INFERPROOF ONE

A Time-Bounded On-Chain Certificate of Paid AI Inference

Blue Paper · v1.1

17 August 2026 · Quick AI LLC (Idaho)

https://inferproof.one

https://x.com/inferproofone

https://discord.gg/hbCyrZ2d2A

https://github.com/Quick-AI-LLC/InferProof-One

This document describes the motivation, design, and operational posture of InferProof One (IP1). It is the formal reference for the apparatus. Public-facing rules, privacy practices, and anomaly policy are maintained in the InferProof One repository, on the official site, and are affirmed by this paper. Version 1.1 records the operational hardening of the live stack after a full review of the mAPP and settlement apparatus.

0. Terminology

iT - Inference tokens (prompt + completion).

MiT - One million inference tokens.

IP1*t* - The IP1 token (the on-chain unit). The terminal *t* is set in italic so the token unit is visually distinct from the project name IP1.

IP1 - The project as a whole, used in public and interpersonal reference.

1-YW - The one-year window. The fixed mining period during which paid inference may be certified on-chain under the rules of this paper.

mAPP - InferProof One Mining Application. The web application through which users register, paste management keys, sign to bind wallets, purchase Minecart Sizes, and view post-compilation figures.

publicId - Sequential identifier assigned at registration (#00001, #00002, …). The sole canonical identity spine.

Management key - A non-spendable OpenRouter key capable of reading account-level paid usage. Users generate and paste this key; it is stored encrypted under custody operated by Quick AI LLC.

Minecart Size - A one-time payment that unlocks a fixed daily mining capacity.

Day N / N+1 / N+2 - Usage day (UTC), compilation + review day, and mining-submission day respectively.

Token decimals exist solely for integration compatibility. The lowest representable unit (0.1 IP1*t*) equals 100,000 iT. Mining accruals themselves remain whole IP1*t* only (1 MiT = 1.0 IP1*t*).

1. Origin

In recent years a number of projects have attempted to incorporate artificial-intelligence inference into Proof-of-Work style security models. Notable examples include Pearl, Nockchain, and related efforts. These systems treat inference as a component of chain security: work is performed, proofs are generated, and the resulting security is claimed to underwrite the ledger.

The surface appeal is understandable. Inference is computationally expensive. If that expense can be harnessed to produce cryptographic security, the argument runs, then the same energy that powers useful AI work can simultaneously secure a blockchain. In practice the construction collapses under a more fundamental property of Proof-of-Work itself.

Proof-of-Work, in every serious formulation, reduces to a single question: who controls the most compute. Whether that compute is applied to hash functions, to matrix multiplications, or to any other verifiable function is secondary. The security of the chain is determined by the economic and operational capacity to outpace competing hash power or competing inference capacity. Legal and illegal sources of compute are treated identically by the protocol. The byproduct of the work (hashes, inference outputs, or anything else) does not alter the underlying contest.

Consequently, AI-augmented Proof-of-Work systems inherit the same centralization pressures, the same vulnerability to concentrated capital or compromised hardware, and the same incentive to acquire compute by any means available. The introduction of inference as the work function does not solve these problems; it merely changes the shape of the hardware and the cost curve. With the rapid advance of highly capable models, the marginal security contribution of novel exotic Proof-of-Work constructions has become increasingly difficult to defend. The security model remains, at root, a contest over who can bring the most silicon to bear.

From the standpoint of a heavy user of paid AI inference, such constructions offered little direct benefit. The inference is executed to secure someone else's chain. The person who already paid for the compute receives no durable, portable record of that expenditure. The energy is consumed, the model returns an answer, the payment is settled with the provider, and the economic fact of the expenditure disappears into the provider's internal ledger. No public, verifiable certificate remains.

InferProof One begins from the opposite premise. It discards the security function entirely. The sole purpose of the apparatus is to take energy that has already been expended in paid inference calls and store a verifiable, time-bounded historical receipt of that expenditure on-chain. The token is not an emission schedule, not a consensus mechanism, and not a claim on future work. It is a certificate that real money was spent on real compute under identical rules for every participant, for exactly one year.

At a L1 level, AI PoW invocation turns the product into a type of digital Fluoride. Where Fluoride is the industrial by-product of fertilizer manufacturing, then repurposed and sold to public and private sectors under the guise of dental health, L1 inference mining provides a direct service to an AI user and emits a coin as a by-product of that interaction. The coin is then repackaged and sold to the market as a liquid, tradeable currency. The real economic lever is the LLM-to-user input/output loop. The emitted token is randomly assigned and carries no backing beyond the claim that "some inference was involved." In practice these AI PoW chains are routinely exploited, inference is faked or duplicated, and absolutely none of this is useful.

For example, Pearl executed a soft fork two weeks prior to this writing; attackers of the same nature promptly returned and again controlled more than half the network's hash (200 EH). This forced an emergency hard fork, the second in a month. This hard fork resulted in miners/traders' coins being frozen on the singular PRL exchange, alongside inaccessible coins due to a wallet update delay. Market buyers, miners, the team, and anyone holding the coin sit under serious and ongoing risk of total loss. The security model itself is the attack surface and is unlikely to be hardened to a transactable state.

InferProof One states that all of that is unnecessary. The Fluoride-style PoW coins are a loose and unstable by-product of real economic activity. IP1*t* is a tangible certificate of one million paid AI inference tokens, metered via API under rules that apply identically to every participant. The tokens are never at risk of a 51% rewrite or soft-fork recovery because the mining apparatus is not an open adversarial network. It is a closed system operated under the watch of an incorporated business with automated health jobs, purposeful delays for review, and a deliberate preference for record integrity over continuous mining. This is not decentralization theater; it is certification of paid compute available to anyone.

This thesis, certification of paid compute rather than contribution to chain security, defines every subsequent design choice. There is no attempt to make the inference useful for consensus. There is no claim that the resulting token secures anything. There is only the record.

1.2 Who Mines on IP1

The apparatus is built for people who already pay for inference or who are prepared to do so in the ordinary course of their work. Four overlapping profiles are expected to find the certificate meaningful:

The long-time crypto participant who once mined Proof-of-Work coins or staked/validated in early L1 PoS systems. Many of these participants watched the original permissionless and decentralized ethos dissolve into pure speculation and return-seeking. They understand the physical and economic cost of compute and how stored energy functions in economies. IP1 offers a return to a simple, transparent mapping: real paid energy in, permanent public record out. No hardware farm is required; the "work" is the inference they already purchase and use meaningfully.

Agentic users and builders with only light interest in cryptocurrency. These are people running agents, pipelines, research loops, or production systems against

OpenRouter and similar providers. They already spend meaningful sums on tokens. The certificate gives them a durable, transferable receipt of that expenditure without requiring them to become market makers or protocol engineers.

AI practitioners and enthusiasts who value historical precedence. For this group the attraction is the time-bounded nature of the record itself. One year of paid inference, sealed under identical rules, becomes a primary source for the early period of widespread API-scale inference. The token functions as a collectible certificate of participation in that window.

Crypto participants who have not yet engaged deeply with AI tooling. A significant number of people in crypto circles remain curious about inference but have been deterred by the need for specialized hardware, cost fear porn, or complex local setups. IP1 removes that barrier: the only requirements are an OpenRouter account, a management key, a Base wallet, and ordinary paid usage. No GPUs, no mining rigs, no cluster management.

Speculators are strongly advised to look elsewhere. IP1 is deliberately constructed as a pure historical certificate. There is no emission schedule designed for trading velocity, no protocol-level liquidity, and no official market-centric integrations during the 1-YW. Any discussion of secondary markets, liquidity provisioning, bridges, or additional utility occurs only after the 1-YW closes and only at the discretion of the restricted DAO that inherits governance on day 366. Participants who enter primarily for speculative price action will find the design hostile to that objective. The operator will not facilitate or encourage such activity during the 1-YW.

2. Conceptual Design of the Apparatus

2.1 Identity and Access

Accounts are anchored by a sequential publicId. External OAuth providers (Discord as primary; GitHub and Google as additive methods) resolve to this publicId. Multiple providers may be linked to a single publicId; they never create duplicate identities.

Access to the mAPP is controlled by an HttpOnly signed session established after successful OAuth completion. The publicId is a display label only. It is not a credential and cannot be restored or assumed by typing the number. Loss of OAuth credentials cannot be recovered by the operator.

Linking of a second provider attaches exclusively to the publicId of the current authenticated session. A caller cannot name an arbitrary publicId and attach an OAuth account to it.

Each publicId is bound one-to-one with a Base wallet address. Binding (and any later change) is performed by EIP-191 personal_sign of a one-time server-issued challenge. The server recovers the signer address from the signature and binds that address; any client-supplied address string is ignored. This guarantees the bound wallet is one the user controls and prevents residual authorized accounts from pinning an unintended address.

Signing is available one-click through an injected wallet (desktop extension, or a mobile in-app / dapp browser such as MetaMask Mobile or the Base app). Hardware keys operate when they sign through that wallet. A collapsed fallback path remains: the user copies the challenge message, signs it in a separate environment (for example cast wallet sign or an air-gapped device), and pastes the signature. Ordinary mobile Chrome or Safari without an injected wallet has no native signing path; that is expected.

The first wallet change is free; subsequent changes are subject to a thirty-day timelock. Every bind or change still requires a fresh signature from the new address. The timelock is a fraud-prevention measure that discourages leasing of mining capacity. Miners are encouraged to register with stable access that does not require rotation, as they will encounter friction on swaps.

Management-key writes require the same authenticated session and are scoped to that publicId. Rotation is limited to at most once per twenty-four hours. Address and management-key changes can be facilitated only through the mAPP.

2.2 Metering Source

OpenRouter OAuth or delegated tokens do not expose the per-user paid daily totals required by the design. Metering therefore relies on account-level management keys. Users generate a non-spendable management key on an OpenRouter account (a dedicated, preloaded account with no auto-top-up is the recommended posture) and paste it into the mAPP. The key is stored encrypted under a hardened custody environment operated by Quick AI LLC.

Should other providers enable similar non-spendable administrative keys, the opportunity to integrate a new vendor is possible within the 1-YW. At time of deployment, OpenRouter is the only major inference provider that offers such a service direct to consumer accounts. Anthropic offers an admin metering key to organizations, which precludes them from inclusion as IP1 will not encourage spoofing credentials or account status to acquire a meterable key within the mAPP. Organizations are welcome in IP1, but Anthropic's clear distinction between personal and business accounts for metering key access stands out in comparison to OpenRouter's simple policy. The operator desires to put no miner accounts at risk.

Although management keys cannot initiate inference, they are secured to the same standard applied to spendable credentials: dedicated environment, short-TTL HMAC-tagged reads, separation of duties between read-monitor, oracle, and operational processes, and a documented incident-response playbook. In the event of a confirmed or strongly suspected breach involving stored keys, immediate notice is published on the official website and through official channels. Automated mass alerts are not employed, because the keys are non-spendable.

Live production servers refuse to start without the IP1_ENCRYPTION_SECRET environment variable. There is no public development default on production hosts. Daily compilation uses exclusively the management key stored for that publicId. The operator's own OpenRouter key is never substituted as a fallback; a missing, invalid, or rotated key simply

drops that account's line for the day. Stored keys are never listed or decrypted over the public HTTP surface. Personal account reads of key status require a valid session.

2.3 Conversion and Eligibility

One million paid inference tokens (1 MiT) equals 1.0 IP1*t*. Eligibility is determined by the presence of a USD value in the OpenRouter activity roll. OpenRouter's internal accounting and activity costs are denominated exclusively in USD regardless of the currency used to purchase credits. Rows that carry no USD value are treated as free and are excluded from mining. Because the distinction is made by the provider's own billing signal, the filter cannot be gamed by renaming models or altering slugs; if OpenRouter does not bill the call, no USD value appears and the activity is ineligible.

This approach replaces earlier reliance on the presence of the word "free" in a model name or slug. The USD-value signal is both more accurate and more robust. Soft integrity monitoring remains in place for anomalous patterns, but the primary free/paid boundary is now the provider's own commercial ledger.

2.3b Demo Mining

Every newly registered account receives a one-time cumulative demo allowance of 25 IP1*t*. Demo mining follows the identical settlement path as paid mining. When an account's total mined IP1*t* reaches 25, further mining is blocked until a Minecart Size is purchased. Purchasing a Minecart Size ends the demo; remaining demo headroom is discarded.

Demo mining serves as a proof of concept for prospective miners. The UX of the mAPP is purposefully simple. The registration sequence is OAuth, paste of a management key, then signature to bind the wallet. For users who already hold both a key and a signing wallet the process is rapid. For those without one or both the steps take only a few minutes depending on wallet provider. From the point of onboarding completion miners have to do nothing beyond use inference the way they already do (or desire to). There is no button to press to claim, no need to revisit management keys unless observing normal rotations or responding to an event.

The flow is use inference and receive an on-chain receipt of that spend to a wallet. It is direct.

New miners are allowed to mine their first 25 IP1*t* absolutely free to experience this flow. To take part in the simplicity of it and realize that the paid inference they use can now be stored on Base, the payment layer of agentic finance. If this process resonates with miners in their first 25, then they will certainly enjoy the remainder of the 1-YW.

2.4 Minecart Size and Payment

After the demo, ongoing mining capacity is governed by a one-time payment that unlocks a daily ceiling (Minecart Size). The capacity ladder was recalibrated in August 2026 against observed single-day paid volumes on testnet. Earlier tiers had been derived from smoothed monthly averages; real usage exhibited high day-to-day variance, with individual days reaching 60+ MiT under ordinary (non-loop / non-organizational) loads. The revised

ladder therefore follows a max-day rather than average-day framing so that users who already purchase substantial inference are not artificially capped below their actual paid spend on a day-to-day basis.

USDC	Daily Cap	Label	Approx. Monthly
$9	1 IP1t	Minecart 30	~30 IP1t
$17	5 IP1t	Minecart 150	~150 IP1t
$25	10 IP1t	Minecart 300	~300 IP1t
$54	25 IP1t	Minecart 750	~750 IP1t
$85	50 IP1t	Minecart 1,500	~1,500 IP1t
$139	100 IP1t	Minecart 3,000	~3,000 IP1t

Payments are accepted in USDC (exact tier prices) or native ETH. ETH amounts are fixed at mainnet deployment to a rolling average of the corresponding USDC value and thereafter remain static. The static ETH price ensures that every participant who pays in ETH for a given Minecart Size expends the same quantity of ETH, independent of later price movement. Payment must originate from the currently bound wallet. There are no refunds.

The first successful verification of a treasury transfer assigns that funding wallet to the publicId for credit purposes. A later publicId that binds the same wallet address cannot claim historical treasury inflows belonging to the first. Each confirmed treasury transfer is recorded by its transaction hash and is credited exactly once. Cumulative paid balance on the same publicId unlocks higher tiers; overpayment credits toward the next size. Any amount beyond the highest size is treated as a tip to the operator.

Any paid inference beyond an account's current daily Minecart ceiling is recorded for transparency but produces no additional IP1t that day. The excess difference (metered MiT minus the active daily cap) may be shown in the mAPP as Phantom IP1t (PhIP1t) solely as an informational quantity. Phantom IP1t does not accrue, does not carry forward, does not survive the day boundary, and creates no claim on future mints or on the contract. It is a tool that allows miners to right size their carts via data.

2.5 Daily Settlement Cycle

Usage is measured in UTC days. Day N runs from 00:00:00.000 to 23:59:59.999 UTC. Usage occurring at or after 23:59:01 UTC is attributed to the following day. Day N usage is compiled on Day N+1 at approximately 00:05 UTC. A review window of roughly twenty-three hours and fifty-five minutes follows. The Day N mining batch is submitted at 00:00 UTC on Day N+2.

The compiled figure after review is final. The review period allows miners to reconcile their usage against mAPP reports. If there is a discrepancy they are encouraged to reach out via email, Discord, or X. Legitimate issues highlighted during the review period can and will be addressed. Once the review period closes and the oracle sends the batch to the contract, it becomes immutable.

There are no credit negotiations, retroactive adjustments, or disputes over individual totals. Daily mining submissions may be delayed or an entire day's list may be held or stricken when integrity concerns arise. Unbroken 365-day mining is not guaranteed. Scarcity created by missing or delayed days is accepted by design. The public Anomaly Review Policy communicates the flags operators examine and the expected response for each.

2.6 Integrity Posture

The operator's primary commitment is to the integrity of the historical record, not to the continuity of mining under every circumstance. In the face of exploits, anomalous patterns, or operational issues, the preferred action is to pause, investigate, remove suspect lines, or strike an entire day rather than force a submission that would compromise the certificate's meaning. Downtime is acceptable. The record must remain trustworthy.

The period of launch announcement to mining genesis will allow miners to register and meter their OpenRouter usage through the mAPP. The mAPP will validate real paid inference usage and report the figures on screen the same as if IP1 mining had begun. Yet the days in this period, most likely the last ~10 days of August 2026, will be struck. Miners should expect to see struck days before genesis, as this action prevents the oracle from communicating the daily inference totals to the contract. Post-genesis, struck days happen only in emergencies.

Public documents governing participation (Mining Rules, Privacy Notice, Anomaly Review Policy) are maintained in the root of the InferProof-One repository, on the official site, and are incorporated by reference. Material changes are announced through official channels.

Social media activity such as X posts, advertisements, community announcements, or similar will be focused on the mining apparatus, not secondary market functions of the IP1 token. The goal is to encourage as much mining as possible during the 1-YW and attract as many miners as possible to the community. All IP1 marketing and public communication efforts will be inference-mining centric. The operator may use personally earned IP1*t* as a promotional tool within these endeavors. If the token is used promotionally for growing followers, fostering engagement, or stimulating distribution, it is always implied the IP1 token value is $0 and collectible in nature.

2.6a Operational Hardening

The apparatus enforces the identity, custody, payment, and settlement rules through the following concrete controls.

Contract. IP1 is an OpenZeppelin ERC-20 with AccessControl and Pausable. MINTER_ROLE is granted once, exclusively to the oracle address, and cannot be reassigned. The admin role is renounced at deployment. mintEndTime is immutable. Pause stops minting only; transfers remain live. Revoke is permanent and one-way: it blocks future mints to an address while leaving existing balances untouched. The contract itself imposes no supply or per-address caps; the oracle-submitted list is the sole capacity control.

Oracle key. The oracle private key is generated and held only on the isolated settlement host. It never resides on developer workstations. Because the MINTER_ROLE cannot be rotated on-chain after renouncement, a compromise is answered by pause; the 1-YW then concludes without further minting.

Mint administration. Compile, edit, release, and mint operations require an operator token. The live mint service will not start without it. The public site does not accept a client-supplied admin header. Admin browser access uses a signed, time-limited token rather than a simple flag.

Heavy-day handling. The oracle splits batchMint calls into gas-safe chunks of approximately 250 recipients. Each confirmed chunk is recorded. A retry after partial failure submits only the unconfirmed recipient-amount pairs, so earlier chunks are never re-minted.

OAuth redirects. Discord, GitHub, and Google callbacks are restricted to the official site origin. Attacker-supplied redirect URLs are ignored.

Public visibility. Daily process state (compiled day status, aggregate line totals) remains visible during the integrity window. Personal account mutations, key material, and wallet binding details do not appear on public surfaces.

2.7 Governance Handoff and Sunset

The 1-YW is finite by design. At its conclusion the operator's privileged role ends. Governance and ongoing stewardship of the resulting historical record pass to a restricted decentralized organization formed from the holder set.

The intended sequence is as follows. During the final period of the 1-YW, eligible holders (determined by a transparent snapshot of holdings) may enroll for DAO participation through a congregation zone built into the mAPP itself. No external third-party site is required for enrollment. After the 1-YW closes, Quick AI LLC transfers operational ownership rights (Discord server, domain, and potentially the X account) to the DAO. The operator does not retain privileged governance roles. The founder may participate thereafter solely as an ordinary personal token holder; neither the founder nor Quick AI LLC holds special DAO authority.

The mAPP itself is planned for sunset within approximately six months after mining ends. The domain is retained for a further period (on the order of two years) and is then transferable to a DAO-designated steward. The on-chain record remains permanent and independent of any website or social channel.

This structure is deliberate. During the 1-YW the apparatus prioritizes fairness, integrity, and operational reliability under a single accountable legal entity. After the 1-YW the same entity deliberately withdraws from governance so that the certificate is not permanently tied to any commercial operator. Speculative features, liquidity arrangements, bridges, and additional token utilities (if any) are exclusively the province of the post-window DAO. They are out of scope for the mining period and will not be advanced by the operator.

3. Testnet Validation

As of the date of this paper the apparatus has completed end-to-end smoke testing on testnet, including live metering, automated compilation, review, mining submission, and public Discord summary generation, running autonomously from a dedicated VPS. Real on-chain mints have been executed and verified on Base Sepolia. External tester activity has also been registered without issue. Mainnet-port validation was performed with a disposable burner contract (TEST5) that exercised the same mechanics before any production IP1 deployment. The operational hardening described in section 2.6a is the configuration under which the live mAPP and settlement host now operate.

Exhibit A - First live mint (manual validation)

Usage day 2026-07-30 - compiled, reviewed, released, then batchMint. Transaction 0x1b7bfb9d…0b8a4e (block 45,044,588), status success - 3.0 IP1*t* to the bound miner wallet.

Exhibit B - VPS automated rolls (no human in loop)

Usage day 2026-08-04 - compiled and submitted 2026-08-05 00:14 UTC. Transaction 0x83e2026b…6e95fc (block 45,060,302), status success - 31.0 IP1*t*.

Usage day 2026-08-05 - compiled and submitted 2026-08-06 00:14 UTC. Transaction 0x82f78fa3…f2b5c4 (block 45,103,493), status success - 26.0 IP1*t*.

Each exhibit submits batchMint to the IP1 contract on Base Sepolia, with Transfer and BatchMinted events verified on-chain. These on-chain artifacts convert the conceptual description into an observable, auditable system.

4. Scale Expectations and Emission Outlook

The conservative planning target is approximately one thousand paid registrants over the life of the 1-YW. This figure is deliberately modest relative to Base's daily active users (on the order of two hundred thousand) and is treated as an attainable floor rather than a ceiling.

Emission is a function of three variables: number of active Minecart holders, the distribution of Minecart Sizes purchased, and the fraction of daily capacity actually utilized. Because capacity is hard-capped per account and the 1-YW is fixed, total emission is bounded.

The table below illustrates approximate total emission under three capacity-mix assumptions (entry-heavy, balanced, and heavier-tier) and three utilization rates. Utilization is the share of purchased daily capacity that is actually filled by paid inference. Figures assume 1,000 paid accounts active for the full 1-YW.

Utilization	Entry-heavy mix	Balanced mix	Heavier-tier mix
30%	~0.8M IP1*t*	~1.5M IP1*t*	~2.5M IP1*t*
60%	~1.5M IP1*t*	~3.0M IP1*t*	~5.0M IP1*t*

90%	~2.3M IP1t	~4.5M IP1t	~7.4M IP1t

These bands are illustrative. Actual emission will depend on the final distribution of Minecart Sizes and the real utilization observed across the 1-YW. Growth in Base DAU or attraction of participants from other chains who already purchase inference would increase the number of registrants and therefore absolute emission; the per-account rules and the 1-YW cutoff remain unchanged and scale accordingly.

The theoretical maximum any single entity could mine during the 1-YW is 36,500 IP1t (100 per day × 365). That figure equals 36.5 billion inference tokens spent by that entity. At an illustrative average price of $2.50 per MiT the corresponding inference spend would be approximately $91,250. At a lower average more reflective of heavily discounted open models (around $0.15 per MiT) the same entity would have spent roughly $5,475. In both cases the entity leaves the 1-YW holding 36,500 IP1t against a $139 Minecart purchase at launch. These illustrations underline that the certificate tracks real paid volume; it does not create volume.

Cross-chain attraction is treated as a wildcard. The apparatus itself is chain-agnostic at the metering layer (OpenRouter) and settles only on Base. Any material inflow from users whose primary activity lies elsewhere would appear simply as additional publicIds and additional paid iT, still subject to the same conversion rate and capacity limits.

5. Conclusion

InferProof One is a time-bounded certificate of paid AI inference. It does not secure a chain, does not emit tokens according to an inflation schedule, and does not intermediate billing or inference itself. It records that a given identity expended real money on real compute during a fixed one-year interval, under rules that apply identically to every participant.

The 1-YW limit is deliberate for more than operational reasons. The present period of widespread API-scale inference will, in a decade, be remembered as an early and comparatively crude phase, analogous to the copper-wire dial-up era of the public internet. Those who lived through the modem handshake never forget the sound; later generations find it almost unrecognizable. IP1 exists to encapsulate a slice of that early inference moment under permanent, public, and uniform rules. The certificate is therefore dual-purpose: a practical receipt for users who already pay for inference today, and a primary historical source for future collectors, researchers, and historians seeking to understand what people actually did with paid inference in 2026-2027.

The design choices: non-spendable management keys under custody, daily settlement with an explicit review window, hard capacity limits calibrated to observed max-day volume, acceptance of downtime in preference to a corrupted record, a clean contractual sunset, a hard refusal to advance speculative infrastructure during the 1-YW, plus session-bound identity, signature-proven wallet bind, one-time payment credits, fail-closed mint and encryption, and chunk-safe oracle submission, follow directly from the original premise - store the energy already spent, nothing more. IP1 allows API inference users to store energy they paid for.

The apparatus is developed and hosted by Quick AI LLC, an incorporated business in the State of Idaho. At the conclusion of the 1-YW the operator's role ends. Governance and ongoing stewardship of the resulting record pass to a restricted decentralized organization formed from the holder set. The historical certificate remains.

End of Blue Paper v1.1

https://inferproof.one