Parallax: A Peer-to-Peer Programmable Cash System

Second edition, August 2026

The first edition of this paper was published before mainnet launch and is preserved, unmodified, in the whitepaper repository at editions/first-edition.md. Editions are immutable once published; corrections and revisions appear only as new editions.

Abstract. A purely peer-to-peer form of programmable cash would allow value, and the agreements that govern it, to move directly from one party to another without passing through any institution empowered to refuse. Bitcoin solved the monetary half of this problem: final settlement and absolute scarcity without a trusted third party. Ethereum solved the computational half: arbitrary programs executing against a shared state. Neither solved both. Parallax is the synthesis: Bitcoin's monetary constitution — Proof-of-Work, ten-minute blocks, a supply fixed at 21,000,000 coins on a halving schedule — carrying the full Ethereum Virtual Machine as its execution layer. The network requires no identity, maintains no registry of persons, and contains no mechanism by which a transaction can be privileged or refused. Rules are enforced by independent verification at every node. History is secured by accumulated physical work. Monetary policy is a constant. The network launched on October 28, 2025 with no premine, no insider allocation, and no privileged accounts, and is governed by no one.

1. Introduction

Commerce on the internet depends on financial institutions serving as trusted third parties. The arrangement is usually described as a cost problem: mediation is expensive, disputes are slow, small payments are impractical. But the deeper cost is permission. An intermediary that processes transactions can refuse them. An institution that holds balances can freeze them. An authority that issues money can debase it. Every trusted third party is a point at which value can be surveilled, censored, seized, or inflated away — and given enough time and pressure, it will be. Trusted third parties are security holes [1].

Bitcoin demonstrated that the intermediary can be removed [2]. By anchoring a public ledger to Proof-of-Work, it produced money that no one issues, a history that no one can cheaply rewrite, and a network that no one can be excluded from. Its script was kept deliberately minimal, and that restraint is why it endures. But it also means the agreements built around Bitcoin — credit, exchange, custody, derivatives — settle somewhere else, almost always back inside the intermediated system Bitcoin was built to escape.

Ethereum demonstrated that the ledger can compute [3]. Arbitrary programs, executing identically on every node, can hold and move value under terms no counterparty can breach. But the platform repriced trust rather than removing it: an uncapped supply, monetary rules revised in flight, fee revenue burned by governance decision, and finally the replacement of physical work with Proof-of-Stake — consensus by the permission of capital, in which influence over history is purchased from those who already hold it.

So the two halves of programmable cash have remained apart: money with fixed rules that cannot compute, and computation whose rules will not stay fixed. The ambition itself is old — a community of untraceable pseudonyms paying one another and enforcing their own contracts

without outside help was specified in outline before either chain existed [4] — and it has waited decades for a construction that keeps the money sound while the contracts run. Parallax exists to hold both halves in one system: sound money and a Turing-complete execution layer under a single set of ossified rules, secured by work, owned by no one. What follows describes a network that is running, not one that is proposed. Any claim in this paper can be checked against the chain itself.

2. Design Constraints

Parallax is designed under constraints, not goals. They are stated fully in the Parallax Doctrine [5]; the ones that shape the protocol are these:

- **Physical cost is the only scalable defense against revision.** Any history that can be rewritten cheaply will be rewritten. Consensus must be anchored to a cost that exists outside the system — one that cannot be voted into existence or socially negotiated.
- **Time cannot be compressed without centralization.** Global agreement requires delay. Systems that push finality below what physics allows are smuggling in advantage: proximity, privileged ordering, coordination. Those advantages compound into control.
- **Trust that can be reassigned has not been removed.** Replacing banks with validator sets, or law with governance, relocates trust; it does not eliminate it.
- **Monetary rules must not respond to circumstance.** Flexibility in money is discretion in disguise. Discretion attracts influence, and influence becomes capture.
- **Permission is incompatible with ownership.** Access that can be revoked is not ownership. The protocol therefore grants no access at all; it defines constraints that anyone may satisfy.
- **Systems that depend on cooperation will fail under stress.** Adversarial conditions are the default, not the exception. Security must emerge from constraints that make misbehavior unprofitable, never from an assumption of goodwill.

Every parameter in the sections that follow is a consequence of these constraints.

3. Ownership and Transactions

A coin in Parallax is a balance held under a public key. The state is account-based: each account is identified by a 20-byte address derived from a secp256k1 public key, and ownership is nothing more or less than the ability to produce a valid signature. There is no register of persons behind the addresses and no protocol concept of identity. An address is a claim, not a name.

A transaction is a signed message that transfers value, invokes a contract, or both. Signatures use the same curve, address derivation, and replay protection (EIP-155, chain ID 2110) as Ethereum, so existing key infrastructure — hardware signers included — operates unchanged. Keys are generated privately, at no cost, without registration. Whoever holds the key holds the coin; no other fact about the holder is known to, or can be demanded by, the protocol.

4. The Timechain

To order transactions without a trusted authority, the network maintains a timechain: a chain of blocks in which each block contains the hash of its predecessor, a timestamp, a set of transactions, and a commitment to the state that results from executing them. Each block proves its transactions existed at its point in the sequence, and each subsequent block reinforces every block before it. To alter a transaction buried under N blocks, an attacker must redo the work of those N blocks and outpace the honest network besides. Immutability is not declared; it accumulates.

The target interval between blocks is 600 seconds, and the choice is deliberate. The centralizing pressure in a Proof-of-Work network is set by the ratio of block propagation delay to block interval: the larger the fraction of each interval consumed by propagation, the greater the advantage of miners with superior connectivity, and the stronger the pull toward consolidation in well-connected data centers. At ten minutes, propagation is a negligible fraction of the interval. The advantage of proximity approaches zero, blocks are heavy with accumulated work, and a modest machine on a residential connection verifies the chain as authoritatively as any industrial operation. Time is not a UX feature. It is the cost of certainty.

5. Proof-of-Work

Blocks are valid only when accompanied by a Proof-of-Work in the manner of Hashcash [6]: a nonce n such that

```
XHash(block_header, n) < T
```

where T is the current target. Finding n requires exhaustive search; verifying it requires one evaluation. The longest chain — precisely, the chain embodying the greatest cumulative work — is the truth of the network, and the majority decision over history is expressed one hash at a time, by expenditure no participant can counterfeit.

Work is the only consensus mechanism compatible with the constraints of Section 2. Proof-of-Stake selects block producers by wealth already recorded inside the system it is supposed to secure: the security budget is internal, self-referential, and — because confiscation and reassignment are software operations — negotiable. Work is external. It converts watts into history at a rate no committee can amend, and it admits anyone: no identity, no minimum stake, no institutional recognition. Influence over the chain is earned only through energy spent on it, never through privilege.

The function itself, XHash, is a modified Ethash [7]: memory-hard, so that commodity GPUs mine competitively, and altered precisely so that the existing stock of Ethash ASICs cannot. A Proof-of-Work network is most fragile in its early years, when total hashrate is small; XHash ensures that security in those years is supplied by widely held hardware rather than by whoever owns the residue of another chain's arms race.

6. Difficulty

The target T adjusts every block by the ASERT algorithm (aserti3-2d family [8]): the target is an exponential function of how far the chain is ahead of or behind its ideal schedule,

```
T_next = T_anchor * 2^((t_actual - 600*h) / 172800)
```

where t_{actual} is the time elapsed since the anchor block's parent, h is the number of blocks produced since that same parent, and 172,800 seconds — two days — is the half-life. For every two days the chain drifts behind schedule, difficulty halves; for every two days ahead, it doubles. The response is smooth, per-block, and leaves no window over which a miner can profitably oscillate.

Parallax launched with Bitcoin's 2016-block windowed retarget. Under a severe hashrate decline the window proved manipulable: with block production slowed to a crawl, the retarget lay far in the future, and the interim could be gamed. The network migrated to ASERT at block 17,560, and has held its ten-minute average since. The episode is recorded here deliberately. This paper's first edition described the windowed algorithm; the chain's history records both the flaw and its repair, and the doctrine requires that failure modes be visible, not curated away. A protocol that hides its scars is asking to be trusted. Parallax asks only to be verified.

7. Network

The network is unstructured and open. The steps are Bitcoin's [2]:

1. New transactions are broadcast to all nodes.
2. Each mining node collects transactions into a candidate block.
3. Each mining node works on finding a Proof-of-Work for its block.
4. When a node finds a Proof-of-Work, it broadcasts the block to all nodes.
5. Nodes accept the block only if every transaction in it is valid and every consensus rule is satisfied.
6. Nodes express acceptance by working on the next block atop it.

Nodes may join and leave at will, accepting the greatest-work chain as the record of what happened while they were gone. Peer discovery requires no registration and no gatekeeper; any reachable node is a sufficient entry point to the network, and every node relays. There are no privileged nodes, no coordinators, and no bootstrapping authority whose absence would matter.

The name states the method. A parallax is how astronomers measure what they cannot touch: sight the same object from positions far enough apart, and the truth falls out of the comparison. The network establishes its facts the same way — every node observes the same history from its own vantage and verifies it independently, and what survives every independent measurement, with no observatory in charge, is the only authority the system contains.

Censorship resistance follows from the topology, not from policy. For a transaction to be censored, every miner must refuse it, forever. The protocol offers no assistance: it has no blacklist, no filter, and no field in which an authority could be named — there is nowhere in the system to put a censor. A miner may decline to include a transaction, but its fee then stands as an open bounty payable to the first miner anywhere on earth who defects, and mining is pseudonymous, permissionless entry by design. Exclusion is not a rule the network can adopt; it is a cartel the network makes unprofitable to sustain. The same holds for accounts: no balance can be frozen and no address disabled, because no such operation exists in any node's vocabulary. What the network cannot do, no one can be compelled to make it do.

8. Incentive

Each block, by consensus rule, credits newly issued coins to the miner who produced it. There is no issuing transaction and no issuer at all: the subsidy is a fact of block validity, applied identically by every node. It began at 50 LAX and halves every 210,000 blocks:

```
R(h) = 50 / 2^⌊h / 210000⌋
```

converging on a total supply of 21,000,000 LAX, of which every unit is mined. There was no premine and no allocation; the schedule is the entire monetary history, past and future. These constants do not respond to adoption, to crisis, or to argument. A monetary rule that answers circumstance is a monetary authority under another name, and the network was built to have none.

Transaction fees go to miners in full, by first-price auction. Nothing is burned. Fee revenue is the network's entire security budget once the subsidy has decayed; a protocol that burns fees is purchasing present scarcity with its future defense. As the subsidy falls, the incentive to mine transitions smoothly from new issuance to fees, and remains permanently.

Newly issued coins do not enter the miner's balance until 100 blocks have been built on top of the block that earned them, so the reward is forfeit if that block is orphaned in a reorganization — binding each miner's revenue to the permanence of the chain they extend. The incentive structure encourages the majority to remain honest by arithmetic rather than ethics: a majority attacker

holds hardware and forthcoming rewards whose value depends on the network's integrity, and defrauding it destroys more than it steals. Playing by the rules pays better than breaking them. That, and not goodwill, is the guarantee.

9. Programmability

The execution layer is the Ethereum Virtual Machine, complete through the Paris fork. Contracts written in Solidity or Vyper deploy unmodified; existing tooling operates with a change of chain ID. Programmability is not an amenity layered beside the money — it is the point. Contracts hold, move, and settle the base asset directly, so credit, exchange, and every other instrument historically built atop scarce money can be built here without a custodian, a wrapper, or a peg: agreements that execute exactly as written, against money that cannot be diluted, on a network that cannot be told to stop.

Execution is metered by gas. The block gas limit began at 600 million — roughly one million gas per second, about half of Ethereum's throughput — and adjusts by at most ±0.1% per block. The ceiling is conservative on purpose. Every unit of throughput is paid for in state growth and verification burden, and that cost falls on the full nodes whose independence is the network's substance. A base layer that grows past what commodity hardware can verify has traded its neutrality for volume, whether or not anyone announces the trade.

The base layer exists to settle, not to impress. Throughput, sub-second confirmation, and experimental execution belong in layers built above settlement — rollups and channels that inherit finality from the timechain while keeping their failures out of it. The EVM makes such layers possible; the constraints of Section 2 make them necessary.

10. Privacy

Privacy in an open society requires anonymous transaction systems, and until digital cash, physical cash was the primary such system [9]. The banking system's substitute is privacy by custody: transactions concealed from the world by being disclosed, completely, to the institutions that process them. Parallax follows Bitcoin's inversion: all transactions are public, and privacy is maintained by keeping public keys anonymous. The chain shows that someone moved value; nothing in the protocol connects the keys to persons. No name, document, or approval is ever collected, because there is no one to collect it and nowhere to store it. Pseudonymity is not a service offered to users; it is a property of the protocol, and it cannot be revoked by an operator because there is no operator.

The account model makes address reuse the path of least resistance, and reuse links activity. Users seeking stronger unlinkability should treat addresses as disposable, funding fresh keys for separate activities. Stronger privacy still — and the protocol's neutrality guarantees the option — can be built in contracts above the base layer, which will neither assist surveillance nor perform it.

11. Security

The cost of rewriting history is the cost of redoing its work. An attacker who would replace a transaction buried N blocks deep must regenerate N blocks of Proof-of-Work and overtake a network that has meanwhile moved on. With less than half the network's hashrate, the probability of success decays exponentially in N — the race is a gambler's ruin [2], and Bitcoin's analysis transfers to Parallax unchanged. Six confirmations, about one hour, is the settlement convention, and each of those confirmations embeds ten minutes of the whole network's work: a confirmation here is a unit of settlement, not a transient micro-step.

Even a majority attacker commands less than is commonly supposed. Hashrate can reorder recent history or suppress transactions for as long as the majority is maintained and its expenditure sustained. It cannot forge a signature, move a balance it does not own, mint a coin off schedule, or alter a rule of the system — because every node validates every block, and a block that breaks the rules is not a chain in a losing race; it is noise, rejected regardless of the work behind it. Verification is the ultimate authority in the network, and every participant wields it in full on commodity hardware.

Security is therefore anchored outside the system, in energy — a resource priced by physics, purchasable by anyone, and creditable to no one by decree. Attacks are visible while they occur, expensive for every second they persist, and powerless against the rules themselves.

12. Governance

There is none, and this section exists to say so precisely. Parallax has no foundation, no treasury, no council, no token vote, no roadmap, and no scheduled forks. The original authors hold no keys to the protocol and are required for nothing; the network would not notice their disappearance. Development of client software continues in the open, but consensus rules are intended to ossify: changes are limited to technical repair, and even repair binds no one — a rule change becomes real only through the voluntary adoption of the node operators, one by one, who choose to run it. That is not a governance process. It is the permanent absence of one, and it is a security property: what has no steering wheel cannot be steered, bribed, subpoenaed, or seized.

13. Genesis

The network launched on October 28, 2025, its source code public before launch and its launch date announced in advance, so every participant stood at the same starting line. The genesis block is minimal: no premine, no pre-deployed contracts, no privileged accounts. The supply at block 0 was zero coins — every LAX in existence was mined afterward, under rules that were public before the first hash was tried. Embedded in the genesis extra-data field is a newspaper headline from launch day:

The Times 28/Oct/2025 Trump tells Japan: Any favours you need, we'll be there

proving the chain could not have been constructed in advance of the news. The genesis hash is:

`0x96b239e015d50f5c3f11b80733e5f38c95882c072719507b7be1a59db4975457`

The first 50 LAX were claimed by a public key, not a name, and every coin since has been issued the same way: by work.

14. Conclusion

We have described a system for programmable cash without trusted parties. The money is scarce by constant rather than by policy; the history is immutable by accumulated work rather than by promise; the programs execute exactly as written against the money itself; and there is no party — author, miner, government, or majority — with the power to refuse a transaction, freeze a balance, or amend the supply. The network assumes its participants are adversaries and requires nothing of them but self-interest. It asks for no belief and offers no assurances beyond what any node can check.

The network is running. The code is open. Verification is available to anyone with a commodity machine, and participation to anyone with a key — which is to say, to anyone.

Reality is the arbiter. Cost is the signal. Time is the filter.

Appendix: Constants

Parameter	Value
Consensus	Nakamoto Proof-of-Work (XHash: Ethash-derived, memory-hard)
Target block interval	600 seconds
Difficulty adjustment	aserti3-2d, per block; half-life 172,800 seconds; active since block 17,560
Initial block subsidy	50 LAX
Halving interval	210,000 blocks (about four years)
Supply cap	21,000,000 LAX
Supply at genesis	0
Coinbase maturity	100 blocks
Fees	First-price auction, paid to miners in full; none burned
Execution layer	EVM, complete through the Paris fork
Block gas limit	600,000,000 at launch; adjustable by ±0.1% per block
Signatures	secp256k1; 20-byte addresses; EIP-155 replay protection
Chain ID / Network ID	2110
Genesis	October 28, 2025; hash in Section 13

References

[1] N. Szabo, “Trusted Third Parties Are Security Holes,” 2001.

[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. bitcoin.org/bitcoin.pdf

[3] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” 2014.

[4] W. Dai, “b-money,” 1998.

[5] The Parallax Doctrine: Axioms and Commentary for Durable Settlement, December 2025. github.com/ParallaxProtocol/parallax-doctrine

[6] A. Back, “Hashcash - A Denial of Service Counter-Measure,” 2002.

[7] Ethash specification, Ethereum Foundation, 2015.

[8] freetrader, J. Toomim, C. Culianu, M. Lundeberg, “ASERT Difficulty Adjustment Algorithm (aserti3-2d),” Bitcoin Cash upgrade specification, 2020.

[9] E. Hughes, “A Cypherpunk’s Manifesto,” 1993.