init.ro0t whitepaper

A migration-free, one-sided locked V3 launchpad on HyperEVM with on-chain fee distribution. Condensed English edition of SPEC v0.18.

version	v0.18
date	2026-09-04
network	HyperEVM (chain 999), testnet 998
web	init.ro0t.xyz
docs	init.ro0t.xyz/docs

CONTENTS

ABSTRACT

init is a token launchpad on HyperEVM. Every token is created with a fixed supply of 1,000,000,000, all of which is placed in a one-sided HyperSwap V3 position (1% fee tier) that is locked permanently. There is no migration step: the pool that hosts the first trade hosts every trade after it. Before a token reaches 100 HYPE of net inflow, all trading passes through a gateway contract that charges a 0.25% fee, applies a 60 second anti-sniper surcharge, and tracks bond progress. After bonding the gateway steps aside. Every fee the protocol receives, in WHYPE, is split by immutable percentages between the token's creator, ROOT stakers and the protocol treasury, with no externally owned account in the path. ROOT is the protocol token; staking it receives the stakers' share as a 7 day stream.

1. PROBLEM

Launchpads on HyperEVM and elsewhere share three weaknesses. First, fee claims are unverifiable: "1% of volume" is advertised, but what actually reaches whom is routed through team wallets, manual sweeps and off-chain pipelines. Second, migration: tokens start on a private curve and are moved to a DEX at graduation, a step that has repeatedly been a source of bugs, delays and admin discretion. Third, admin keys: fee rates, recipients and even creator payout addresses are often changeable by a single key.

init's design goal is stated in one sentence in the spec: the differentiator is not exaggerating gross fees, but proving on-chain, without EOA custody, how the WHYPE that the contracts actually received was distributed to creator, staker and treasury.

2. DESIGN

2.1 One pool, forever

Each token's entire supply is minted into a single HyperSwap V3 position covering the price range from P0 (the launch price) to infinity. With all tokens and no HYPE in the position, the pool behaves exactly like a constant-product bonding curve with a virtual reserve of 30 HYPE: price rises as HYPE enters, falls as it leaves. The position NFT is owned by `InitLocker`, a contract with no transfer or decrease function. The starting FDV is 30 HYPE (effective 30.09 HYPE at tick −173,200, aligned to the 1% tier's spacing of 200).

Because the pool is a genuine V3 pool from the first block, bonding requires no migration. The state change at bonding is confined to the token contract and the fee splitter.

2.2 Warm slots

Creating a pool and minting a position costs about 5.6M gas, more than HyperEVM's 3M small block. `InitSlotWarmer` therefore prepares slots in advance in big blocks: clone the token, mint 1B to itself, create and initialise the pool at P0, mint the one-sided position to the locker, and mint a 1e12 wei WHYPE "dust band" just outside P0 that prevents free out-of-range price moves. Clone addresses use a salt of (nonce, warmer, previous blockhash), and pools pre-created by a front-runner in the same block are reused if uninitialised or skipped (at most 32 per transaction). Warming is permissionless and pays a reward of min(0.01 HYPE, gas × basefee × 1.2) while the queue is below its target of 20 to 30 slots. Launch itself then costs about 250k gas.

2.3 The pre-bond gate

Until a token bonds, its transfers are restricted by a pair matrix and an execution context. Allowed: gateway ↔ pool inside a gateway swap, EOA → gateway inside a gateway swap, gateway → EOA, pool → locker during collect, pool → quoter during a quote, EOA → EOA, and burns. Everything else, in particular any transfer where a contract other than the system set is an endpoint, reverts. This blocks router swaps, third-party pools, external LP additions and contract wallets, so that all trading passes through the gateway and bond accounting is complete. The context is stored in transient storage where available. The gate is skipped entirely after BONDED, TIME_UNLOCKED, or 60 days after launch (fallback), so no launched token can ever be stranded.

The token contract has no owner, no mint, no tax and no blacklist. The gateway is exempt from allowances in `transferFrom`, but only for the caller's own tokens, which gives one-click sells without an approval step.

2.4 The gateway

On a buy the gateway wraps the HYPE, pays the surcharge and 0.25% fee to the FeeSplitter, swaps the remainder through SwapRouter02 with itself as recipient, forwards the tokens to the recipient (which must be an EOA), and adds swapInput × 0.99 to bond progress. On a sell it pulls the tokens, swaps to WHYPE, pays

0.25% of the output to the FeeSplitter, subtracts the pool's output from progress, and sends native HYPE to the seller. Balances are checked as deltas against the entry state so that donated tokens cannot brick a launch. Direct buy and sell principal per address is recorded so the front end can show creator activity.

3. FEE MODEL

FEE	RATE	SPLIT C / S / T
Launch	0.02 HYPE	0 / 0 / 100
Gateway (pre-bond buys and sells)	0.25%	35 / 40 / 25
Sniper guard (buys, first 60 s)	4,875 bps × (60 − t) / 60	0 / 60 / 40
Pool, HYPE side (all buys)	1%	50 / 35 / 15
Pool, token side (all sells)	1%	burned

Execution order on a buy is gross → surcharge + gateway → pool 1% → curve. The effective total is 49.51% at t = 0, 25.6% at t = 30 and 1.2475% from t = 60. The guard is always on, applies only to public buys (the creator's atomic opening buy is exempt), does not count toward bond progress, and pays the creator nothing, so a creator cannot profit from sniping their own launch. Simulation shows the guard cuts a 2 second bot's expected profit by 69% when the bot selects tokens with real demand, and moves that money to stakers; a linear guard cannot and does not try to stop a token that triples in minutes.

Creator economics: 50% of pre-bond creator fees are escrowed until bonding, and forfeited to stakers if the token time-unlocks. After bonding, the treasury's 15% of that token's pool fees is redirected to the creator until a cumulative 1 HYPE bonus is paid. The spec forbids quoting "x% of volume" as income: only the HYPE side of pool fees becomes WHYPE; the token side is burned.

The `FeeSplitter` accepts `onFee(token, amount, kind)` only from the fixed caller for each kind (gateway, locker, factory), pulls the WHYPE in the same call, and updates buckets. Outflows (`claimCreator`, `flushStaking`, `flushTreasury`) are permissionless and their recipients are fixed. Invariant: WHYPE balance ≥ Σ creator claimable + escrow + bonus + stakerPending + treasuryPending.

4. CURVE AND BOND

With Y HYPE net in the curve, FDV(Y) = 30 × (1 + Y/30)² and the sold fraction is Y / (30 + Y). The bond target is fixed at 100 net HYPE: FDV 563.3 HYPE (18.8×), 76.9% sold, about 101.26 HYPE gross with no sells. Progress is the gateway's own tally of net inflow, not the position's principal, because a third party can place WHYPE-only liquidity inside the pool that absorbs sells.

When progress first reaches the target, `bondReachedAt` is recorded once and never reset. From 10 minutes later, any gateway trade that finds progress ≥ target bonds the token before executing (`_autoSettle`). The deadline is max(createdAt + 30 days, bondReachedAt + 10 minutes). After it, a trade bonds the token if progress ≥ target, or time-unlocks it if progress has been below target for at least 10 minutes (`lastAboveTargetAt` hysteresis, refreshed also on the sell that drops progress below target, so a sell-and-unlock bundle cannot confiscate a nearly bonded token). Explicit `finalizeBond` and `finalizeOrUnlock` remain as permissionless fallbacks with identical predicates. Both paths collect pre-bond pool fees first so they are split under pre-bond rules.

Bonding releases the escrow, ends the gateway fee and lifts the gate. Time-unlock does the same except that the escrow goes to stakers and no bonus is ever paid. Liquidity, NFT and treasury do not move in either case. A creator can self-bond for a net loss of about 0.9 HYPE, and a flash-loan bundle can force any token to bond for about 4 HYPE of fees; both are accepted because neither is profitable, and the spec calls for the site to label single-transaction bonds.

5. CONTRACTS

```
Ro0tRegistry     version address book (Timelock append only), factoryOf(token)
InitFactory      createToken: pop warm slot, launch, register, 0.02 HYPE → FeeSplitter(LAUNCH),
InitSlotWarmer   clone + mint 1B + createPool + initialize(P0) + one-sided LP → Locker + dust ba
InitToken        EIP-1167 clone, 1B, state machine WARMED → PREBOND → BONDED | TIME_UNLOCKED, t
InitGateway      buy / sell / quote, guard, 0.25%, bond progress, _autoSettle, finalizeBond, fina
InitLocker       holds LP NFTs forever, permissionless collect: WHYPE → FeeSplitter, tokens → b
FeeSplitter      immutable splits, escrow, bonus waterfall, permissionless flush and claim
Ro0tStaking      ROOT stake, WHYPE 7 day stream, pendingPot, bootstrap bonus stream
Ro0tLauncher     one-shot ROOT TGE: token, pool, 650M position → Ro0tLocker, vesting, bootstrap
```

Measured on a mainnet fork (100 runs): createToken p95 250k gas without an opening buy, 521k with one; warm slot p95 5.59M; buy about 230k; sell about 265k. The implementation passed two code-level adversarial rounds with zero Critical, High or Medium findings, and is covered by unit, fork and invariant suites. Deployed addresses are on Contracts.

6. ROOT ECONOMICS

ROOT is a separate fixed-supply token of 1,000,000,000 with no owner. It is not an InitToken, because the 65/15/10/10 allocation cannot be expressed with a token whose entire supply sits in one position.

BUCKET	SHARE	MECHANISM
Fair launch	65%	650M in a one-sided HyperSwap 1% position at FDV0, locked in RoOtLocker; no presale, no gate
Treasury	15%	On-chain vesting, 48 months linear from TGE, no cliff
Team	10%	On-chain vesting, 12 month cliff then 36 months linear
Staking bootstrap	10% cap	emitted = min(cap, k × WHYPE streamed to stakers since TGE); unreleased after 12 months is burned

FDV0 rule. FDV0 = annualised WHYPE streamed to stakers over the 30 to 60 days before TGE ÷ 1.0, that is the fair value for a buyer demanding a 100% yearly yield. Simulated bear-case income (about 1,816 HYPE per year) gives FDV0 ≈ 2,000 HYPE (tick 131,400, effective 1,966). Because the ROOT pool has no gate, launching below fair value hands the discount to launch-block snipers: about 14% of organised inflow if the market settles at 2× FDV0, about 32% at 4×.

k rule. k = 100M ÷ the same annualised income, so that the bootstrap cap is exhausted in exactly 12 months if the pre-TGE trend continues, proportionally less if income falls, and capped if it rises. Reference values: about 55,000 ROOT per WHYPE (bear), 25,400 (base). Zero income means zero emission. Pre-TGE receipts, including the parked pot, are excluded.

Value logic. Staked ROOT receives the staker share of every WHYPE the init contracts actually receive, about 42% blended, streamed over 7 days, plus the WHYPE side of the ROOT pool's own fees. Simulation (v0.15, guard on) gives stakers about 1,816 / 3,932 / 12,428 HYPE per year at 15 / 40 / 120 launches per day; with no guard income, about 46% of that. The spec requires narrative and treasury planning to use the no-guard figures. In the worst simulated combination (bear demand, no guard, 1/6 protocol fee, 30% buys, 30% third-party pre-bond LP) stakers receive about 600 HYPE per year and the fee treasury about 218 ± 33, which is roughly the operating cost floor; below that, operations are funded from the ROOT treasury allocation.

7. GOVERNANCE AND ADMIN

There is no token governance. Two roles exist. The **Guardian** can pause new launches and slot warming immediately and nothing else; existing tokens, trading, claims, collects, unlocks, payouts, liquidity and fees are out of its reach. The **Timelock** is a 3-of-5 multisig with a 48 hour delay; it can append a new version to the registry, unpause, and call the ROOT launcher once. Economics of any deployed version cannot be changed by anyone. Creator payout addresses can be changed only by the current payout. The treasury receives `flushTreasury` and cannot pull from any bucket.

8. RISKS

- Smart-contract risk: no external audit yet; eight internal adversarial rounds and invariant tests do not replace one.
- Income scale: guard-free staker income is tens of HYPE per month in early scenarios; more than half of base-case income depends on buyers paying the guard.
- HyperSwap dependence: the factory owner can enable a protocol fee (1/6 to 1/4) on any pool; post-bond volume can migrate to a lower-fee third-party pool (at 20% share, staker income retains about 91%).
- Pre-bond third-party WHYPE-only liquidity inside the canonical pool cannot be blocked and shares fees on trades through its band.
- Tick-density griefing can push large trades past the small-block gas limit; the front end splits trades.
- Warm queue exhaustion costs an attacker about 0.6 HYPE per 30 slots and affects availability only.
- Vesting sell pressure: 25% of ROOT unlocks over four years against a small market.
- Regulation: a fee-distributing token may be restricted in some jurisdictions. Meme-cycle dependence.

9. PARAMETERS (SPEC §8)

PARAMETER	VALUE
HyperSwap tier	1% (tick spacing 200)
Protocol fee assumption	base 0, stress 1/6 and 1/4
Pre-bond gateway fee	0.25% = C35 / S40 / T25 (total 1.25% with pool)
Pool WHYPE split	C50 / S35 / T15
Pool token-side fee	burned
Guard	always on, 48.75% → 0 over 60 s (effective 49.51% → 1.2475%), C0 / S60 / T40
Bond target	100 net HYPE, fixed
Initial FDV	30 HYPE
Bond bonus	up to 1 HYPE from the token's post-bond treasury share
Bond confirmation	bondReachedAt recorded once; after 10 minutes, progress ≥ target settles at the next trade; deadline max(30 days, +10 min) then finalizeOrUnlock
Pre-bond transfers	contract-counterparty block + pair matrix + execution context
Warm	clone + 1B + createPool (reuse uninitialised, skip ≤ 32) + initialize + LP → Locker + dust band; salt = keccak(nonce, warmer, blockhash(n − 1)); max 4 per tx
Escrow	50% of pre-bond creator fees, until bond or 30 day deadline
Opening buy	≤ 5% of supply
Launch fee	0.02 HYPE
Warm queue	low 20 / high 30, reward min(0.01 HYPE, gas × basefee × 1.2), vault 5 HYPE topped up monthly
createToken gas	target ≤ 0.5M, gate ≤ 1.0M
Time unlock	30 days; token-level fallback 60 days
Staking	WHYPE 7 day stream, pendingPot, min notify 0.05 WHYPE or 1 hour
ROOT	65 / 15 / 10 / 10; treasury 48 m; team 12 m cliff + 36 m; FDV0 = annualised staker WHYPE ÷ 1.0; k = 100M ÷ annualised streamed WHYPE; bootstrap burn after 12 months
Admin	Guardian pause only; 3/5 multisig + 48 h Timelock

10. STATUS AND SEQUENCE

Contracts are implemented in Foundry and deployed on HyperEVM testnet (chain id 998) with a full end-to-end run and an ROOT TGE rehearsal. The sequence to mainnet: internal review (done) → external audit → bug bounty → mainnet deployment of init → 30 to 60 days of live fee data → ROOT TGE with FDV0 and k computed from that data.

> NOTE
>
> This document condenses `docs/SPEC.md` v0.17 (Korean). Where the two differ, the spec and the deployed contracts are authoritative. Nothing here is investment advice.