payload: proofs fast enough, small enough and sound enough for the base layer can be reused by everything above it through precompiles, at which point the boundary between a rollup and base-layer execution stops being an architecture and becomes a configuration - and a base layer that can verify its own blocks in real time can raise its gas limit without asking home stakers to re-execute what they can now merely check. The sixteen seconds is not a vanity metric; it is the load-bearing number under the largest capacity roadmap in the field.

> **VERDICT SPLIT** Real-time proving is VERIFIED as a benchmark result: public, corroborated, reproducible in its published setting. As a deployed reality it is TRACKING: off-chain, on curated hardware, with the specification's security line still open. Quote the sixteen seconds with the asterisk attached.

PART TWO

The Supply Chain

CHAPTER 04

The zkVM layer: generality won

The machine at the centre of the proving economy is the zero-knowledge virtual machine, and its significance is easiest to state as what it removed: the circuit artisan. A zkVM takes an ordinary program - Rust, mostly, compiled to the open RISC-V instruction set - executes it, and emits a proof that the execution was faithful, without the developer designing cryptographic circuits or, ideally, knowing what one is. Two years ago that was a research demo; in 2026 it is the production interface of the entire field. The public block-proving race is run on zkVMs; the marketplaces of the next chapter sell zkVM cycles; and the year's most instructive single proof - a March demonstration in which Google used one to prove the existence of a quantum-computing result without revealing the result itself - was a zkVM job, and a neat bridge to the inference proofs of this report's companion volume, since proving an AI model's execution and proving a block's execution are, to the machine, the same job at different sizes.

Because the layer matured, its vendors did what vendors of maturing layers do: they started benchmarking each other, and the dispute is a better guide to the field's state than either party's numbers. One major zkVM team published measurements putting its system at least seven times cheaper than its principal rival, and up to sixty times cheaper on small workloads; the rival replied that the comparison misleadingly set CPU results against GPU results, and countered with a two-cent, roughly two-minute proof from a prover that was, at the time of the claim, closed source. This publication's proving-benchmark manual exists for exactly this exchange, and its questions dispose of it cleanly: whose hardware, whose workload, whose security parameters, and can anyone outside the lab rerun it? Until both sides answer identically, the honest ledger entry is CONTESTED - and the deeper finding is that a field with a public per-block benchmark for one workload still lacks a neutral, cross-vendor benchmark for the general case, which is a strange gap for an industry selling verifiability.

One more development belongs to this layer's record because of where it points. The proving industry spent part of 2026 walking into the subject of our first report: one prover operator shipped a consumer camera application that signs photographs at capture inside the phone's secure hardware and embeds the record in the open provenance standard - the content-credential machinery of Report No. 01, built by a proving company. Hash-based, post-quantum-oriented proof variants also moved from papers toward product, at low single-digit prover overhead by their developers' measure. The layer, in short, is no longer only selling to blockchains; it is selling to every buyer the first report surveyed, which is the strongest available evidence that the zkVM has become what its builders always claimed: general infrastructure.

> VERDICT VERIFIED — The zkVM layer is the proving economy's settled ground: general programs, ordinary languages, production scale, multiple independent implementations. Its benchmarks against each other remain CONTESTED - a field this instrumented owes itself a neutral cross-vendor ruler, and does not yet have one.

CHAPTER 05

The marketplaces: two auctions in search of a price

If the zkVM is the factory, 2025-26 built the exchange floor: open networks where anyone needing a proof posts the job and anyone with hardware bids to produce it. Two are live at scale, and they are a controlled experiment in market design, because they chose opposite answers to every question. One

runs a reverse Dutch auction - the price starts at or near zero and rises until a prover locks the order - with rewards flowing mostly through a points-and-token programme that pays for verifiable work performed; its supply side is long-tailed and open, its direct fees, in the current oversupplied phase, routinely compress to zero. The other runs a sealed low-bid auction denominated in its own staked token, with a base fee plus metered compute paid immediately, deadlines measured in minutes, and slashing for provers who lock work and miss it; its supply side is smaller and more capitalised - on the order of thirty active provers by its own dashboard - and its clearing prices are legible but shaped by the stake required to play. One network reports millions of proofs generated for production protocols and several billion dollars of value secured; the other reports a high-frequency open marketplace absorbing substantial compute across chains, with a May protocol upgrade its team credits with cutting proof costs by up to half. Every number in this paragraph is operator-reported and ledgered as such.

What the twin experiment has already demonstrated is genuinely important: proof generation can be outsourced to an open market and delivered against deadlines with economic penalties - the fifth property of the Commodity Test, functioning. What it has not yet demonstrated is a price. When direct fees clear at zero because token emissions backfill the revenue, the posted price is an advertisement for the subsidy, not a measurement of the cost; when the alternative design's floor is set by staking requirements, the price includes a capital charge that has nothing to do with computation. Both networks know this - oversupply plus incentives is a bootstrapping phase, not a scandal - but the commodity claim rests on price discovery, and the honest reading of mid-2026 is that the auctions are discovering the shape of the market faster than the level of the price. The centralisation ledger cuts both ways too: the open design spreads work across many small operators at the cost of near-zero operator revenue; the staked design pays operators real fees at the cost of concentration among the well-capitalised, and independent analysis of both notes the familiar endgame risk - proving pools, and beneath some pools, a single entity renting cloud GPUs behind a decentralised facade. Secondary analyses of the wider prover-services market - a market such reports size in the tens of millions of dollars, with a handful of providers taking most fees and the large majority of validity-proof networks relying on a few proving services - point the same direction, and we log those figures as the estimates they are.

> **VERDICT EARLY** The marketplaces prove the mechanism: open supply, deadlines, slashing, delivery. They do not yet prove a price - fees near zero under emission subsidy are a bootstrap reading, not a market reading. The Commodity Test's second property stays open until a proof clears at a fee somebody actually paid because they had to.

CHAPTER 06

The hardware floor

Beneath the markets sits the machine room, and its 2026 state is easy to summarise: the graphics processor won the first era, and everyone building the second era is aiming at one named bottleneck. Proving is not matrix arithmetic - the operations that dominate it, multi-scalar multiplications and number-theoretic transforms over finite fields, are precisely the work GPUs were never designed for, and after years of optimisation squeezing the former, practitioner accounts now place the latter at up to ninety percent of proof-generation latency on graphics hardware. That number is the entire investment case for specialised silicon, and the field's direction of travel is visible in its instruction set politics: the same open RISC-V architecture the zkVMs execute is becoming the design substrate for proving accelerators, which keeps the hardware race inside an open standard rather than a proprietary one - a small structural mercy the rest of computing did not get.

The economically interesting ceiling, though, was set not by a chipmaker but by the specification of the previous chapter: about one hundred thousand dollars and ten kilowatts. Those two numbers define the home prover - the independent operator the base layer's decentralisation story requires - and they are the quiet answer to the centralisation anxieties of the marketplace chapter. If meeting the latency line keeps requiring curated clusters, proving consolidates into data centres and the proof market inherits the industrial structure of cloud computing, with its economics and its jurisdiction. If commodity hardware inside the ceiling holds the line as software improves, the long tail survives. The record so far supports cautious movement toward the second outcome - the forty-five-fold cost collapse was achieved substantially on hardware within the specification's envelope - but capital intensity has its own gravity, and the specialised-silicon era, if it arrives, arrives with fabrication costs that only concentrate. The desk's rule for this chapter's claims: any latency or cost figure quoted without its hardware bill attached is an advertisement, and the public benchmark's habit of publishing the bill is most of why this field's speed story earned its VERIFIED above.

> **VERDICT TRACKING** GPU proving is production fact; the bottleneck is named and public; the specification's cost-and-power ceiling gives the decentralisation question a number. Specialised silicon remains a thesis with excellent arguments and no shipped verdict. Watch the hardware bill on every record claim.

CHAPTER 07

The soundness reversal

Then came December, and the most consequential paragraph the proving economy has published about itself. Having declared the performance race won, the base layer's governing foundation announced that the mathematics underneath much of the field had been quietly weakening: several STARK-family systems rest on conjectures that researchers had begun formally disproving, and each fallen conjecture takes security bits with it - a system advertising one hundred bits, in the foundation's own formulation, may actually possess eighty. The consequence was stated with unusual bluntness for institutional prose: a forged proof is not a bug like other bugs, because whoever can forge a proof can mint assets, rewrite state and make the system lie. Speed without soundness, the argument concluded, is a liability - which is a striking sentence to publish three paragraphs after declaring the speed target crushed.

What followed is the assay office the Commodity Test found missing. The foundation imposed a common ruler: soundcalc, a maintained calculator that estimates a proof system's security from current cryptanalytic bounds rather than from its vendor's assumptions, with integration mandated for every participating team by the end of February. It then published hard gates with names and dates: by the end of May - the Glamsterdam window - at least one hundred bits of provable security as soundcalc estimates it, final proofs at or below six hundred kilobytes, and a public account of each team's recursion architecture with an argument for its soundness; and by the end of the year, under the H-star label, the full 128 bits, proofs back under three hundred kilobytes, and formal soundness arguments. Two honest footnotes attach. The May gate quietly treats one hundred bits as an interim standard, walking the original 128 back for early deployment - a pragmatic retreat the record should state plainly. And the ruler itself moves: soundcalc exists precisely because the safe-parameter frontier keeps shifting as conjectures fall, so today's compliant one hundred bits is a measurement, not a promise.

The foundation's post is also careful to argue the gates are reachable rather than aspirational, and the named path matters for anyone auditing progress: compact polynomial-commitment schemes and related techniques - WHIR and JaggedPCS are the ones cited - plus deliberate grinding and a

well-structured recursion topology are presented as sufficient machinery for the milestones, with recursion singled out as the under-documented joint: modern systems compose many circuits through custom recursion with, in the foundation's phrase, lots of glue in between, and documenting that glue is itself a security deliverable. The longer arc is stated too - once architectures stabilise against these gates, the formal-verification investment already underway can bind to fixed targets, which is how a moving field eventually gets mathematics-grade assurance rather than deadline-grade assurance.

And here this report must log a silence. The Glamsterdam deadline passed at the end of May, five weeks before this report went to press, and the indexed public record as we closed contained no consolidated scorecard of which teams met it - no foundation tally, no cross-team accounting, while the benchmark site's promised security columns were still being awaited. Absence of a report is not failure; teams may have cleared the gate quietly, and January's promised formalisation may simply be running behind the engineering. But a field whose entire product is checkability, five weeks past its own first security deadline, without a public pass-fail list, is a finding this publication is built to record - and the first entry in this report's marker table is the commitment to publish that list, ours or theirs, the moment it exists.

VERDICT CONTESTED

The proving economy's quality grade was self-reported until December, was found inflated by falling conjectures, and is now being rebuilt around a common ruler with dated gates - the first of which has passed without a public scorecard. This is the Commodity Test's failing property and the year's real story. What would move it: the Glamsterdam tally, published.

PART THREE

The Economics

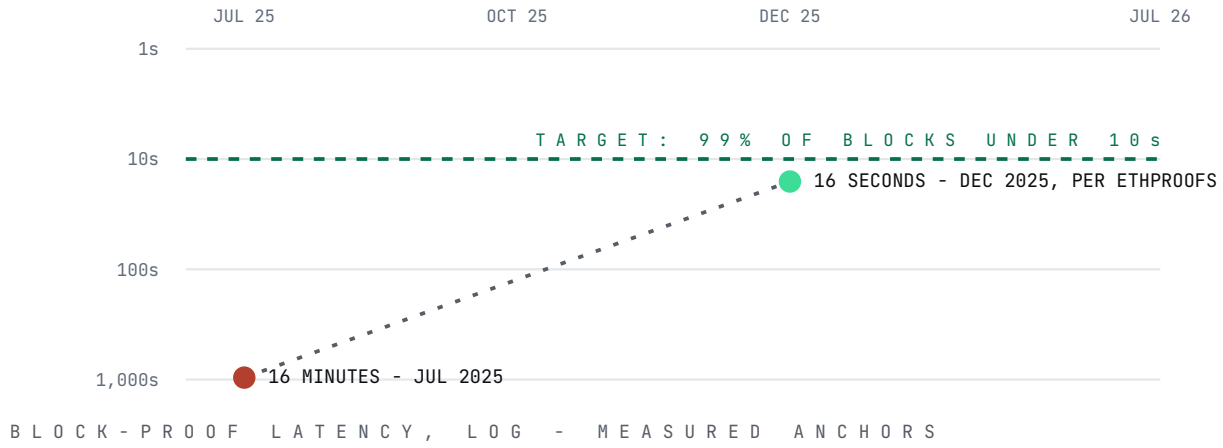
CHAPTER 08

The price of a proof

Assemble the supply chain into a bill, and the proving economy's honest price list for mid-2026 reads as follows. The cost of proving an Ethereum block collapsed forty-five-fold in a year by the referee's accounting - the trend every independent party corroborates and the single best-evidenced number in this report. The most aggressive absolute price claimed is two cents per proof at roughly two minutes, a vendor figure for a system closed at the time of the claim, ledgered as such. Open-market auction fees clear at or near zero - a subsidy reading, per the marketplace chapter, not a cost reading. A protocol upgrade on one network is credited by its operator with halving proof costs in May. And the specification's capital ceiling prices the means of production at one hundred thousand dollars and ten kilowatts - the first time this field has had a canonical hardware bill to divide its per-proof numbers by.

WHAT A PROOF COSTS - THE JULY 2026 PRICE LIST, WITH PROVENANCE

LINE ITEM	FIGURE	WHO MEASURED IT
Ethereum block, cost trend	Down 45x across the year	Ethereum Foundation, per EthProofs - corroborated
Ethereum block, latency	16 minutes to 16 seconds; 99% under 10s	Ethereum Foundation, per EthProofs - corroborated
Cheapest claimed proof	~$0.02 at ~2 minutes	Vendor claim, system closed-source at time of claim
Open-auction clearing fee	At or near zero	Operator dashboards - under token-emission subsidy
Cost cut from one May upgrade	Up to 50%	Operator-reported
The means of production	Roughly $100,000 and 10kW	The base-layer specification's ceiling



The collapse, on a log scale - block-proof latency across the year the speed debate ended. The asterisk is the hardware bill and the security grade.

Read as an economy rather than a chart, the price list resolves into one structural sentence: proving costs are falling like early cloud-compute costs, and being reported like early crypto yields - which is to say, the trend is real and the levels are promotional. The commodity claim's economic core - cheap enough to disappear - is genuinely in sight for the workloads the benchmark measures; what has not appeared is the unsubsidised clearing price that tells a buyer what disappearing costs. The strategic question this report posed of verification in general applies with full force to its cheapest supplier: who has to believe you, and what is their belief worth? A rollup settling billions can already justify proving at almost any of this table's prices. The question the next two years answer is what everyone smaller pays once the emissions stop - and whether the answer still ends in cents once the security grade of the previous chapter is priced in, because bits of soundness, like everything else in this report, are not free.

> The trend is real and the levels are promotional. Proving costs are falling like early cloud compute - and being quoted like early crypto yields.

CHAPTER 09

Who buys a proof

A commodity is defined by its buyers as much as its exchanges, and the demand side of the proving economy in 2026 sorts into four customers with very different willingness to pay. The first and largest is settlement: validity rollups whose entire security model is a proof accepted by the base layer, and whose operators are the marketplaces' anchor tenants - one operator's accounting has a single major chain proving deposits in the billions of dollars through its stack, and the exclusive arrangements now being signed for whole rollup ecosystems show what anchor tenancy looks like in contract form. For this buyer, proving is not a feature but the product's load-bearing wall, and almost any price on this report's list clears. The second buyer is the bridge and the light client - the replacement of committee signatures and multisignature custodianship with a proof anyone can check, and, on the roadmap this desk tracks, full clients of the base layer syncing on a phone from a single verified proof rather than a re-executed history. This buyer pays for trust reduction directly: the alternative line item is not compute but counterparty risk. The third is the institution arriving through compliance - the payments-ledger integration of April and the screened-vault products announced on top of it are the early shape of proofs sold as regulatory furniture, verifying that checks ran without exposing what they checked. And the fourth, smallest and most indicative, is the buyer from outside the industry entirely: the March demonstration in which a proof attested to the existence of a quantum-computing result without

revealing it had no token, no rollup and no chain in its story - it was a company using proof as a communications instrument, which is the demand curve this report's companion volume spent twenty-five pages mapping. The commodity claim's demand-side test is simple to state: the first two buyers already cannot operate without proofs; the market matures when the last two stop being demonstrations. The record says that started this spring.

CHAPTER 10

The verifier’s toolkit

The house rule: a report about a checkable industry must itself be checkable, and this industry is the most publicly instrumented this desk covers. The block-proving race can be audited from a laptop this afternoon: the public benchmark lists proofs per block with latency, cost and size attached, per team, downloadable - the reader is invited to pull one and check the arithmetic behind the sixteen seconds. Proofs themselves verify on commodity hardware in well under a second using published verifiers; checking one requires no belief in anyone. The marketplaces run public dashboards - auction clearing prices, prover counts, stake, deadlines - from which every operator-reported number in the marketplace chapter can be re-derived and watched for the day a fee clears above zero without a subsidy behind it. The soundness chapter's ruler is itself public: the security calculator and its integrations are inspectable, and the promised security columns on the benchmark site are the single most useful thing a reader can watch for in the next quarter. And the desk's proving-benchmark manual compresses to five questions that dispose of most record claims in this field: whose hardware, and what did it cost; which workload; p50 or p99; which security parameters, by whose calculator; and can anyone outside the lab rerun it. This document closes the loop on itself the usual way - the fingerprint on the integrity page recomputes from the canonical text with one line of standard tooling, recipe in Appendix B.

PART FOUR

The Scoreboard

CHAPTER 11

One year on the record

THE RECORD, DATED

DATE	EVENT	WHY IT CARRIES WEIGHT
Jul 2025	The base layer publishes its real-time proving specification - latency, cost, energy, openness, size, security in one definition	The field gets its first complete product description
Sep 2025	The first open proof marketplace reaches mainnet	Proof generation becomes a market, not a service
2025, full year	Block-proof latency falls 16 minutes to 16 seconds; costs fall 45x; millions of proofs generated for production protocols	The performance sprint, corroborated in public
Dec 2025	The foundation declares the performance target met - and pivots the field to soundness: conjectures disproven, advertised bits inflated, a common ruler mandated	The assay office opens; the year's most consequential post
Feb 2026	soundcalc integration deadline for all participating teams	Self-reported security ends, formally
Mar 2026	A major technology company proves the existence of a quantum-computing result inside a zkVM without revealing it	Proving's first mainstream demonstration outside crypto - and a bridge to Report No. 01
Apr 2026	A prover operator ships consumer capture-provenance; another network's verifier lands on a major payments ledger	The proving industry crosses into content credentials and institutional rails
May 2026	A marketplace upgrade cuts proof costs by up to half, operator-reported; the Glamsterdam security gate falls due	Price and grade, same month - one reported loudly, one not yet reported at all
Jul 2026	This report goes to press with no consolidated Glamsterdam scorecard in the public record	The silence this report's first marker exists to end

CHAPTER 12

Twelve months of checkable markers

The markers this publication will score in public, phrased so success and failure are both recognisable. The Glamsterdam tally: which teams met the one-hundred-bit, six-hundred-kilobyte, documented-recursion gate - published by the foundation, the teams, or failing both, by this desk from the public calculator; its continued absence past the next quarter is itself a scored outcome. The H-star gate at year end: 128 provable bits, proofs back under three hundred kilobytes, formal recursion arguments - met, missed, or moved. The benchmark's security columns: live alongside its latency columns, or still promised. The first unsubsidised fee: an open-market proof clearing at a price a buyer actually paid without emissions behind it - the day the Commodity Test's second property closes. The home prover: a documented independent operator proving inside the hundred-thousand-dollar, ten-kilowatt envelope at the specification's latency, or the quiet consolidation of proving into clusters. The neutral cross-vendor benchmark: a workload suite both major zkVM camps accept, ending the seven-times-versus-misleading dispute on shared ground, or another year of duelling blog posts. And the

first mainnet consequence: a base-layer deployment actually gated on the security milestones, which would convert the whole apparatus from roadmap to constraint. Where each lands, the next edition prints it beside what we predicted.

CHAPTER 13

What would change our verdict

The composite verdict below would move toward VERIFIED on two events: the Glamsterdam and H-star gates met on schedule with the tally public - converting the quality grade from contested to enforced - and a sustained period of open-market proofs clearing at real, unsubsidised fees, converting the price from promotional to discovered. It would move toward CONTESTED, or worse, on any of: a further round of conjecture failures cutting compliant systems below their gated bits; a forged proof accepted anywhere in production, which would be this field's category-redefining event; the marketplaces consolidating into single-entity pools behind decentralised branding; or the security milestones slipping into the indefinite futures that performance milestones, in this field, conspicuously did not. Readers with evidence we have weighed wrongly are invited onto the record; the corrections log is part of the report.

CHAPTER 14

The verdicts

The claim under test was that proof is a commodity now - real-time, market-priced, cheap enough to disappear. Against the Commodity Test: the unit is EARLY, the price is CONTESTED, the suppliers are TRACKING, the grade is CONTESTED, and the delivery guarantee is TRACKING. Against the supply chain: real-time proving VERIFIED as benchmark and TRACKING as deployment; the zkVM layer VERIFIED with its comparative benchmarks CONTESTED; the marketplaces EARLY; the hardware TRACKING; the soundness reversal CONTESTED and the year's defining event; the price trend VERIFIED.

The composite is TRACKING, and the sentence-length version of this report is this: in one year the proving economy built the speed, the factories, the exchange floor and the delivery penalties of a real commodity market - everything except the two things a commodity cannot trade without, a price someone actually pays and a grade someone else enforces. Both are now dated line items on the industry's own calendar, which is more than could be said twelve months ago and less than the word "commodity" claims. The proof got fast. The trust is still in escrow - and this report, like the market it grades, will settle on delivery.

APPENDIX A

The claims ledger

Every material claim in this report, with the status The Verifier assigns it and the source that carries it. Statuses: VERIFIED (checked against the primary record), TRACKING (credible, single-sourced or vendor-reported, monitored), CONTESTED (sources genuinely conflict, or the claim is an absence we assert), EARLY (a category-state judgement).

VERIFIED	The Ethereum Foundation's July 2025 real-time proving specification: 99% of mainnet blocks proven within 10 seconds, hardware at roughly $100,000, power within 10kW, fully open source, 128-bit security, proofs at or below 300KB; real-time defined against the 12-second slot minus ~1.5s propagation	Ethereum Foundation north-star definition (Jul 2025); contemporaneous coverage
VERIFIED	On 18 December 2025 the foundation declared the performance target met per EthProofs: block-proof latency down from 16 minutes to 16 seconds, costs down 45x, 99% of blocks proven under 10 seconds on target hardware	Ethereum Foundation, "Shipping an L1 zkEVM #2: The Security Foundations" (18 Dec 2025); EthProofs
VERIFIED	The same post states that several STARK-based systems rely on conjectures researchers have disproven, that advertised 100-bit security may actually be 80 bits, and that a forged proof would permit minting assets and rewriting state	Ethereum Foundation (18 Dec 2025)
VERIFIED	soundcalc integration was mandated for all participating zkEVM teams by end-February 2026 as a common security ruler	Ethereum Foundation (18 Dec 2025)
VERIFIED	The Glamsterdam milestone (end-May 2026) requires at least 100-bit provable security per soundcalc, final proofs at or below 600KB, and a public recursion-architecture account - implicitly treating 100 bits as an interim step back from 128	Ethereum Foundation (18 Dec 2025); analyst coverage noting the walk-back
VERIFIED	The H-star milestone (end-2026) requires 128-bit provable security, proofs at or below 300KB, and formal recursion soundness arguments	Ethereum Foundation (18 Dec 2025); milestone coverage
CONTESTED	As of this report's press date, no consolidated public scorecard of Glamsterdam compliance had appeared in the indexed record five weeks after the deadline - an absence we assert and will correct on evidence	Survey of foundation, team and benchmark publications through early Jul 2026
VERIFIED	EthProofs publishes per-block proofs from competing zkVM teams with cost, latency and size metadata, downloadable and comparable	EthProofs documentation
VERIFIED	The real-time result is an off-chain benchmark on curated hardware and workloads, with an acknowledged gap to independent home operators	Ethereum Foundation framing; analyst coverage (Dec 2025)
VERIFIED	zkVMs execute ordinary programs compiled to RISC-V and emit proofs of faithful execution, removing hand-built circuits as the developer interface	zkVM technical documentation across implementations
VERIFIED	In March 2026 Google generated a zero-knowledge proof using SP1 attesting to the existence of a quantum-computing result without revealing it	Succinct announcement (31 Mar 2026)
CONTESTED	RISC Zero published benchmarks claiming its zkVM at least 7x cheaper than SP1 and up to 60x on small workloads; Succinct replied the comparison misleadingly set CPU against GPU results and cited a ~$0.02, ~2-minute proof from its Hypercube prover, closed-source at the time of the claim	RISC Zero and Succinct public statements; comparative coverage (2025-26)
VERIFIED	Succinct's prover network runs a low-bid auction denominated in a staked token with a base fee plus metered compute, immediate payment, deadlines on the order of ten minutes, and slashing for missed work	Network documentation; independent technical analysis (2025-26)

VERIFIED	Boundless runs a reverse Dutch auction on RISC Zero's zkVM with rewards flowing substantially through a proof-of-verifiable-work points-and-token programme; in the current oversupplied phase direct fees frequently clear at or near zero	Network documentation; comparative prover-network analysis (2025-26)
TRACKING	Succinct reports on the order of 31 active provers and several billion dollars of value secured; it reported more than six million proofs generated across 2025 - operator figures	Succinct site and 2025 recap
TRACKING	Boundless's May 2026 Surge upgrade cut proof costs by up to 50%, with Taiko and Base support added - operator-reported	Boundless announcements (May 2026)
VERIFIED	A RISC Zero verifier was integrated with the XRP Ledger in April 2026, with compliance-screening vault products announced on top	Ecosystem reporting (Apr 2026)
VERIFIED	Succinct launched Zcam in April 2026, an iPhone application signing photos at capture via the Secure Enclave and embedding C2PA content credentials	Launch coverage (23-24 Apr 2026)
TRACKING	Secondary analysis sizes the centralised prover-services market in the tens of millions of dollars, with a small number of providers taking 60-70% of fees and over 90% of validity-proof networks relying on a few proving services - estimates, logged as such	BlockEden analysis (Jan 2026)
TRACKING	Independent analyses of both marketplace designs identify pool formation and single-entity pools behind decentralised branding as the standing concentration risk	Technical critiques of prover-network designs (2025-26)
VERIFIED	Practitioner accounts place number-theoretic transforms at up to 90% of proof-generation latency on GPUs after years of multi-scalar-multiplication optimisation	ZK hardware analyses (2025-26)
VERIFIED	RISC-V is the common instruction set of the major zkVMs and an emerging design substrate for proving accelerators	zkVM documentation; hardware-direction analyses
VERIFIED	Hash-based, post-quantum-oriented proof variants have been demonstrated at low single-digit prover overhead by their developers' measure	VEIL publication via Succinct materials (2025-26)
VERIFIED	An exclusive one-year arrangement delivers SP1-based zkVM proving to Arbitrum chains through August 2026	Partnership coverage (2025-26)
VERIFIED	Base is using SP1-based proving for roughly $7.4 billion in deposits, per the operator's 2025 recap	Succinct 2025 recap
VERIFIED	The cost and latency collapse was achieved substantially on hardware within the specification's $100,000/10kW envelope, per the benchmark's published configurations	EthProofs configurations; foundation accounting
VERIFIED	The base-layer roadmap ties real-time proofs to precompile reuse by rollups and to gas-limit increases with stakers verifying rather than re-executing blocks; full ZK light clients syncing from a single proof are a stated aim	Ethereum Foundation and EthProofs roadmap materials (2025-26)
VERIFIED	The foundation names compact polynomial-commitment schemes (WHIR, JaggedPCS), grinding and structured recursion as a tractable path to the security gates, with recursion documentation itself a deliverable and formal verification to follow once architectures stabilise	Ethereum Foundation (18 Dec 2025)
VERIFIED	Report No. 01 in this series records the state of verifiable AI, including the zkML inference proofs this report's zkVM layer generalises	The Verifier, Report No. 01 (Jul 2026), fingerprint on its integrity page

APPENDIX B

Method and fingerprint

The fingerprint on the integrity page is computed by the house recipe, identical to Report No. 01 and to every article this publication ships. Take the canonical text file published alongside this report (report-02-canonical.txt) - the report's manuscript of record, front matter through Appendix C, structural markers included. Decode any character entities, remove every whitespace character of any kind, convert the result to lower case, and compute the SHA-256 digest of the UTF-8 bytes; the hexadecimal digest must match the fingerprint printed in this document exactly. Any correction produces a new canonical text, a new fingerprint, and a dated entry in the corrections log on the report's page. The fingerprint proves the text you hold is the text we published; the ledger, the sources and the markers are for whether it is true.

APPENDIX C

Sources

Primary and institutional: Ethereum Foundation, real-time proving north-star definition (Jul 2025) and "Shipping an L1 zkEVM #2: The Security Foundations" (18 Dec 2025); soundcalc documentation and integration examples; EthProofs benchmark documentation and per-block data; Glamsterdam and H-star milestone records. Operators and vendors: Succinct - SP1 documentation, prover-network and auction documentation, 2025 recap, Hypercube claims, VEIL materials, Zcam launch (Apr 2026), Google quantum-proof announcement (31 Mar 2026); RISC Zero and Boundless - zkVM documentation, marketplace and proof-of-verifiable-work documentation, Surge upgrade (May 2026), XRPL verifier integration (Apr 2026), comparative benchmark publications. Analysis and secondary: independent prover-network comparative analyses and design critiques (2025-26); BlockEden prover-market analysis (Jan 2026); ZK hardware bottleneck analyses; December 2025 milestone coverage across trade press, including notes on the interim 100-bit walk-back. The Verifier's own reporting drawn on throughout: the base-layer proving beat, "How to Read a Proving Benchmark," "Why the Quantum Debate Flatters STARKs," "The Biggest Rebuild Since the Merge," and Report No. 01, "The State of Verifiable AI."