



Rain Chain

Layer 1 Specification — the chain for outcomes

Date
7 October 2026

Document
RAIN-L1-SPEC-2026-10 v0.2

Classification
Confidential — internal

Document control

Field	Value
Document	RAIN-L1-SPEC-2026-10 v0.2 — Rain Chain Layer 1 Specification
Date	7 October 2026
Status	Draft v0.2 (adds in-play leverage and a burn-and-mint RAIN bridge). Supersedes the Arbitrum Orbit design (RAIN-CHAIN-SPEC v0.1, System Architecture v0.1), which is retained as an evaluated alternative.
Owner	Rain — protocol architecture
Audience	Rain management, investors, core engineers, auditors, validator candidates, market makers
Classification	Confidential — internal

Conventions. Requirements are numbered `AREA-n` and use RFC 2119 keywords: **MUST** (required for the phase named), **SHOULD** (expected unless a written reason exists), **MAY** (optional). Every external fact carries a source URL or is labelled **Assumption** or **TBC**. Throughput and latency figures for Rain Chain are **design targets** until a published load test replaces them. Prices and on-chain reads are point-in-time values taken on 6 October 2026 and move daily.

Verified facts used throughout.

Fact	Value	Source
RAIN total supply (S0)	1,142,408,474,514 RAIN (18 decimals)	<code>eth_call totalSupply()</code> on Arbitrum One, 6 Oct 2026, token 0x2511...099d
RAIN implementation	0x4771...3f0b (ERC-1967 slot read)	<code>eth_getStorageAt</code> on the proxy, same date
Mint / burn · upgradeability	Current implementation has <code>burn(uint256)</code> and <code>burnFrom</code> , no <code>mint</code> . The ERC-1967 proxy is upgradeable by its owner, so a bridge-only mint can be added by upgrade	Bytecode scan; confirmed by Rain, 7 Oct 2026
RAIN price · market cap	\$0.011545 · \$8.19B (implies $\approx 709\text{B}$ RAIN circulating)	api.coingecko.com, id <code>rain</code> , 6 Oct 2026
HL in-block ordering	Non-GTC/IOC actions $\rightarrow$ cancels $\rightarrow$ GTC/IOC actions	hyperliquid.gitbook.io/hyperliquid-docs (Order book)
HL latency / throughput	Median 0.2 s, p99 0.9 s end-to-end; $\approx 200\text{k}$ orders/s	hyperliquid.gitbook.io/hyperliquid-docs (HyperCore overview)
HL nonces	100 highest nonces per signer; window (T - 2 days, T + 1 day)	.../for-developers/api/nonces-and-api-wallets
HL rate limits	1 request per 1 USDC traded, 10,000 initial buffer; cancels <code>min(limit + 100000, 2 * limit)</code>	.../for-developers/api/rate-limits-and-user-limits
HL dead-man switch	<code>scheduleCancel</code> ≥ 5 s ahead, max 10 triggers per day	.../for-developers/api/exchange-endpoint

Fact	Value	Source
HL staking	10k HYPE self-delegation locked 1 year; commission increase only if new $\leq 1\%$; 7-day unstaking; no automatic slashing	.../hypercore/staking
HL bridge	Validators sign withdrawals; pending withdrawal disputable for a period; lockers can lock, cold-wallet quorum unlocks	github.com/hyperliquid-dex/contracts/blob/master/Bridge2.sol
HL outcomes (HIP-4)	YES and NO books merged: buy YES at $p \equiv$ sell NO at $1 - p$	.../hip-4-outcome-markets
Consensus libraries	Malachite — circlefin/malachite , Apache-2.0, v0.8.1, active; Commonware — commonwarexyz/monorepo , Apache-2.0, release v2026.9.0, active; CometBFT — Apache-2.0 (Go)	api.github.com/repos/..., 6 Oct 2026

1 Executive summary

Rain Chain is a purpose-built Layer 1 for **outcomes**: prediction markets first, then sports exchanges, short-dated up/down options, parametric insurance, lotteries, casino games and AI trading agents. It follows the Hyperliquid pattern: one Rust node binary runs a native trading state machine (**RainCore**) and a general-purpose EVM (**RainEVM**) in the same blocks, finalised by a pipelined BFT consensus in about 200 ms.

Why an L1 and not an L2. An Orbit rollup was specified and evaluated (superseded documents). It inherits Ethereum security for funds, but sequencer-ordered EVM execution cannot match a native matching engine for latency, cancel priority, gasless trading or validator-enforced ordering. Rain chose performance and sovereignty; this document takes that choice and makes its main cost — the bridge and validator security — the most carefully specified part.

What it delivers in v1 (mainnet beta).

- On-chain central limit order books for binary and multi-outcome markets, mint-on-match, gasless trading, MM-grade tooling (batching, dead-man switch, agent keys, 100-nonce set), consensus-enforced cancel priority.
- Native resolution (Olympus AI → Lex AI → oracle vote) with RAIN-bonded disputes and automatic settlement.
- **Conservative leverage**: isolated, long-only margin on outcome shares, 2× at launch rising to 5×, funded by a lending vault, with a four-step liquidation waterfall.
- **Native randomness beacon** (threshold BLS) exposed to RainEVM, so casino and lottery operators can build without Rain being the operator.
- RainEVM with gas in RAIN, EIP-1559 base-fee burn, open ERC-20 creation.
- 7 genesis validators, growing to 26 by stake, with a 10% voting-power cap, slashing and a lockbox bridge to Arbitrum One.

Token in one line. 10% of S0 (114.2B RAIN) is released to stakers over 8 years; protocol inflation is 0.5% per year in years 1–4 and 1.0% from year 5, permanently; 35% of protocol trading fees buy and burn RAIN and all RainEVM base fees burn. Year-1 net inflation is 0.18–0.50% depending on volume (Table T3).

Key numbers.

Parameter	v1 value
Block time · finality	200 ms target · single-slot (one block)
End-to-end latency	p50 ≤ 300 ms, p99 ≤ 1 s (co-located, target)
Throughput	≥ 20,000 order actions/s sustained on commodity bare metal (target; publish only after load test)
Validators	7 at genesis (f = 2), active set up to 26, top-by-stake, 10% power cap
Min self-bond	25M RAIN (≈ \$289k), locked 1 year
Unbonding	21 days
Commission	5%–20%, increase ≤ 1 pp per 7 days
Trading fee	20 bps taker, 0 bps maker (+ builder fee ≤ 50 bps)
Leverage	2× at launch, 5× ceiling in v1
Bridge withdrawals	≥ 2/3 stake signatures; 3 min to 24 h delay by size; hourly outflow cap
Budget	≈ 9–11 months to stable mainnet; audits \$0.6–1.0M (assumption)

2 Scope, goals and non-goals

2.1 Goals

1. **G1 Performance.** Hyperliquid-class: 200 ms blocks, sub-second p99, a matching engine that is the chain, not a contract on it.
2. **G2 Outcome-native.** Every primitive an outcome business needs — books, complete sets, resolution, randomness, settlement, builder fees — lives in the protocol.
3. **G3 Safe leverage.** Leverage ships in v1 with bounded losses, explicit eligibility and kill switches.
4. **G4 Credible decentralisation.** An open, stake-competitive validator set that cannot be captured by buying seats.
5. **G5 Continuity.** RAIN and stablecoins move from Arbitrum One through a rate-limited lockbox bridge; the existing Rain app and SDK migrate.
6. **G6 Infrastructure stance.** Rain provides infrastructure; operators and front ends own licensing, KYC and geo-blocking.

2.2 Non-goals for v1

- Perpetual futures on external assets; cross-margin and portfolio margin.
- Leverage above 5×; the 10–100× in the product roadmap is explicitly deferred (\$9.9).
- Permissionless market creation (Phase 3), spot-token listings on RainCore (Phase 3).
- A Rain-operated memecoin launchpad (not in year 1) and Rain-operated casino games.
- Native issuance of a Rain stablecoin on Rain Chain (USDR may be bridged later once audited).

3 System overview

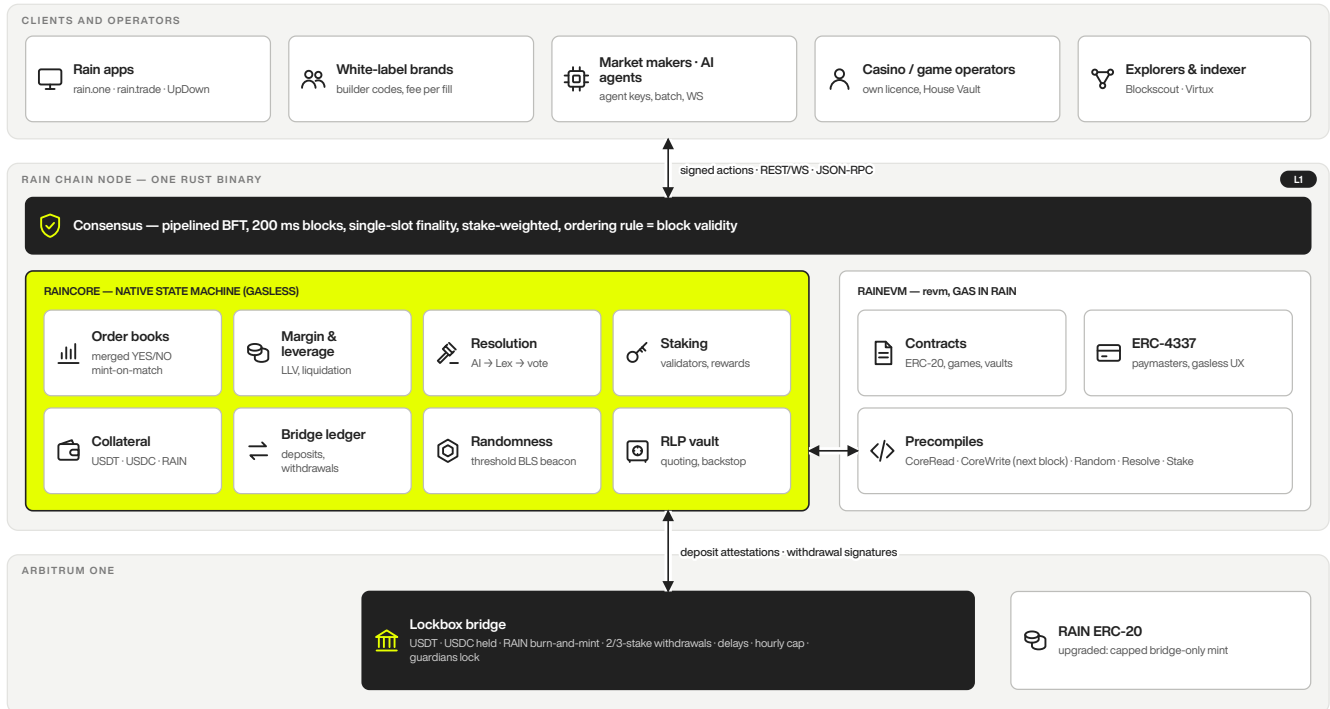


Figure 1. Rain Chain system overview. One node binary runs consensus, RainCore and RainEVM; the bridge contract on Arbitrum One is the only place user funds sit outside Rain Chain.

3.1 Components

Component	Responsibility	Language / basis
Consensus	Pipelined BFT, single-slot finality, stake-weighted voting, block validity rules (including ordering)	Rust; Malachite or Commonware (Phase-0 spike), CometBFT fallback
RainCore	Native state machine: accounts, collateral, order books, matching, outcome tokens, margin and liquidation, resolution, staking, bridge accounting, randomness beacon	Rust, integer-only, deterministic; reuses Rain CLOB engine concepts
RainEVM	General EVM in the same block; gas in RAIN; precompiles for RainCore reads and queued writes	Rust, <code>revm</code>
Bridge	Lockbox contract on Arbitrum One for USDT, USDC and RAIN; validator-signed withdrawals	Solidity (Rain Solidity team)
Node services	Mempool, gossip, API (REST/WS), state sync, snapshots	Rust
Explorers	Blockscout for RainEVM; RainCore explorer (markets, books, fills, validators, bridge)	Blockscout; Virtux
Apps	rain.one, rain.trade, UpDown, white-label brands, SDK, MM and agent clients	Existing stack, migrated

3.2 Design principles

- **ARCH-1** The node **MUST** be a single binary in which consensus, RainCore and RainEVM share one state root per block.
- **ARCH-2** RainCore **MUST** use integer arithmetic only (no floating point anywhere in state transition), fixed-width big-endian canonical encoding and a domain-tagged SHA-256 state hash per module, as in the existing engine (`state_hash.rs` , tag `RAINB00Kv1`).
- **ARCH-3** Any honest node replaying the block log from genesis **MUST** reproduce every state hash bit-for-bit.
- **ARCH-4** Trading on RainCore **MUST** be gasless; spam is bounded by volume-based rate limits (§7.6).
- **ARCH-5** Protocol-level ordering rules **MUST** be block-validity rules checked by every validator, not proposer goodwill.

4 Consensus and networking

4.1 Engine selection

Criterion	Malachite (<code>circlefin/malachite</code>)	Commonware (<code>commonwarexyz/monorepo</code>)	CometBFT (fallback)
Licence	Apache-2.0 (verified)	Apache-2.0 (verified)	Apache-2.0 (verified)
Language	Rust	Rust	Go (ABCI++ boundary)
Algorithm	Tendermint-family, formally specified	Simplex-family primitives, BLS threshold tooling	Tendermint
Maturity	v0.8.1, active (6 Oct 2026); note <code>informalsystems/malachite</code> is now a fork, upstream is Circle	Release v2026.9.0, active	Production in many chains
Fit	Embeds as a library; Tendermint semantics well understood	Library-of-primitives; native threshold crypto helps the beacon	Proven, but adds IPC hop and ~1 s typical blocks

Decision. Phase 0 runs a two-week spike on both Rust candidates with the same harness (4 and 7 nodes, 3 regions, 200 ms target, adversarial delay). Selection criteria, in order: safety evidence (formal spec, audits), p99 finality at 7 nodes across regions, ease of embedding the ordering rule and vote extensions (for beacon shares and bridge signatures), and maintenance health. CometBFT is the fallback only if both fail; its use would relax the block target to 500 ms.

4.2 Requirements

- **CONS-1** Block time target **MUST** be 200 ms under normal conditions with 7–26 validators in at most 3 continents; p99 time-to-finality **MUST** be ≤ 600 ms in Phase 2 testing (target).
- **CONS-2** Finality **MUST** be deterministic and single-slot: a block with commit signatures from $> 2/3$ of voting power is final and **MUST NOT** be reverted except by social-layer recovery (§12.6).
- **CONS-3** Voting power **MUST** be stake-weighted, with each validator's counted power capped at 10% of total counted power (§12.3).
- **CONS-4** The proposer **SHOULD** rotate weighted by power. Vote extensions **MUST** carry the validator's randomness beacon share and any pending bridge-withdrawal signatures.
- **CONS-5** Execution **MUST** be pipelined: consensus on block $h+1$ proceeds while block h executes; the state root of h is committed in $h+1$ (or $h+2$ — fixed by the spike).
- **CONS-6** Validators **MUST** sit behind sentry nodes; validator IPs **SHOULD NOT** be public.

4.3 Why 7 validators at genesis

BFT tolerates f faulty validators among $n \geq 3f + 1$. $n = 4$ tolerates one fault, which leaves no margin during a planned upgrade or a single datacentre outage. **$n = 7$ gives $f = 2$** : the chain survives one validator down for maintenance plus one malicious or failed validator at the same time. A minimum of 5 still only tolerates $f = 1$ ($5 \geq 3 \cdot 1 + 1$), so it buys little over 4. Seven is therefore the smallest number with real operational margin, and it remains cheap to coordinate during beta. The protocol **MUST** refuse to produce blocks with fewer than 5 active validators (halt-safe floor) and **SHOULD** operate with ≥ 7 .

5 Block pipeline and ordering

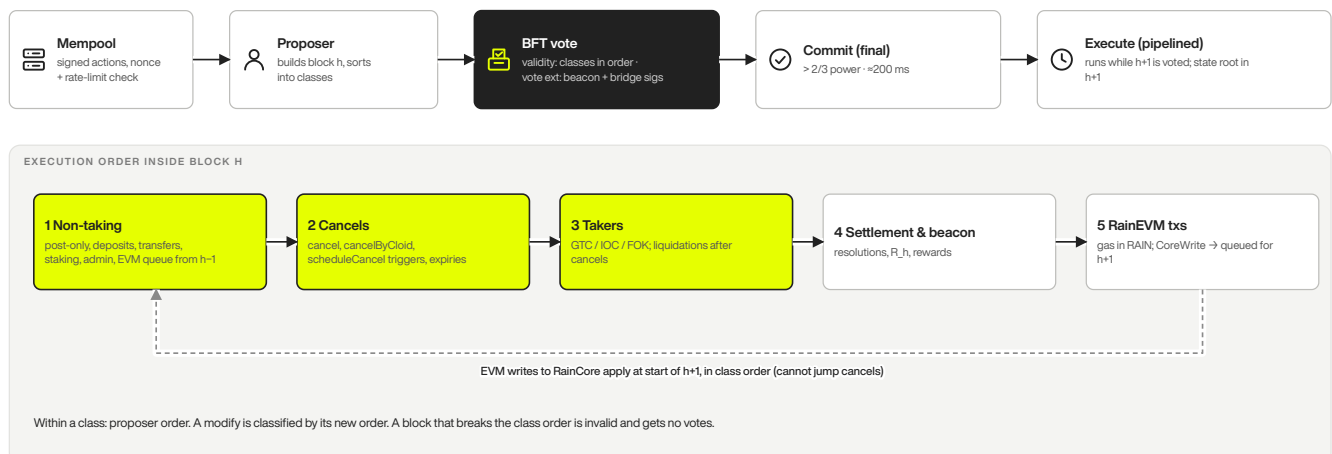


Figure 2. Block pipeline. Validity includes the three-class ordering rule; RainCore executes before RainEVM, and EVM writes to RainCore are applied at the start of the next block.

5.1 In-block ordering (consensus rule)

- **ORD-1** Within each block, RainCore actions **MUST** be sorted into three classes and executed in this order: (1) actions that place no GTC or IOC taker order — post-only (ALO) orders, deposits, transfers, staking, admin and oracle actions; (2) cancels (by order id or cloid, including `scheduleCancel` triggers and expiries); (3) actions that place at least one GTC, IOC or FOK order. Within a class the proposer's order is kept. A modify is classified by the new order it places. This mirrors Hyperliquid's published rule.
- **ORD-2** A block whose actions violate ORD-1 **MUST** be rejected by every validator (prevote nil).
- **ORD-3** RainEVM transactions **MUST** execute after all RainCore actions in the block. EVM-originated RainCore writes (via precompile) **MUST** be queued and applied in class order at the start of block $h+1$, so EVM contracts cannot jump the cancel queue.
- **ORD-4** The proposer **MUST NOT** reorder within a class by price or by sender; deviation from first-seen mempool order is detectable but not provable, so it is handled by monitoring and social slashing (risk R-7), not consensus. A future upgrade **MAY** add encrypted mempool or batch auctions per block.

Rationale. Classes 1 and 2 before class 3 mean a market maker who quotes and cancels is never picked off within a block by a taker that arrived in the same block. This is the single most important property for tight spreads on news-driven outcome markets.

5.2 Halts and restarts

- **ORD-5** After any chain halt, global trading pause or market pause, the affected markets **MUST** enter a **post-only window** of 10 blocks (≈ 2 s) in which only class-1 and class-2 actions are accepted, letting makers refresh quotes before takers return.
- **ORD-6** Market-level circuit breakers (§8.7) **MUST** use the same post-only reopening.

6 RainCore — accounts, collateral and the order book

6.1 Accounts and signing

- **ACC-1** Accounts are secp256k1 addresses (EVM-compatible), so the same key controls RainCore and RainEVM balances. RainCore actions are EIP-712 typed messages, not EVM transactions.
- **ACC-2 Agent keys:** a master account **MAY** authorise up to 10 named agent keys with scopes `trade` (place, modify, cancel) or `cancel-only`, with an expiry ≤ 180 days. Agent keys **MUST NOT** withdraw, transfer, change agents or alter staking.
- **ACC-3 Nonces:** each signer keeps the 100 highest used nonces. A new action's nonce **MUST** be greater than the smallest in the set, unused, and within $(T - 2 \text{ days}, T + 1 \text{ day})$ of block time in ms. Agent-key nonce state **MUST NOT** be pruned while the agent is registered; re-registration of a pruned agent address **MUST** be rejected (avoids the replay hazard Hyperliquid documents).
- **ACC-4 Sub-accounts:** up to 20 per master, each isolated for margin.

6.2 Collateral assets

Asset	Source	Use in v1
USDT (USD₯0 on Arbitrum One)	Lockbox bridge	Settlement and margin
USDC (native on Arbitrum One)	Lockbox bridge	Settlement and margin
RAIN	Lockbox bridge (native on Rain Chain)	Gas, staking, bonds, settlement token for RAIN-denominated markets; not margin for leverage in v1

- **COL-1** Each market **MUST** settle in exactly one quote asset. USDT and USDC are separate quote assets (no implicit 1:1 assumption); a market **MAY** be listed in both.
- **COL-2** All balances are stored as `u128` in the asset's smallest unit; outcome prices use a 6-decimal fixed-point scale (1.000000 = full payout).

6.3 Market model — one book per outcome

Decision: a single merged book per binary outcome, expressed in YES price. An order to buy NO at q is stored as a sell of YES at $1 - q$ on the same book. Rationale: liquidity is not split across two books, a single price-time queue removes cross-book arbitrage, and the existing engine already implements a single two-sided book. Hyperliquid's HIP-4 chose the same merged model.

Matching then has three execution paths, chosen automatically by what each side holds:

Taker	Maker	Execution
Buy YES (has quote)	Sell YES (holds YES)	Transfer YES and quote (ordinary trade)
Buy YES (has quote)	Buy NO, i.e. "sell YES" without YES (has quote)	Mint-on-match: taker pays p , maker pays $1 - p$, protocol mints one YES + one NO from the 1.00 collateral
Sell YES (holds YES)	Sell NO (holds NO), i.e. a NO holder's "buy YES"	Burn-on-match: YES holder receives p , NO holder receives $1 - p$; the pair is merged and 1.00 collateral released

- **BOOK-1** Mint-on-match and burn-on-match **MUST** be atomic within the fill; the invariant `quote locked in market = outstanding complete sets × 1.00` **MUST** hold after every action and be part of the market's state hash.
- **BOOK-2** Price-side-time priority: at equal merged price, resting holders' sells **SHOULD** queue ahead of dual (mint) orders, as in HIP-4, because they release rather than lock collateral.
- **BOOK-3** Order types: limit GTC, IOC, FOK, post-only (ALO), market (IOC/FOK only), reduce-only flag, GTD (expiry timestamp) and `expiresAfter` (action rejected if included after this time). All exist in the current engine except GTD/expiresAfter, which are added.
- **BOOK-4** Self-trade prevention per order: `CancelNewest` (chain default), `CancelOldest`, `Decrement` — exactly as `StpPolicy` in `types.rs`.
- **BOOK-5** Client order id: 128-bit `cloid`, unique per account among open orders.
- **BOOK-6** Batch actions: up to 50 place/cancel/modify operations per signed action, executed atomically per operation (not all-or-nothing) and counted as `n` requests for rate limiting.
- **BOOK-7** Dead-man switch: `scheduleCancel(t)` with $t \geq 5$ s in the future; max 10 triggers per UTC day per account.
- **BOOK-8** Limits: max 1,000 open orders per account per market (raised by volume tier), min order notional \$1.

6.4 Tick size

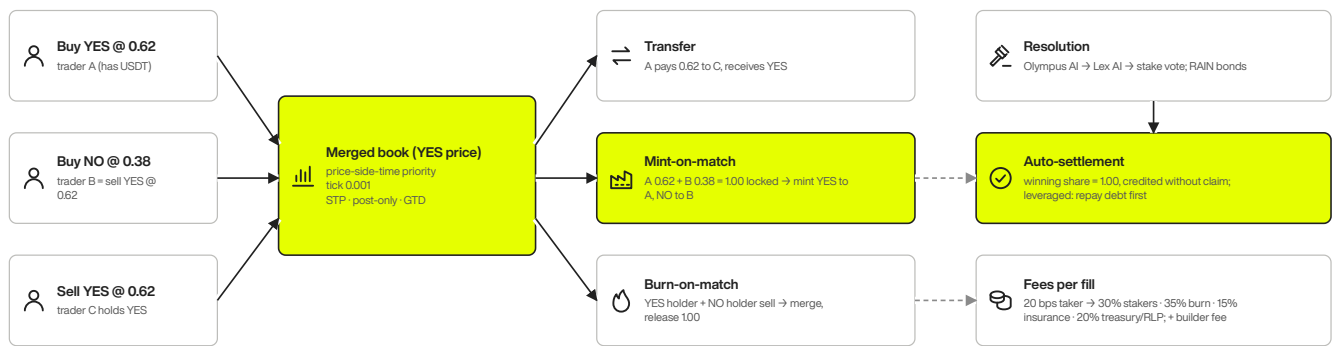
Decision: tick 0.001 (0.1¢) over the range 0.001–0.999, with a market-level option of 0.01. Rationale: outcome markets routinely trade at 1–3¢ and 97–99¢, where a 1¢ tick is a 30–100% relative spread; 0.1¢ lets makers quote tight tails and is cheap for a native book. Markets where the book is thin **MAY** be listed with 0.01 to concentrate liquidity; the tick is fixed at listing and changes only via governance with 24 h notice.

6.5 Multi-outcome markets

- **MULTI-1** A multi-outcome market groups `N` binary outcomes ($N \leq 64$) with the constraint that exactly one resolves YES.
- **MULTI-2 Conversion (negRisk-style):** a holder of NO on `k` outcomes **MAY** convert it into $(k - 1)$ units of quote plus YES on each of the other $N - k$ outcomes, atomically. This keeps prices across outcomes arbitrage-consistent without a single `N`-way book.
- **MULTI-3** A "basket mint" of one YES on every outcome costs exactly 1.00 and **MAY** be merged back.

6.6 Fees and builder codes

- **FEE-1** Protocol fee: **20 bps taker, 0 bps maker** on notional ($\text{price} \times \text{size}$) at launch; volume tiers **MAY** reduce taker fees to 10 bps and introduce maker rebates paid only from fee revenue.
- **FEE-2 Builder codes:** an order **MAY** name a registered builder and a builder fee ≤ 50 bps (approved by the user once per builder, revocable). The builder fee is paid on top of the protocol fee directly to the builder's account in the quote asset, per fill.
- **FEE-3** Protocol fee split (per fill, in quote asset): **30% stakers** (distributed per epoch in quote asset), **35% buy-and-burn RAIN** (executed on the RAIN/USDT book via TWAP), **15% insurance fund, 20% treasury / RLP**.



Invariant (every action, in state hash): quote collateral locked in a market = outstanding complete sets × 1.00

Figure 3. Order to settlement. Orders enter the merged book; a match either transfers shares, mints a complete set, or merges one; resolution pays winning shares automatically.

7 Resolution, settlement and liquidity

7.1 Native resolution module

The current Rain flow (Rain System Architecture v1.2 §3.5) moves into RainCore as a native module:

Tier	Who decides	Window	Bond (RAIN, v1)
1 Proposal	Olympus AI resolver key posts outcome	60 min	Resolver bond for non-resolver closers: 0.1% of market open interest, min 50k RAIN, max 2M RAIN
2 Dispute	Lex AI judge key re-decides	60 min	Dispute bond 0.1% of OI, clamped 20k–2M RAIN
3 Appeal	On-chain oracle vote by staked RAIN holders who opt in (quorum 5% of bonded stake, 24 h)	24 h	Appeal bond 0.2% of OI, clamped 50k–5M RAIN

- **RES-1 Bonds MUST** be in RAIN; the losing side's bond is split 50% to the winning challenger, 50% burned.
- **RES-2 Change from Arbitrum flow:** tier-3 voting **MUST** be open to any staker who opts in, weighted by stake, with a 1-day commit and 1-day reveal; voters on the minority side lose 1% of voted stake (to align with the truthful majority). This replaces the mostly-internal voter set.
- **RES-3** Resolver keys (tier 1, 2) **MUST** be governance-rotatable in one action for all markets; they **SHOULD** be held in HSM/KMS.
- **RES-4 Auto-settlement:** at finality of the outcome, RainCore **MUST** convert every winning share to 1.00 quote (and losing to 0) in the holder's balance without a claim transaction; open orders in the market are cancelled first. Settlement of very large markets **MAY** be spread over ≤ 20 blocks with a deterministic cursor.
- **RES-5** Settlement fees (creator, resolver shares) are snapshot at resolution, capped at 20% each and $< 100\%$ total, as today.
- **RES-6** Markets whose resolution source is unavailable **MUST** remain tradable (book open) until resolved; there is no forced fallback outcome on Rain Chain (the Arbitrum "last option" fallback is removed).

7.2 Market creation

- **MKT-1** Phase 2: markets are created by the Foundation and approved partners through a governance-controlled listing role.
- **MKT-2** Phase 3: permissionless creation with a 500k RAIN creation bond (refunded at clean resolution, slashed if the market is voided for being ambiguous) and a Dutch-auction slot fee if listings are congested.

7.3 RLP — Rain Liquidity Provider vault

- **RLP-1** A protocol vault (HLP-style) **MUST** exist, holding USDT/USDC from depositors, with strategies: (a) quote new markets with a capped two-sided book for their first 72 h, (b) backstop liquidations (§9.6), (c) supply idle balance to the Leverage Lending Vault up to 30% of RLP.
- **RLP-2** Deposits have a 4-day lock-up; RLP receives the 20% treasury/RLP fee share (split 50/50 RLP/treasury) plus its strategy PnL.
- **RLP-3** Per-market RLP inventory is capped at 2% of RLP equity; RLP **MUST** quote in post-only mode only.

7.4 Rate limits (gasless trading)

- **RL-1** Each address receives **10,000 requests initial buffer** plus **1 request per 1 USD of filled volume** cumulatively; rate-limited addresses get 1 request per 10 s.
- **RL-2** Cancels **MUST** have limit `min(limit + 100,000, 2 × limit)`.
- **RL-3** Under congestion, block space per address **MAY** be capped at 2× its previous-day maker share.
- **RL-4** Agent keys share the master's budget. Accounts with < \$10 collateral **MUST** be limited to 100 open orders total.

8 RainEVM

- **EVM-1** RainEVM **MUST** be an EVM equivalent (Cancun-level opcodes, `revm`), chain id TBC, executing in the same block after RainCore.
- **EVM-2** Gas is paid in RAIN with EIP-1559: base fee **burned**, priority fee to the proposer. Block gas target 15M, limit 30M per 200 ms block (target; tuned in Phase 1).
- **EVM-3** ERC-4337 EntryPoint and paymasters **MUST** be deployed at genesis so apps can sponsor gas or charge in USDT. Rain's existing account-abstraction SDK migrates.
- **EVM-4** ERC-20 creation is open. Rain **MUST NOT** operate a token launchpad in year 1.
- **EVM-5 Precompiles** (addresses TBC):

Precompile	Function	Notes
CoreRead	Balances, positions, book top-N, mark price, market status	Reads state at start of current block
CoreWrite	Place/cancel orders, transfer to/from RainCore, open/close leverage	Queued, applied in block h+1 in class order (ORD-3)
Random	<code>request(k) → id; get(id)</code> returns 32 bytes once beacon round h+k is final	\$10
Resolve	Read market outcome and resolution stage	Lets EVM contracts build on resolved outcomes
Stake	Delegate/undelegate on behalf of contract	For liquid-staking contracts

- **EVM-6** Assets move between RainCore and RainEVM via a system contract; ERC-20s created in RainEVM **MAY** be linked to RainCore spot balances only after winning a listing auction (§11.3).

9 Leverage v1

9.1 Model and choice

Decision: isolated-margin, long-only spot leverage on outcome shares, funded by a Leverage Lending Vault (LLV). A trader with margin m buys shares of YES (or NO) worth $L \cdot m$, borrowing $(L - 1) \cdot m$ in the market's quote asset from the LLV. The shares are held as collateral in the position. Shorting YES is expressed as long NO, so every position's worst case is the share price going to 0, and the loss is bounded by notional.

Compared with a perp-style synthetic (funding, mark-to-oracle, unbounded short side), this model keeps every share fully collateralised by complete sets, needs no funding rate and no external oracle, and settles naturally at resolution. Its cost is borrowing interest and a lending vault that can suffer loss in a gap; both are bounded below.

9.2 Leverage limits

Maximum leverage for a new position is the minimum of four caps:

```

L_max = min( L_tier(market), L_price(p), L_time(τ), L_phase )
L_price(p) = 1 + (L_tier - 1) · clamp( (min(p, 1-p) - 0.10) / 0.20 , 0, 1 )
L_time(τ) = 1 + (L_tier - 1) · clamp( (τ - 24h) / (7 days - 24h), 0, 1 )

```

- p is the mark price of the share bought; τ is time to scheduled resolution.
- No leverage on shares priced below 0.10 or above 0.90 (lottery-ticket tails gap hardest); full tier leverage only between 0.30 and 0.70.
- **Pre-event markets** (resolution not tied to a live event): leverage decays linearly to 1× from 7 days to 24 h before resolution; inside **T - 24 h the market is reduce-only for leveraged positions**.
- **Live-event markets** (sports, debates, award shows, election nights): leverage **continues during the event** under the stricter in-play regime of §9.2a; L_{time} is replaced by the in-play rules.
- **L_{phase}** : 2× at mainnet beta; 3× after 60 days without bad debt; 5× (Tier A only) after 120 days and a governance vote.

Tier	Eligibility (all required)	L_tier	Per-market leveraged OI cap	Per-account cap
A	Book depth $\geq$ \$250k within $\pm 2\phi$ (7-day median), age $\geq$ 14 days, OI $\geq$ \$2M, objective resolution source, scheduled resolution time	5×	min(10% of OI, \$2M)	\$100k notional
B	Depth $\geq$ \$50k within $\pm 2\phi$, age $\geq$ 7 days, OI $\geq$ \$500k, objective source, scheduled time	3×	min(10% of OI, \$500k)	\$25k notional
C	Everything else	1× (no leverage)	—	—

- **LEV-1** Global leveraged OI **MUST** be capped at 50% of LLV deposits and \$20M at beta.
- **LEV-2** Markets that resolve on a live event **MUST** switch to the in-play regime (§9.2a) at scheduled event start. Positions above the in-play caps **MUST** be reduced to those caps (not to 1×) starting 15 min before the start, via reduce-only orders with no penalty fee.
- **LEV-3** Markets resolving on subjective or AI-judged questions without an objective source are Tier C.

9.2a In-play leverage (live events)

Leverage during a live event is the riskiest feature in this specification: a goal, a red card or a called state can move a share from 0.55 to 0.05 in one block. It is offered in v1 because live events are where sports and event traders want it most, but under its own, stricter regime. Every parameter below is a governance parameter with a conservative launch value.

Parameter	Pre-event (§9.2)	In-play (launch value)	Rationale
Max leverage	Tier cap (2× → 3× → 5×)	min(L_tier, 2×) at beta; 3× for Tier A only after 90 days in-play with no bad debt; never above 3×	A full gap to 0 costs lenders 50% of notional at 2×, 67% at 3×
Price band for new leverage	0.10–0.90	0.20–0.80 ; full tier leverage only 0.35–0.65	Late-game prices sit near the tails and jump hardest
Maintenance margin	max(10%, 0.5 / L)	max(20%, 0.6 / L)	More buffer against adverse blocks
Per-market leveraged OI cap	min(10% of OI, tier cap)	Half the pre-event cap , max \$1M at beta	Bounds the worst single gap
Event-family cap	Shared (INS-2)	All markets on one match or event share one in-play cap	One goal moves every market on the match
End of event	—	Reduce-only in the final window: last 15 min of scheduled play (football), last quarter (basketball), or a governance-set window per event type	The outcome is nearly decided; leverage adds only gap risk
Borrow rate	LLV curve	LLV curve + 5% APR in-play premium	Prices the extra risk; premium goes to the in-play reserve
Liquidation fee	1.0%	1.5% (2/3 reserve, 1/3 liquidator)	Funds the in-play reserve

Protections that make in-play leverage workable

- **LIVE-1 Taker delay with free cancels.** In live-event markets every taking action (including leveraged opens, but **not** liquidations or reduce-only closes) waits **1 s** (governance range 0.5–3 s) before matching; cancels and post-only orders are never delayed. Unlike Polymarket's sports delay, during which orders cannot be cancelled, Rain lets makers pull quotes inside the delay window. This protects makers, and therefore the depth that liquidations sell into, from traders who see the goal before the book does.
- **LIVE-2 Suspension.** A live-event data feed attested by validators (at least two independent providers, TBC; median of timestamps) puts a market into **suspended** state on a scoring or review event (goal, penalty, VAR, red card): new orders and leveraged opens are rejected, cancels and repayments are allowed, liquidations queue. On reopen the market runs **5 s post-only**, then normal trading; queued liquidations go first among takers.
- **LIVE-3 Jump-aware mark price.** In-play, the per-block clamp of \$9.4 is removed, because a clamp would delay recognising a real jump and grow bad debt. The mark is the median of mid, a 5 s EMA and the \$5k depth price; after a suspension the first mark is taken from the post-only book.
- **LIVE-4 Gap liquidation goes straight to backstop.** A position that is below maintenance by more than half its margin after a jump skips partial book liquidation and is transferred to RLP at mark – 5% in the same block; any shortfall goes to the in-play reserve. This avoids dumping into a thin post-goal book.
- **LIVE-5 In-play reserve.** A ring-fenced sub-account of the insurance fund backs in-play positions: seeded with **\$0.5M** on top of the \$1.5M seed, funded by the in-play premium and liquidation fees, and required to stay $\geq$ the worst single-event gap at current caps (beta: $\$1M \times 50\% = \$0.5M$). If it falls below, in-play leverage becomes reduce-only automatically until it is replenished.
- **LIVE-6 Data-feed failure.** If feeds disagree or stop for > 10 s, the market is suspended; if they stay down > 2 min, in-play leverage on that market becomes reduce-only for the rest of the event.
- **LIVE-7 Simulation gate (in-play).** Before in-play leverage goes live, the team **MUST** backtest these exact rules on in-play price paths: at least 300 resolved live-event markets (Polymarket sports history plus a licensed betting-exchange data set, source TBC), with scoring events marked. Acceptance: modelled in-play bad debt $\leq 1\%$ of in-play leveraged volume, no single event $> 50\%$ of the in-play reserve, and $\geq 95\%$ of gap events fully absorbed by RLP and the reserve.
- **LIVE-8 Global in-play cap.** In-play leveraged OI **MUST NOT** exceed 25% of global leveraged OI ($\leq \$5M$ at beta).

Worst case at beta (2×, \$1M per-event cap): a match flips from 0.80 to 0.00 with every leveraged position long the losing side $\rightarrow$ lender loss $\leq \$0.5M$, fully covered by the in-play reserve; the general insurance fund is untouched. Several matches gapping at once are bounded by LIVE-8.

9.3 Leverage Lending Vault

- **LLV-1** One vault per quote asset. Depositors earn interest; utilisation $u = \text{borrowed} / \text{deposits}$.
- **LLV-2** Interest (APR) = $4\% + 16\% \cdot u$ for $u \leq 80\%$, then $+ 200\% \cdot (u - 80\%)$; borrowing **MUST** be refused above 90% utilisation.
- **LLV-3** 10% of interest goes to the insurance fund. Withdrawals are instant up to available liquidity, otherwise queued.

9.4 Mark price

```

mid_t      = (best_bid + best_ask)/2  if spread ≤ 5¢, else last_mark
ema_t      = EMA of trade prices, half-life 30 s
book_t     = depth-weighted price to fill $5k each side
raw_t      = median(mid_t, ema_t, book_t)
mark_t     = clamp(raw_t, mark_{t-1} ± 2¢ per block)

```

- **MARK-1** Mark price is computed by RainCore every block from on-chain data only (no external oracle).
- **MARK-2** The per-block clamp slows manipulation but cannot stop a genuine jump; jump risk is handled by sizing (§9.7), not by the mark.

9.5 Margin

```

equity      = shares · mark - debt - accrued_interest
initial     : equity ≥ notional / L_max
maintenance: equity ≥ MMR · notional,  MMR = max(10%, 0.5 / L_max)

```

At 2× the position is liquidated when equity falls below 25% of notional; at 5×, below 10%.

9.6 Liquidation waterfall

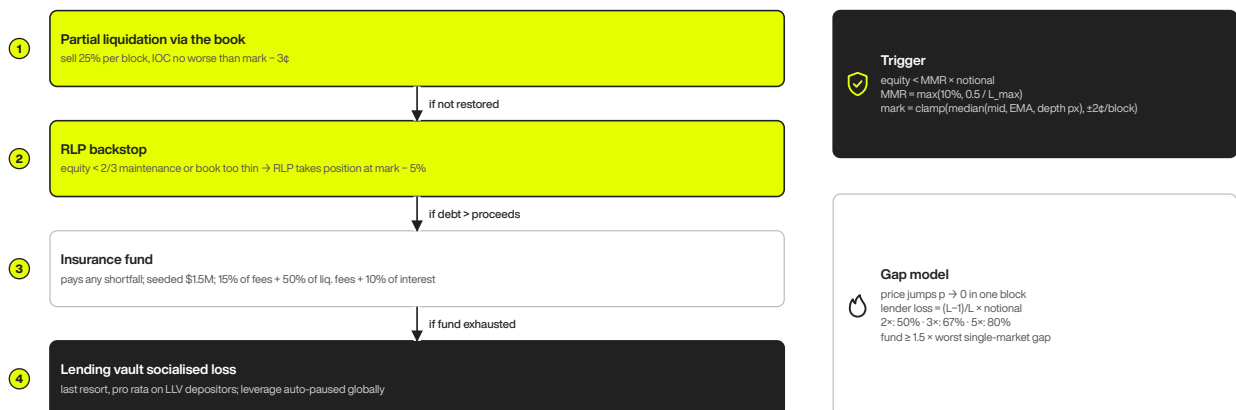


Figure 4. Liquidation waterfall. Each step only runs if the previous one could not close the position without loss to the lending vault.

1. **Partial liquidation via the book.** RainCore sells 25% of the position (or all if notional < \$500) with an IOC limit no worse than mark - 3¢; repeated each block until maintenance is restored.
 2. **RLP backstop.** If equity < 2/3 of maintenance, or the book cannot absorb the order within the slippage cap, RLP's liquidator strategy takes the remaining position at mark - 5% and assumes the debt.
 3. **Insurance fund.** Any shortfall (debt > proceeds) is paid by the insurance fund of that quote asset.
 4. **LLV socialised loss.** Only if the insurance fund is exhausted, the shortfall is written off pro rata against LLV depositors and leverage is automatically paused globally.
- **LIQ-1** Liquidation fee: 1.0% of liquidated notional, split 50% insurance fund, 50% to the liquidator (RLP or a permissionless liquidator in Phase 3).
 - **LIQ-2** Liquidations are class-3 actions generated by the protocol at the start of the block, after cancels.

9.7 Gap risk and insurance sizing

Outcome prices jump on news: a share at 0.70 can be 0.00 one block later. Worst case for a position bought at price p with leverage L when the price jumps to 0: proceeds 0, debt = $(L - 1)/L \cdot \text{notional}$, so **lender loss = $(L - 1)/L$ of notional**: 50% at 2×, 80% at 5×.

Stress case used for sizing: the largest Tier-A market gaps to 0 with leveraged OI at its cap.

Phase	Leveraged OI cap (global)	Single-market cap	Worst single-gap lender loss	Insurance fund required
Beta (2×)	\$20M	\$2M	\$1.0M	$\geq \$1.5M$ (1.5× worst gap)
3×	\$35M	\$2M	\$1.33M	$\geq \$2.0M$
5× (Tier A)	\$50M	\$2M	\$1.6M	$\geq \$3.0M$ and $\geq 6\%$ of leveraged OI

- **INS-1** The insurance fund **MUST** be seeded with \$1.5M (treasury) before leverage launches and **MUST** stay $\geq$ the requirement above; if it falls below, L_{phase} drops one step automatically.
- **INS-2** Correlated markets (same event family) **MUST** share one OI cap.

9.8 Resolution, kill switches and simulation

- **LEV-4** At resolution, a leveraged position settles automatically: payout repays debt and interest first, the remainder goes to the trader; a losing position's debt is covered by the waterfall. Pre-event markets reach resolution with no leverage (reduce-only from $T - 24$ h); live-event markets reach it after their reduce-only final window.
- **LEV-5** Kill switches: per-market leverage pause and reduce-only mode (guardian or governance), a separate global in-play leverage pause, global leverage pause (guardian, 3-of-5), automatic pause on any socialised loss. Pauses **MUST NOT** block closing or repaying.
- **LEV-6 Simulation gate**: before mainnet leverage, the team **MUST** backtest the exact formulas on ≥ 500 resolved Polymarket markets (public price history) plus Rain's own history, with synthetic gaps (in-play rules have their own gate, LIVE-7). Acceptance: modelled bad debt $\leq 0.5\%$ of cumulative leveraged volume, no single event $> 50\%$ of insurance fund, and liquidation success via the book $\geq 90\%$ by count.

9.9 Why not 10–100× in v1

At 10× an 8¢ move wipes the margin; outcome shares move 8¢ in one block routinely around news. Above 5×, the waterfall would rely on the insurance fund for ordinary events rather than for tails, and lender losses per gap approach 100% of notional. Higher leverage needs portfolio margin and per-event correlation models, which are Phase 3+ research items. For the same reason in-play leverage is capped at 3× in this version.

10 Randomness beacon and outcome applications

10.1 Beacon

- **RNG-1** Validators **MUST** run a distributed key generation (DKG) at each validator-set change to create a threshold BLS key (threshold $t = \lfloor 2n/3 \rfloor + 1$ of current validators).
- **RNG-2** For each block h , each validator includes its signature share over (chain id, h) in its vote extension; the aggregated signature σ_h is unique and verifiable, and $R_h = \text{SHA-256}(\sigma_h)$. It is unbiased (BLS signatures are deterministic) and unpredictable until t validators reveal shares.
- **RNG-3** Contracts **MUST** use commit-then-reveal: a request in block n receives $R_{\{n+k\}}$, $k \geq 2$ (default 3). The `Random` precompile reverts if read before that round is final.
- **RNG-4** If σ cannot be formed in a block (fewer than t shares), the round is skipped and pending requests roll to the next available round; there is no fallback to proposer randomness.
- **RNG-5** Collusion of $\geq t$ validators can predict (not bias) R ; casino contracts **SHOULD** cap the single-bet payout at a fraction of house-vault equity accordingly. This is disclosed in operator docs.

10.2 House Vault template and operators

- **CAS-1** Rain **MUST** publish open-source, audited templates: House Vault (LPs deposit, share house edge and variance, withdrawal delay 24 h, per-bet max payout 1% of vault equity), dice, lottery (scheduled draw), and a crash-style game.
- **CAS-2** Rain **MUST NOT** operate games. Operators deploy their own instances, own their licences and front ends, and may set builder-style fees.
- **CAS-3** UpDown (5- and 15-minute BTC/ETH markets) migrates as a RainCore outcome market type with a price-feed resolver (Chainlink Data Streams or equivalent, verified on-chain); TBC whether the feed is available on Rain Chain at launch (fallback: signed price relayed with validator attestations).

10.3 Other outcome products

Product	Primitive used	Phase
Sports exchange (back/lay)	Merged book, in-play leverage (§9.2a), taker delay, suspension	2
Short-dated up/down options	Recurring outcome markets, price resolver	2
Parametric insurance	Outcome markets + EVM vaults reading <code>Resolve</code>	3
Lotteries · casino games	<code>Random</code> , House Vault	2 (templates), operators thereafter
AI trading agents	Agent keys, gasless trading, WS feeds	2

11 Token, issuance and fees

11.1 RAIN across two chains

The Arbitrum RAIN proxy is upgradeable. Its current implementation has `burn` and `burnFrom` but no `mint`; an upgrade can add a mint function that only the bridge may call. This removes any constraint on moving inflation-minted RAIN back to Arbitrum.

Decision: RAIN is native on Rain Chain and moves between the chains by burn-and-mint, with one global supply. Stablecoins use the lockbox.

- **TOK-1** Rain upgrades the Arbitrum RAIN implementation to add `bridgeMint(address,uint256)` callable **only** by the Rain Chain bridge contract, keeping storage layout, balances, `burn` / `burnFrom` and all ERC-20 behaviour unchanged. The upgrade **MUST** be audited, executed by the proxy owner behind a ≥ 7 -day timelock, and announced to exchanges and integrators in advance.
- **TOK-2 Deposit (Arbitrum → Rain Chain):** the bridge burns RAIN on Arbitrum (`burnFrom` after approval) and Rain Chain mints the same amount natively. **Withdrawal:** RAIN is burned on Rain Chain and, after the BR-3 delay, `bridgeMint` mints it on Arbitrum. No RAIN sits in a lockbox, so there is no RAIN honeypot.
- **TOK-3 Supply invariant:** Arbitrum supply + Rain Chain supply = global supply $S(t) = S_0 + \text{protocol inflation} - \text{burns}$. Validators check the invariant at every checkpoint; any breach pauses RAIN bridging automatically.
- **TOK-4 Mint limits on Arbitrum:** `bridgeMint` **MUST** enforce a rolling cap inside the token contract itself (launch: 0.1% of S_0 per hour, 0.5% per 24 h), so a compromised bridge cannot mint unbounded RAIN. Raising the cap needs the same timelocked upgrade path.
- **TOK-5** Total supply is reported as the global figure. Inflation minted on Rain Chain can be withdrawn to Arbitrum like any RAIN, within the TOK-4 caps. xERC20/OFT adapters for other chains **MAY** follow, with Rain Chain as the canonical home.

11.2 Issuance

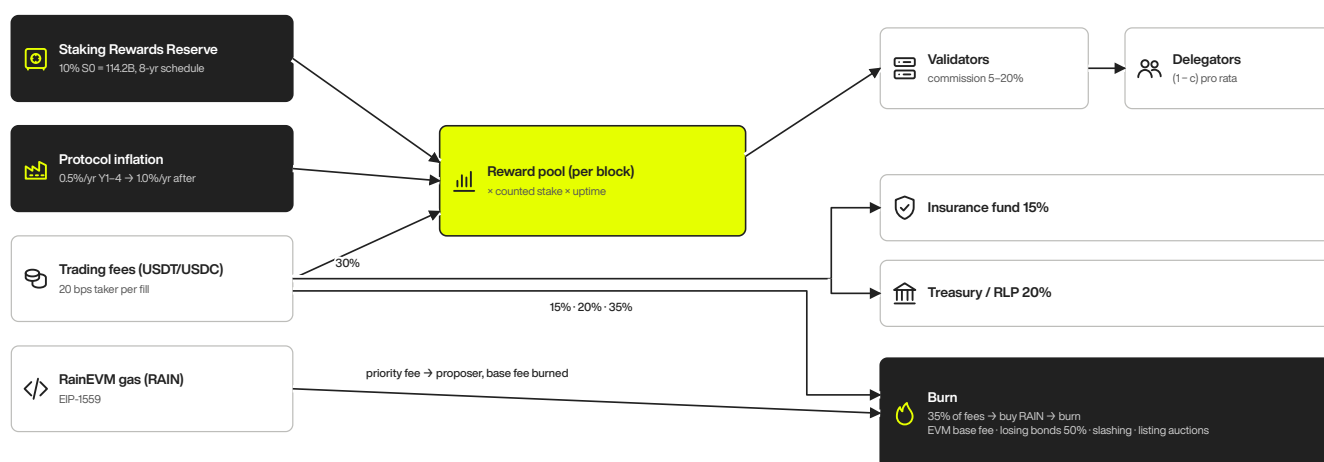


Figure 5. Token flows. Rewards come from the reserve, inflation and fees; burns come from EVM base fees, buy-and-burn and lost bonds.

- **ISS-1 Staking Rewards Reserve:** 10% of S0 = 114.24B RAIN from existing supply, transferred by the Foundation into a genesis module account and released per block: Y1 2.00%, Y2 1.75%, Y3 1.50%, Y4 1.25%, Y5 1.00%, Y6 1.00%, Y7 0.75%, Y8 0.75% of S0.
- **ISS-2 Protocol inflation:** 0.50% per year of current supply in years 1–4, **1.00% per year from year 5, permanently**, minted per block. Rationale: the network needs a permanent security budget; a low start keeps net inflation small while the reserve does the heavy lifting, and the step-up at year 5 replaces the declining reserve so the security budget never falls off a cliff.
- **ISS-3 Dynamic adjustment (Phase 3):** governance **MAY** enable a ± 0.25 pp adjustment per year targeting a 50% staking ratio; until then inflation is fixed.

Table T1 — Issuance schedule (no burn)

Year	Reserve release (% S0)	Protocol inflation (% supply)	New supply minted (RAIN)	Supply end of year	Gross issuance to stakers (% of supply)
1	2.00%	0.50%	5.71B	1,148.12B	2.49%
2	1.75%	0.50%	5.74B	1,153.86B	2.23%
3	1.50%	0.50%	5.77B	1,159.63B	1.98%
4	1.25%	0.50%	5.80B	1,165.43B	1.72%
5	1.00%	1.00%	11.65B	1,177.08B	1.96%
6	1.00%	1.00%	11.77B	1,188.85B	1.95%
7	0.75%	1.00%	11.89B	1,200.74B	1.70%
8	0.75%	1.00%	12.01B	1,212.75B	1.70%
9	0.00%	1.00%	12.13B	1,224.88B	0.99%
10	0.00%	1.00%	12.25B	1,237.13B	0.99%

Reserve releases are pre-existing tokens (locked at genesis), so they do not raise total supply; only protocol inflation mints.

Table T2 — Staking APR before commission (year 1 and year 5)

Staking ratio	Bonded RAIN	Bonded USD	APR Y1	APR Y5	APR Y9
10%	114.24B	\$1.32B	24.88%	19.61%	9.90%
30%	342.72B	\$3.96B	8.29%	6.54%	3.30%
50%	571.20B	\$6.59B	4.98%	3.92%	1.98%
70%	799.69B	\$9.23B	3.55%	2.80%	1.41%

Token-denominated, excludes the fee share (Table T3). Validators keep commission on delegated rewards.

Table T3 — Fees, burn and net inflation, year 1

Scenario	Monthly volume	Annual protocol fees	To stakers	Buy-and-burn (USD)	RAIN burned	Net supply change	Net inflation
low	\$50M	\$1.20M	\$0.36M	\$0.42M	0.04B	+5.68B	0.50%
med	\$500M	\$12.00M	\$3.60M	\$4.20M	0.36B	+5.35B	0.47%
high	\$5,000M	\$120.00M	\$36.00M	\$42.00M	3.64B	+2.07B	0.18%

Fee rate 20 bps taker / 0 bps maker on notional; split stakers 30% · burn 35% · insurance 15% · treasury/RLP 20%. Burn assumes constant price \$0.01154533.

Table T4 — Cost to attack consensus (buying new stake, no price impact)

Staking ratio	Bonded USD (B)	Halt: buy > B/2	Control: buy > 2B	Control as % of all RAIN
10%	\$1.32B	\$0.66B	\$2.64B	20%
30%	\$3.96B	\$1.98B	\$7.91B	exceeds unstaked circulating supply
50%	\$6.59B	\$3.30B	\$13.19B	exceeds unstaked circulating supply
70%	\$9.23B	\$4.62B	\$18.47B	exceeds unstaked circulating supply

An attacker must ADD stake: control needs $A/(B+A) > 2/3 \Rightarrow A > 2B$; halting needs $A > B/2$. Seats are irrelevant — voting power is stake-weighted.

Table T5 — Validator revenue check, genesis (7 validators, 10% staked, 10% commission)

Item	Value
Year-1 staking rewards (RAIN)	28.56B
Year-1 staking rewards (USD)	\$329.7M
Per validator, equal stake (USD/yr)	\$47.1M
Commission income per validator (USD/month)	\$393k
Operating cost (assumption, USD/month)	\$5k–\$12k
Min self-bond 25M RAIN at 1-year lock (USD)	\$289k

Circulating (CoinGecko-implied) $\approx$ 709.26B RAIN. Reference: $S_0 = 1,142,408,474,514$ RAIN; price \$0.01154533; FDV $\approx$ \$13.19B.

Reading the tables. Year-1 gross staking yield is $\approx 2.5\%$ of supply. At a realistic early staking ratio of 10–30% that is an APR of 8–25% in RAIN before fees, which is enough to attract delegators; at 50% it is $\approx 5\%$. Net inflation in year 1 is 0.18–0.50% depending on volume, and turns negative only at roughly \$8B/month of volume at today's price (scales with volume $\div$ price).

11.3 Spot listing auction (Phase 3)

- **LIST-1** RainEVM ERC-20s **MAY** obtain a RainCore spot book by winning a 31-hour Dutch auction for a listing slot (HL HIP-1 pattern): start at $2\times$ the last clearing price, floor 5M RAIN; proceeds 100% burned.
- **LIST-2** v1 RainCore books are for outcome markets and the RAIN/USDT, RAIN/USDC pairs only (needed for buy-and-burn).

12 Validators, staking and security

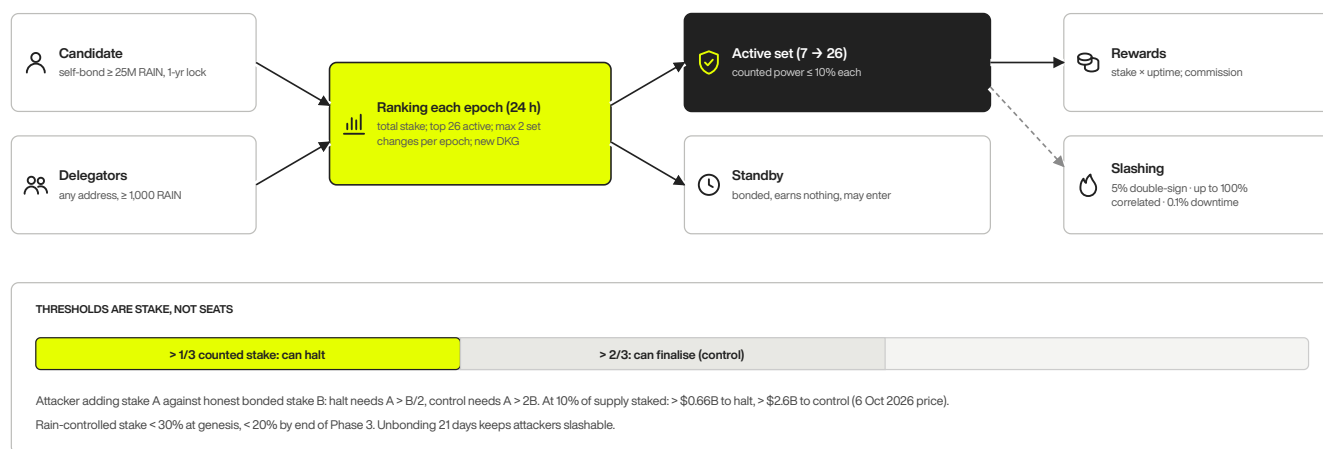


Figure 6. Validator set and staking flow. Anyone can bond; the top 26 by stake are active; counted voting power is capped at 10% each.

12.1 Parameters

Parameter	Value	Rationale
Genesis set	7 validators ($f = 2$)	\$4.3
Active set	Top 26 by total stake (self + delegated); min 5 to produce blocks	Rain decision; 26 keeps BFT message cost low at 200 ms
Min self-bond	25M RAIN ($\approx \$289\text{k}$), locked 1 year from activation	Comparable skin in the game to HL's 10k HYPE requirement (USD value depends on HYPE price — TBC); high enough that a seat is a serious commitment, low enough for professional operators
Delegation	Open to any address; min 1,000 RAIN	
Unbonding	21 days	Longer than any slashing evidence window and the bridge's longest withdrawal delay
Redelegation	Instant, once per 7 days per delegation	

Parameter	Value	Rationale
Set changes	Max 2 entries/exits per epoch (1 epoch = 24 h)	Prevents sudden set capture; gives time for DKG
Voting-power cap	10% of counted power per validator; excess stake still earns rewards at 50% rate	Prevents a single whale validator
Commission	Min 5%, max 20% ; increase ≤ 1 pp per 7 days, announced 7 days ahead; decreases instant	Stakers protected from bait-and-switch (HL allows increases only to $\leq 1\%$)

12.2 Rewards and commission

- **VAL-1** Each block, the reward pool (reserve release + inflation + RAIN-side priority fees) is distributed to active validators in proportion to **counted stake $\times$ uptime factor**, where uptime factor = signed blocks / blocks in the last epoch, floored to 0 below 90%.
- **VAL-2** Each validator takes commission c on delegators' rewards; delegators receive $(1 - c)$ pro rata. The 30% fee share in stablecoins is distributed the same way once per epoch.
- **VAL-3 Economics check (Table T5):** at 7 validators and 10% staked, the year-1 reward pool is $\approx \$330\text{M}$ at today's price; a 10% commission yields $\approx \$390\text{k/month}$ per validator against $\$5\text{--}12\text{k/month}$ operating cost. Even at 26 validators and a 90% lower token price, commission covers costs comfortably. **Implication:** the APR at low staking ratios is high; this is intended to attract stake fast (a higher staking ratio is the security budget), but it is also the main source of sell pressure — see risk R-9.

12.3 Answering "26 seats $\times$ \$1M = \$26M takeover"

The critique assumes seats carry equal votes. They do not.

1. **Votes are stake-weighted, not seat-weighted.** Controlling the chain requires $> 2/3$ of *counted bonded stake*, and halting it requires $> 1/3$. The number of seats an attacker holds is irrelevant; only stake matters.
2. **The attacker must add stake on top of honest stake.** With honest bonded stake B , an attacker needs $A > 2B$ for control and $A > B/2$ to halt (Table T4). At just 10% of supply staked ($B \approx \$1.32\text{B}$), control costs $> \$2.6\text{B}$ and halting $> \$660\text{M}$ of RAIN bought on the market — before price impact, which makes acquiring 20% of supply practically impossible (daily RAIN liquidity is orders of magnitude smaller, assumption).
3. **The 10% cap means one entity needs many validators**, each with its own 25M RAIN self-bond, and the entry rate limit (2 per day) gives the community days of visible warning.
4. **Slashing makes the attack self-destructive:** double-signing loses 5% of stake, correlated double-signing by $\geq 1/3$ of power loses 100%, and the 21-day unbonding means the attacker's stake is still slashable afterwards.
5. **Social layer:** a safety violation is publicly provable; validators and exchanges coordinate a fork that burns the attacker's stake (§12.6).

What the critique does identify correctly is the **genesis-phase risk**: if little RAIN is staked, B is small. Mitigation: the Foundation delegation program bonds enough RAIN at genesis that $B \geq 10\%$ of supply, while the Rain-controlled share stays $< 1/3$ of counted power (§12.5).

12.4 Why not NFT seats

NFT seats were rejected: (a) they decouple voting power from economic stake, so security becomes the price of 18 NFTs rather than the value of bonded RAIN; (b) they create a scarce, tradable object that invites regulatory characterisation as a sale of revenue rights; (c) they cannot be slashed proportionally and make removal of a bad operator a governance fight; (d) they give RAIN holders no way to participate, which undermines the decentralisation narrative.

12.5 Slashing, jailing and Foundation stake

Offence	Penalty
Double-sign (equivocation)	5% of validator and delegated stake, tombstoned (permanent removal)
Correlated double-sign	Penalty = $\min(100\%, 3 \times \text{fraction of power that double-signed in the same 21-day window})$
Downtime	Jailed after missing 95% of blocks in a 10,000-block window (~33 min); 0.1% slash; unjail after 1 h
Invalid bridge signature (signing a withdrawal not in Rain Chain state)	100% of validator self-bond and 5% of delegations; tombstoned
Beacon withholding	Counted as downtime

- **SEC-1 Foundation delegation program:** at genesis the Foundation delegates to independent operators so that no entity exceeds 10% counted power and Rain-controlled entities together stay **below 30%** of counted power. Rain-controlled stake **MUST** fall below 20% by the end of Phase 3.
- **SEC-2** Slashed RAIN is burned (not redistributed) to remove any incentive to frame validators.

12.6 Governance and upgrades

- **GOV-1** Parameter changes are on-chain proposals voted by bonded stake (quorum 33.4%, pass > 50% yes, veto > 33.4% no-with-veto), with a 7-day vote and 48 h execution timelock.
- **GOV-2** Binary upgrades are coordinated by validators at a governance-approved height with a ≥ 72 h timelock; emergency security patches **MAY** use 24 h with a 2/3 validator signal.
- **GOV-3 Foundation multisig (4-of-7 hardware signers)** has limited powers: list markets (until Phase 3), rotate resolver keys, appoint guardians, pause leverage. It **MUST NOT** move user funds, mint, or change consensus. Its powers sunset to governance by end of Phase 3 + 12 months.
- **GOV-4 Social-layer recovery:** if a safety fault is proved, validators **MAY** coordinate a halt and a state rollback to the last honest finalized block with slashing applied. The procedure is pre-published.

13 Bridge (Arbitrum One ↔ Rain Chain)

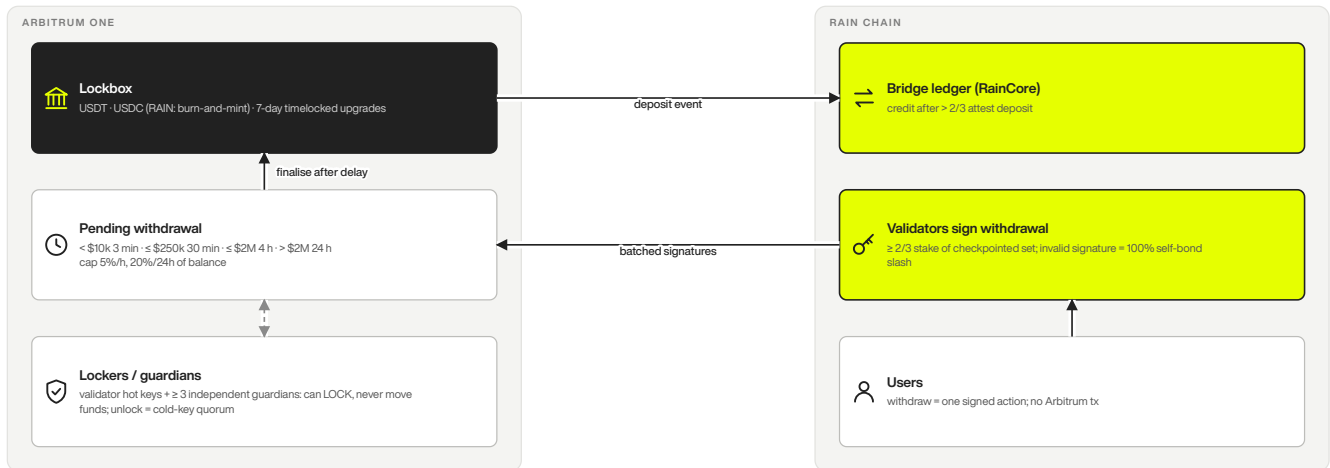


Figure 7. Bridge security. Deposits are credited after Arbitrum finality; withdrawals need 2/3 stake signatures, wait a size-based dispute delay, and stay under an hourly cap. Guardians can pause but never move funds.

13.1 Requirements

- BR-1** A lockbox contract on Arbitrum One **MUST** hold USDT and USDC (RAIN uses burn-and-mint, §11.1). It **MUST NOT** be upgradeable except through a 7-day timelocked validator-quorum upgrade.
- BR-2 Deposits** are credited on Rain Chain when > 2/3 of validator power attest to the event after the Arbitrum block is final on Ethereum-batch posting (Assumption: ~10–20 min soft-confirm vs instant; v1 uses Arbitrum "safe" head, typically < 1 min, with a per-deposit cap of \$250k on fast path).
- BR-3 Withdrawals** require signatures from validators holding ≥ 2/3 of power in the last checkpointed validator set, then a dispute delay:

Withdrawal size (USD)	Delay
< \$10k	3 min
\$10k–\$250k	30 min
\$250k–\$2M	4 h
> \$2M	24 h

- **BR-4 Outflow cap:** total withdrawals per asset per rolling hour **MUST NOT** exceed 5% of the lockbox's balance (and per rolling 24 h, 20%); excess queues automatically.
- **BR-5 Lockers / guardians:** every validator hot key plus ≥ 3 independent guardians (security firms, assumption) **MAY** lock the bridge if a pending withdrawal does not match Rain Chain state. Unlock requires a quorum of validator **cold** keys, matching Hyperliquid's Bridge2 design. Guardians **MUST NOT** be able to move funds.
- **BR-6** Validator-set updates on the bridge follow the same signature + dispute flow; the old set remains slashable during unbonding.
- **BR-7 Deposit caps** during beta: \$25M total stablecoins, raised by governance after each audit milestone.
- **BR-8** Optional address screening (sanctions lists) **MAY** be enabled at the bridge by governance; front ends do their own screening.
- **BR-9** The bridge **MUST** have two independent audits and formal verification of the signature-threshold logic before mainnet.

14 Non-functional requirements

ID	Requirement	Target
NFR-1	Block time / finality	200 ms / 1 block (target)
NFR-2	End-to-end order latency, co-located client	p50 $\leq$ 300 ms, p99 $\leq$ 1 s
NFR-3	Sustained throughput	$\geq$ 20,000 order actions/s; burst 50,000/s for 10 s (target)
NFR-4	Availability	$\geq$ 99.9% of blocks on time per month ($\leq$ 43 min degraded)
NFR-5	Determinism	Replay from genesis reproduces all state hashes; CI replays each testnet day
NFR-6	State sync	New full node synced from snapshot in $\leq$ 30 min; snapshots every 10,000 blocks, signed
NFR-7	Archive	Full block + fill history retained; archive nodes serve historical queries
NFR-8	Recovery	Coordinated restart after halt in $\leq$ 30 min (runbook)

14.1 Node roles and hardware (assumption)

Role	Purpose	Hardware
Validator	Votes, proposes, holds consensus and bridge keys (HSM)	16–32 cores $\geq$ 3.5 GHz, 128 GB RAM, 2× 2 TB NVMe, 10 Gbit
Sentry	Shields validator, gossips	8 cores, 32 GB, 1 TB NVMe
Full node	Non-voting replica, apps	16 cores, 64 GB, 2 TB NVMe
RPC / API	REST, WS, EVM JSON-RPC	Full node + load balancer
Archive	All history	16 cores, 128 GB, 10+ TB NVMe

14.2 Observability

Every node **MUST** export Prometheus metrics (block time, round count, mempool depth per class, execution time per module, state-hash agreement), structured logs, and an OpenTelemetry trace per action id. A public status page shows block production, validator uptime and bridge queue.

14.3 APIs and explorers

REST and WebSocket APIs for books (L2 depth and order-level L3), fills, user state; EVM JSON-RPC; an indexer that streams every fill and event. Blockscout serves RainEVM; Virtux builds the RainCore explorer (markets, books, fills, validators, bridge queue).

15 Security, compliance and costs

15.1 Security programme

- **SECP-1** Audits before mainnet (estimates, assumption): consensus integration and RainCore engine \$250–400k; bridge contracts + validator signing \$150–250k; RainEVM and precompiles \$100–150k; leverage and liquidation \$100–200k. Total **\$0.6–1.0M**.
- **SECP-2** Bug bounty from testnet: up to \$1M for critical bridge or consensus bugs (scaled to TVL), via Immunefi or similar.
- **SECP-3** Keys: validator consensus keys on remote signers with double-sign protection; bridge cold keys on hardware wallets; Foundation multisig 4-of-7.

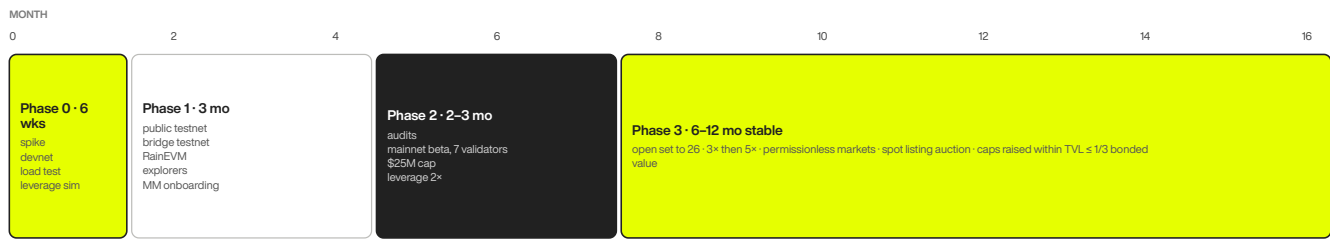
15.2 Compliance stance

Rain provides infrastructure; operators of front ends and games run their own products. Legal positioning is covered by Rain's existing legal opinion and is outside the scope of this specification. Protocol-level options are bridge screening (BR-8) and market-listing policy.

15.3 Infrastructure cost (assumption)

Item	Testnet	Mainnet early
Rain-operated validators / sentries (bare metal, Hetzner/OVH/Latitude)	4–7 × \$400–900	2–3 × \$900–1,500 (rest independent)
RPC/API cluster, archive, indexer	\$800–1,500	\$3–8k
Explorers, monitoring, snapshots, CDN	\$500–1,000	\$2–5k
Monthly total	\$2–5k	\$8–20k

16 Delivery plan



Gates: Phase 0 → state-hash replay + 20k actions/s execution · Phase 1 → 30 days ≥ 99.5% on-time blocks · Phase 2 → audits closed + simulation gate + insurance seeded

Figure 8. Roadmap. About 9–11 months from start to stable mainnet; leverage begins at 2× in beta.

Phase	Duration	Scope	Acceptance criteria
0 Foundations	6 weeks	Consensus spike (Malachite vs Commonware); engine inside node; 4-node devnet; load test harness; leverage simulator	Engine replays 1M random actions with identical state hash on 4 nodes; ≥ 20k actions/s on one node's execution; consensus decision memo; first backtest report
1 Public testnet	3 months	7-node testnet; mint-on-match, multi-outcome, resolution module; MM onboarding (≥ 3 MMs); bridge on Arbitrum Sepolia; RainEVM + precompiles; explorers; SDK	30 days with ≥ 99.5% on-time blocks; p99 ≤ 1 s; bridge chaos tests pass; RainEVM runs Rain AA + House Vault templates
2 Mainnet beta	2–3 months	Audits, fixes; 7 validators (≥ 4 independent); deposit cap \$25M; leverage 2× on Tier A/B; Rain app migration	All critical/high audit findings closed; insurance fund seeded; 30 days with no consensus fault; leverage simulation gate passed
3 Stable	6–12 months	Open set to 26; 3× then 5×; permissionless markets; spot listing auction; caps lifted gradually	≥ 15 validators, Rain stake < 20%; zero bad debt beyond insurance; bridge TVL growth with no incident

16.1 Team

Role	Owner	Responsibility
Product & management	Rain leadership	Decisions, partners, MM and validator relations
Core protocol	Dario (writes code) + 1–2 Rust engineers (to hire, assumption)	Node, RainCore, consensus integration, leverage
Contracts	Rain Solidity team	Bridge lockbox, RainEVM system contracts, House Vault templates
DevOps	Rain DevOps	Validators, sentries, RPC, monitoring, snapshots
Explorer	Virtux	RainCore explorer, indexer UI

16.2 KPIs

KPI	Phase 2 target	Phase 3 target
Monthly volume	\$50M	\$500M
Active MMs	5	15
Median quoted spread (Tier A)	≤ 2¢	≤ 1¢
Independent validators	4 of 7	≥ 15 of 26
Staking ratio	≥ 10%	≥ 30%
Bad debt beyond insurance	0	0

17 Risk register

#	Risk	Likelihood	Impact	Mitigation
R-1	Bridge exploit (key compromise, signature bug)	Medium	Critical	2/3 stake signatures, size delays, hourly cap, lockers, two audits, formal verification, deposit caps
R-2	Consensus or determinism bug halts or forks the chain	Medium	High	Proven library, replay CI, multi-client fuzzing, post-only restart, runbooks
R-3	Leverage bad debt from gaps (highest in-play)	Medium	High	Price/time caps, Tier eligibility, OI caps, in-play regime (taker delay, suspension, reserve), insurance sizing, simulation gates, kill switches
R-3a	Live data-feed error or delay	Medium	Medium	Two independent feeds, median, auto-suspend on disagreement, reduce-only fallback
R-4	Liquidity cold start	High	High	RLP quoting, MM incentives, existing Rain flow migrates, builder codes
R-5	Regulatory change	Low	High	Infrastructure stance per Rain legal opinion, operator licensing, optional screening
R-6	Validator collusion / capture	Low	Critical	Stake weighting, 10% cap, slashing, entry rate limit, social recovery
R-7	Proposer front-running within class	Medium	Medium	Monitoring of first-seen order; later encrypted mempool
R-8	Key management failure (resolver, guardian, multisig)	Medium	High	HSM, rotation, 4-of-7, separation of roles
R-9	RAIN price fall shrinks security budget; reward selling	Medium	High	Bonded-value monitoring, deposit caps tied to bonded value (bridge TVL ≤ 1/3 of bonded USD), declining reserve schedule
R-10	Small core team / key-person risk	High	High	Hire 1-2 Rust engineers, documentation, audits as review
R-11	AI resolver error	Medium	Medium	Bonded disputes, open tier-3 vote, no forced fallback outcome

R-9 rule (adopted): stablecoin TVL in the bridge **SHOULD NOT** exceed one third of bonded stake value; governance raises deposit caps only within this bound.

18 Competitive positioning

Dimension	Rain Chain (planned)	Hyperliquid	Polymarket	Kalshi	dYdX v4	Injective
Type	Outcome-focused L1	Trading L1	App; settles on Polygon	Regulated US exchange (CFTC DCM)	Cosmos app-chain	Cosmos finance L1
Order book	Native, in consensus	Native (HyperCore)	Off-chain matching, on-chain settlement	Centralised	Off-chain books in validators, on-chain settlement	Native on-chain module
Outcome markets	Core product	HIP-4 (initial binary BTC market)	Core product	Core product	Not core (assumption)	Via apps (assumption)
Leverage on outcomes	Yes, $\leq 5\times$, long-only	Not on outcomes ("does not involve leverage", HIP-4 docs)	No (assumption)	No (assumption)	Perps	Perps
Native randomness	Yes (BLS beacon)	No (assumption)	No	No	No (assumption)	No (assumption)
Gasless trading	Yes, rate-limited	Yes	Yes for users (relayed)	n/a	Yes (assumption)	Gas fees (assumption)
Sources	This spec	hyperliquid.gitbook.io	Assumption: public docs	Assumption: public docs	Assumption	Assumption

Rain's wedge is not raw throughput (Hyperliquid will remain faster for years) but being the **only chain where outcome primitives — merged books, resolution, randomness, bounded leverage — are all native.**

19 Glossary

Term	Meaning
ALO / post-only	Order that is rejected if it would take liquidity
BFT, f	Byzantine fault tolerance; f = number of faulty validators tolerated ($n \geq 3f + 1$)
Complete set	One YES + one NO share, always redeemable for 1.00
Mint-on-match / burn-on-match	Creating or merging a complete set when two opposite-side buyers (or sellers) match
Counted power	Validator stake after the 10% cap
DKG / threshold BLS	Distributed key generation; signatures that need t of n shares
LLV	Leverage Lending Vault
RLP	Rain Liquidity Provider — protocol vault for quoting and backstop

Term	Meaning
Lockbox	Arbitrum contract holding bridged assets
Builder code	Registered front-end identifier that earns a per-fill fee
Tier A/B/C	Market eligibility levels for leverage
S0	RAIN total supply at 6 Oct 2026 = 1,142,408,474,514
In-play	Trading while the underlying live event is in progress
Taker delay	Short hold before a taking order can match; cancels are not held

20 Decisions taken in this spec

#	Topic	Decision	Rationale
D1	Chain type	Own L1, single Rust binary, RainCore + RainEVM	Rain decision; performance
D2	Consensus	Malachite or Commonwealth after 6-week spike; CometBFT fallback	Both Apache-2.0 Rust, active
D3	Genesis validators	7 ($f = 2$); min 5 to run; max 26	Margin for 1 maintenance + 1 fault
D4	Seats	Stake-ranked, no NFTs, 10% power cap	Security tracks bonded value
D5	Self-bond · unbonding	25M RAIN, 1-year lock · 21 days	Commitment; covers evidence windows
D6	Commission	5–20%, +1 pp / 7 days max	Protects delegators
D7	Issuance	Reserve 10% S0 over 8 yrs; inflation 0.5% (Y1–4), 1.0% after	Permanent security budget; smooth issuance
D8	Fees	20 bps taker / 0 maker; 30/35/15/20 split; builder ≤ 50 bps	Burn + security + insurance
D9	Book	One merged book per outcome; tick 0.001	Shared liquidity; tight tails
D10	Leverage	Isolated long-only via LLV; $2\times \rightarrow 3\times \rightarrow 5\times$ pre-event; in-play $\leq 2\times$ at beta, never $> 3\times$	Bounded loss, no oracle
D10a	In-play	1 s taker delay with free cancels, suspension on scoring events, 0.20–0.80 band, reduce-only final window, ring-fenced reserve	Leverage stays live during events with bounded gap risk
D11	RAIN home	Native on Rain Chain; burn-and-mint bridge to Arbitrum via audited upgrade adding a capped, bridge-only mint	One global supply, no RAIN honeypot
D12	Bridge	2/3 signatures, 3 min–24 h delay, 5%/h cap, lockers, \$25M beta cap	Largest risk, most guarded
D13	Resolution	Native 3-tier; RAIN bonds; open stake-weighted tier 3; no forced fallback	Decentralise final tier
D14	Randomness	Threshold BLS per block; reveal at $n + k$	Unbiasable, verifiable
D15	Bridge TVL bound	$\leq 1/3$ of bonded stake value	Attack must cost more than it can steal

21 Open items

1. **Rain:** confirm the source wallets for the 114.24B RAIN staking reserve and the Foundation delegation amount at genesis (target $\geq 10\%$ of supply bonded).
2. **Rain:** approve the \$1.5M insurance-fund seed, the \$0.5M in-play reserve and the \$25M beta deposit cap.
3. **Technical (Phase 0):** consensus library choice; whether the state root lags by one or two blocks; Chainlink Data Streams availability for UpDown on Rain Chain.
4. **Technical (Phase 1):** live-event data providers for in-play suspension (two independent feeds) and the licensed in-play price data set for LIVE-7.
5. **Commercial:** first 7 genesis operators (≥ 4 independent) and ≥ 3 launch market makers, including at least one with sports in-play experience.
6. **Token upgrade:** audit and timelocked execution of the Arbitrum RAIN upgrade adding the capped `bridgeMint` (TOK-1, TOK-4); notice to exchanges and integrators.