Zycord: Launch, Eras and Parameters

The Simstoshi
2026 — v2.0
GPG: E724 39CE DD85 11F9 D607 550B 87FD 60D5 EB4A 0B29

This document is the companion to *Zycord: A Peer-to-Peer Network of Self-Certifying State Transitions*, v2.0 (“the paper”). The paper defines the mechanisms. This document states how the mainnet was launched, how the coin is issued, which era activates what, and the value of every parameter. It replaces §13 and §14 of the v1.0 paper in full; where they differ, this document governs.

1. Launch

Mainnet genesis: 2026-10-07 00:00 UTC (1791331200), chain id 1.

- Blocks every 30 seconds under proof of work; every 5 seconds from the switch to proof of stake (§6). Proof of work: RandomX v2, CPU-minable. Difficulty: LWMA over a 90-block window.
- Block 0 contains no certificate, no address and no key. No coin exists before block 0. Genesis is reproducible from published sources.
- No investor round and no admin keys. No code path lets any key pause, upgrade, mint, censor or reorganize.

The launch commitment. The parameter set carries a commitment to a secret launch message. Block 1 must open that commitment in its header, so only the holder of the message can produce block 1, and nobody else can accumulate work on a chain that starts before the announced genesis; the issuance ramp makes any head start worth little. From block 2 on, any miner can build.

Chain ids are recorded in a ledger. The ledger, with the genesis id each live network carries, is embedded in every binary and checked at start-up: the node refuses a retired id, and a parameter set that would give a recorded id a different genesis. A node refuses to start with a work engine other than the one the network declares.

2. Issuance

The subsidy decays smoothly to a perpetual tail. The rate is constant within an epoch of one day and steps down at each epoch boundary, by exact integer arithmetic over four constants:

```
E(0) = E0
E(n) = max(tail, E(n−1) − floor(E(n−1) / Q))
```

with E0 = 21 ZCD per block, Q = 1054 and tail = 0.33 ZCD per block, at the proof-of-work interval of 30 seconds. The rate halves about every two years. There are no floats and no table. The genesis block pays no coinbase. The tail begins at epoch 4,376, about year 12, with 61,836,900.03 ZCD scheduled: the 62,744,838.47 the schedule sums to, less the launch ramp and the genesis block. Those figures are whatever the recurrence produces; no node ever computes a closed form. One ZCD is 100,000,000 drops.

A slow start. The first 86,400 blocks (30 days) are a ramp: block h pays `E(30) · h / 86,400`, the rate of the epoch in which the ramp ends, rounded down, so the reward rises in a straight line from near zero to the schedule. What the ramp withholds, about 907,917 ZCD, is never paid back.

The change of interval. From the switch to proof of stake (§6), the epoch is 17,280 slots and the subsidy per block is E(n)/6, rounded down in drops; the recurrence does not change. What a day of full slots pays is the same under both intervals: 21 ZCD per block on the genesis curve equals 3.5 per 5-second block, and the tail of 0.33 equals 0.055. The tail begins at the same epoch, 4,376. The rounding withholds less than a thousandth of a ZCD per epoch and is never paid back.

The tail pays whoever secures the current era without conscripting the fee markets. Against it run the base-fee burn of both markets and the burn of every skipped certificate (paper §9), so net issuance is tail minus burn and can be negative under load. As a fraction of supply the tail tends to zero.

3. Subsidy Split

Every block subsidy is split **94** / **3** / **3** by consensus from block 0. The split applies to the subsidy only, never to fees, and identically to every block. During the proof-of-stake ramp (§6) the producer's 94% is itself divided between miner and drawn staker, by the fraction the ramp has reached.

Share	Recipient	Until
94%	the block's producer, after a maturity of 2 hours (240 blocks under proof of work, 1,440 under proof of stake)	always
3%	the founder's persistent address, credited directly with no maturity	epoch 1,095 (three years)
3%	the treasury cell	always; from epoch 1,095 it also takes the founder's 3%

There is no premine: the split is a rule applied to every block mined, not an allocation at genesis. Over its three years the founder's share sums to less than 2% of the pre-tail supply. A producer that bursts the soft ceiling (paper §9) forfeits from its own share only; the treasury and founder shares are taken from the unreduced subsidy.

4. Treasury

The treasury cell is the native balance of the protocol address. No key hashes to it, no certificate can debit it, and genesis names no quorum. It accrues from block 1, and this release carries no spending path at all. A spending path is defined by an upgrade, not before height 259,200 (about 5 January 2027), with signers chosen by the community and not by the founder. Until then the cell is a public integer anyone can audit and nobody can touch.

5. Stewardship: The First Three Years (proposal)

Status. This section is a direction for community review. Nothing in it is a consensus rule until the treasury upgrade of §4 pins a key set, and the details are specified only after the direction is accepted.

What the treasury receives. About 533,000 ZCD in year 1, 396,000 in year 2 and 280,000 in year 3: about 1.21 million in total. From year 4 it also takes the founder's 3% (§3), for about 396,000 that year in all. What this buys depends on a price nobody knows, and a thin market cannot absorb large sales, so the plan must work at the low end:

ZCD price	Treasury, year 1	One seat (8%)	Infrastructure (20%)
US$ 0.01	US$ 5,300	US$ 430	US$ 1,100
US$ 0.05	US$ 27,000	US$ 2,100	US$ 5,300
US$ 0.50	US$ 267,000	US$ 21,000	US$ 53,000
US$ 20	US$ 10.7 million	US$ 853,000 before the cap	US$ 2.1 million

Every amount below is therefore a share of treasury inflow, never a figure in dollars or in ZCD.

Five seats. The seat is defined before its holder. Each seat has a public charter: its duties, its deliverables, how it reports and what it is paid. Anyone may apply. Whoever holds the seat serves the charter, as under a contract.

Seat	Mandate
Lead developer	The protocol and its releases. First holder: the founder.
Reviewing developer	Independent review of every consensus change.
Miner	An active miner; speaks for block producers.
Community	Channels, documentation, support and onboarding.
Public representative	A publicly identified person; exchanges, partnerships and agreements signed on the project's behalf.

Decisions.

- A spend needs 3 of 5.
- Replacing a holder, rotating keys, spending the reserve or amending a charter needs 4 of 5, and is public for 7 days before it takes effect.
- Terms last one year and are renewable. Candidacies are public for 30 days. The first five holders are the key set pinned by the upgrade node operators adopt; a later hard fork can re-pin it.

Pay is participation, not salary. A seat's share accrues locked and is released every six months, against a published report and the votes of 3 of the other 4 holders. No holder votes on the release of their own pay. What is not released returns to the reserve. Seat pay is fixed by the charters and is not set by a spending vote. A cap per seat, measured at market price on the release date, sends any excess to the reserve.

Budget, as shares of inflow.

Share	Purpose	Rule
40%	the five seats, 8% each	locked, released every six months as above
20%	infrastructure	reimbursed at cost against published receipts
25%	hackathons, events and bounties	by proposal, 3 of 5, paid on delivery
15%	reserve	4 of 5 only

Infrastructure has first claim: nodes, seeds, explorer and build servers cost about US$ 500 per month today. Reimbursement converts at the market price on the day it is paid. The share covers that cost at about US$ 0.06 per ZCD in year 1, US$ 0.08 in year 2 and US$ 0.11 in year 3; below it, the shortfall is carried forward without interest and paid when the share allows.

The founder. The founder's 3% of the subsidy (§3) rewards the work done up to and at launch. It is separate from the lead-developer seat, which is paid like any other seat for ongoing work. The founder holds one key of five and does not vote on the release of that seat's pay.

What consensus enforces. Once the upgrade lands: the 3-of-5 spend and the 4-of-5 rotation with its delay. Everything else in this section is a norm. What enforces a norm is that every spend is an ordinary certificate, public and countable from the chain alone.

Open. The cap per seat. The legal form under which the public representative signs. Whether the six-month lock is enforced by an escrow contract of the standard library once the machine is active.

6. Eras

Eras are height constants compiled into public releases. A block below a gate that carries a program the gate enables is invalid, and that height check is the only thing separating eras, except era 2's ramp and switch, which are triggered by state within height bounds. A new era may add rules and record types; it never changes what an existing block means below its activation height.

Era	Activates at	What exists
0 — Mine and pay	block 0	Proof of work under Nakamoto rules; native assets (paper §5); one-shot and persistent addresses; the two fee markets; the subsidy split; the treasury accruing, sealed
1 — The machine	height 80,640 (28 epochs, about one month)	The cEVM and the standard library (paper §6); contract records with sequencer and admin; intents, fills and co-sequencing (paper §7); the directory; the forced path (paper §8)
2 — Proof of stake	**Bonding:** epoch 182 (height 524,160, 7 April 2027). **Ramp:** active stake ≥ 10% of supply sustained for 30 epochs, at the latest at epoch 273 (7 July 2027). **Switch:** the first block of the epoch after the ramp completes; at the latest epoch 363 (5 October 2027) if the gate never pauses it	BOND, UNBOND and DELEGATE; during the ramp, mined blocks co-signed by the drawn staker; from the switch, 5-second slots produced by stake alone, proof of work retired (paper §11)
S — Confidential payments	after independent audits and an adversarial public testnet	Hidden amounts and one-time addresses

Eras 2 and S each ship as their own release by hard fork, with a specification, an adversarial devnet and review. Era 2 opens bonding by height, starts its ramp by stake with a deadline, and switches when the ramp completes: the earliest the switch can happen is epoch 303 (month 10), and the deadline on the start guarantees the ramp is under way by the end of month 9. For the 10% threshold, stake is active stake with its delegations and supply is the coin issued, both at the opening of the epoch. The gate may pause the switch past epoch 363; what it cannot do is keep it from starting.

Stake. The minimum bond is 1,000 ZCD, and a stake participates one epoch after it is bonded. A bond that only delegates has a smaller minimum, fixed by the era's release, and never leaves the delegator's custody. The minimum is in ZCD and not in dollars because no rule can read a price; it is revised at era boundaries as the block ceiling grows.

Era 0 is deliberately tiny and era 1 is reduced to what the design needs: with no admin keys there is no pause button, so every consensus line is a line that can kill the network without remedy. Unreachable consensus code is unauditable consensus code and is not shipped. An era that does not prove worth its complexity is never triggered.

The transition is tractable because the fold is agnostic to who orders: era 2 changes whose signature is on the header.

Era 1 gate. The gate block writes the era's compiled constants into protocol cells, so the state root commits to them from then on. In the first 240 blocks after the gate, a certificate that runs SETSEQ must carry a TTL at least 240 blocks past the gate and wait for it to come into range.

Era 2 and heights that measure time. After the switch, height advances six times faster. Every genesis constant that is really a duration (the end of the founder's share, the coinbase maturity, the maximum TTL, the intent window, the undo depth, the median-time window, the lifetime of a directory entry) is read by era 2 in the unit it measures: height 3,153,600 is 1,095 epochs of 2,880, and the era ends the founder's share at epoch 1,095. The genesis parameter table does not change, because the consensus root walks every parameter and moving one would move the genesis id of every live network; the era's constants are compiled, like era 1's.

7. Parameters

The parameter set is frozen at genesis, embedded in every binary at compile time, and mutable only by hard fork. Its consensus root enters every signature. `zcd params` prints the compiled values of a build; `zcd genesis` prints the network, chain id, parameter hash, genesis id and state root.

Parameter	Mainnet value
chain id	1
genesis time	1791331200 (2026-10-07 00:00 UTC)
block interval	30 s
epoch	2,880 blocks
work engine	RandomX v2
difficulty window	90 blocks, LWMA
genesis subsidy	21 ZCD
tail subsidy	0.33 ZCD
decay divisor	1054 per epoch
issuance ramp	86,400 blocks
producer / founder / treasury	94% / 3% / 3%
end of founder share	height 3,153,600 (read as epoch 1,095 by era 2)
coinbase maturity	240 blocks
maximum TTL	240 blocks
skip fee	1,000,000 drops
maximum reads / writes / signatures per certificate	64 / 64 / 16
moves per transfer	32
retired addresses per certificate	64
sequential gas target	1,600,000
sequential target cap	5,120,000
parallel gas ratio	3×: parallel target 3T, ceiling 6T
certificates per block	4,000 at genesis
signatures per block	6,000 at genesis
block bytes	2.5 MB at genesis, 8 MB capacity
ceiling growth / decay divisor	512 / 1024
health gate	2% cited competing headers
initial base fee, sequential / parallel	1000 / 10
base-fee step	1/8 per block
citations per block	4
undo depth	1,024 blocks
future time limit	180 s
median-time blocks	11
era 1 (h1_vm)	80,640
height reserved for proof of stake	1,576,800 (frozen at genesis; no rule reads it)

Era 1 constants are compiled, not parameters, because the consensus root walks every parameter and adding one would move the genesis id of every live network.

Constant (era 1)	Value
intent window (TTL − NotBefore)	at most 8 blocks
forced certificates per block	16
forced parallel budget per certificate	4,000 derivation units (200,000 machine gas)
lifetime of a directory entry	259,200 blocks (about 90 days)
signers per fill	at most 16

Era 2 constants are compiled for the same reason.

Constant (era 2)	Value
bonding opens	epoch 182
ramp start	active stake ≥ 10% of supply for 30 epochs; at the latest epoch 273
ramp length	90 epochs that pass the gate; k starts at 1 and rises with each, and the staker's fraction is k/180
ramp gate	90% of the epoch's blocks signed, and active stake ≥ 10% of supply
unsigned block during the ramp	valid; its producer's share of the subsidy and its priority fees are burned; at equal work a signed block wins
slot interval after the switch	5 s
epoch after the switch	17,280 slots
subsidy per block after the switch	E(n)/6, rounded down in drops (3.5 ZCD on the genesis curve; tail 0.055); an empty slot pays nothing
coinbase maturity and maximum TTL after the switch	1,440 blocks; a maturity, TTL or directory expiry height x above the switch height S becomes S + 6·(x − S)
intent window after the switch	at most 48 blocks
median-time blocks after the switch	67
undo depth after the switch	6,144 blocks
lifetime of a directory entry after the switch	1,555,200 blocks
per-block ceilings after the switch	sequential target, its floor and its cap divided by 6, rounded down; the certificate, signature and byte limits follow T as at genesis, their caps divided by 6
forced certificates per block after the switch	2
recommended finality wait	20 blocks before the switch, 120 after (10 minutes)
end of founder share	epoch 1,095
minimum bond	1,000 ZCD
delay between bonding and participating	1 epoch
minimum delegation	open; below the minimum bond
exit delay	open; longer than the undo horizon of the era in force
fraction of a burned bond paid to the reporter	open; below 50%
minimum pool margin	open
draw function and seed source	open