PrimeLayer: BTCFi Without Compromise

Bluepaper v1.0 – Academic Edition
Authors: Dan Wasyluk, Jag Sidhu
Date: October 2025
Tagline: BTCFi Without Compromise - A Bitcoin-Anchored zkEVM Economy

Citation: Wasyluk, D., & Sidhu, J. (2025). *PrimeLayer Bluepaper v1.0 - Academic Edition.* PrimeLayer Token Genesis DAO LLC; Research Publication.

Table of Contents

Abstract

1. Overview and Motivation
- 1.1 Terminology
- 1.2 The Case for Bitcoin-Anchored Programmability
- 1.3 The Problem with Blockspace Competition
- 1.4 Vision of a Hyper-bitcoinized Economy
- 1.5 Liquidity Incentives and Long Term Economic Sustainability as a Core Principle
- 1.6 PrimeLayer Objectives and Ethos
- 1.7 Economic Participation and Non-Custodial Yield
- 1.8 Plain-Language Summary

2. Core Components
- 2.0 Core Components
- 2.1 Gauges, Buckets, and Emission Directionality
- 2.2 Identity NFTs, vePRML, veBTC, and Binding
- 2.3 Committee Roles and Quorum Concepts
- 2.4 Plain-Language Summary

3. System Architecture – Components and Interactions
- 3.1 Subsystems and Trust Boundaries
- 3.2 Value and Data Flows across DAO, DEX, Vault, and Bridge
- 3.3 Fee Routing and Revenue Accounting
- 3.4 Modularity and Fault-Containment
- 3.5 Plain-Language Summary

4. Validator Economy (NV, HV, vePRML, veBTC, Bond NFTs)
- 4.1 Roles and Responsibilities
- 4.2 Hardware Validator Cohort Selection and Sortition

4.3 Network Validator Finality and Governance
4.4 Identity and Bond NFTs
4.5 Rewards, Slashing, and Reputation
4.6 Plain-Language Summary

5. Emission Allocation and Distribution
5.1 Fixed Allocations (Infrastructure) vs Governance-Directed Buckets
5.2 Bucket A – Liquidity and BTC Vault
5.3 Bucket B – Infrastructure, Treasury, Burn and Buyback Gauges
5.4 Early-LP Bonus and Gauge Warm-Up Rules
5.5 Plain-Language Summary

6. DAO Security and Governance Resilience
6.1 Bicameral Governance Model
6.2 Monetary Policy Proposals and Emergency Procedures
6.3 Veto Committee and Gauge Lifecycle
6.4 Warm-Up Escrow and Activation Delay
6.5 Treasury, Backstop Vault, and Recapture
6.6 Plain-Language Summary

7. BTC Participant Yield Layer
7.1 veBTC – Day-One Activation and Voting Scope
7.2 BTC Vault – Revenue, Distribution, and Pause/Resume Criteria
7.3 Binding veBTC to HV Identity – Market Design and Decay Benefits
7.4 Bribe Market Participation
7.5 Plain-Language Summary

8. pUSD Stablecoin System
8.1 Collateralization and Health Metrics
8.2 Mint, Redeem, and Liquidation Mechanics
8.3 Stability Tools and Backstop Integration
8.4 Plain-Language Summary

9. Bridge Operations and Decentralization Roadmap
9.1 Security Model and Objectives
9.2 Stage I – Federated Bridge (FB)
9.3 Stage II – Semi-Federated Bridge (SFB)
9.4 Stage III – Fully Decentralized ZK Garbled-Circuit Bridge (ZK-GC)
9.5 Operator Roles and Rotation
9.6 Route Safety, Limits, and Circuit Breakers
9.7 Fees, Revenues, and Accounting
9.8 Governed Stage Cutovers and Evidence
9.9 Plain-Language Summary

10. Infrastructure Continuity and Migration Protocol (Types I-III)
- 10.1 Overview and Objectives
- 10.2 Type I – Anchor Shift Migration
- 10.3 Type II – Full Infrastructure Migration
- 10.4 Type III – DA-Only Migration
- 10.5 Migration Types – Summary Table
- 10.6 Evidence, Monitoring, and Exit Criteria
- 10.7 Plain-Language Summary

11. Tokenomics – Allocation, Vesting, Long-Run Supply, EIP-1559 Fees
- 11.1 Initial Allocation and Vesting Schedules
- 11.2 Per-Epoch Allocation and Safety Order
- 11.3 Burn Gauge and Treasury Buybacks
- 11.4 PRML EIP-1559 Fee Model
- 11.5 Long-Run Issuance and Net Supply
- 11.6 Plain-Language Summary

12. Security and Auditing (Controls and Observability)
- 12.1 Control Surfaces and Mandatory Invariants
- 12.2 Monitoring and Public Observability
- 12.3 Audit Domains and Evidence Artifacts
- 12.4 Incident Response and Recovery
- 12.5 Key Management and Operational Separation
- 12.6 Migration Verification and Exit Tests
- 12.7 Formal Checks and Machine-Readable Attestations
- 12.8 Plain-Language Summary

13. References and Appendices
- 13.1 References
- 13.2 Variables and Master Tables
- 13.3 Appendix A – Formulas and Identities
- 13.4 Appendix B – Glossary of Terms
- 13.5 Appendix C – Tables and Diagram Identifiers
- 13.6 Plain-Language Summary
- 13.7 Document Status and Parameter Finalization

Abstract

PrimeLayer is a Bitcoin-anchored zkEVM Layer 2 that makes BTC productive without custodial risk. The system anchors state to Bitcoin via AuxPoW merge-mined tag commitments on a Bitcoin-aligned sidechain substrate. Today this substrate is provided by an AuxPoW chain, and the design retains a clean cutover path so no single substrate is a point of failure. PrimeLayer

avoids competing for scarce Bitcoin blockspace and instead commits succinct state under the hashpower umbrella, combining Bitcoin-anchored security with Ethereum-class programmability.

The validator architecture is separated into two specialized groups: Hardware Validators (HVs) produce and attest L2 blocks, while Network Validators (NVs) provide economic finality and govern parameters. Emissions follow a fixed-plus-governed split: a predictable infrastructure slice funds essential hardware production, while bicameral governance directs the majority through two buckets (Bucket A and Bucket B). Bitcoin holders participate from day one through vote-escrowed Bitcoin (veBTC), which is minted by locking PBTC (PrimeLayer's native wrapped-Bitcoin token). veBTC confers voting power over liquidity and revenue distribution, passive yield through the BTC Vault, and optional binding of veBTC to HV identities for slower vote-decay and aligned revenue sharing.

PrimeLayer's ethos is conservative on trust and progressive on usability: non-custodial BTC yield, permissionless liquidity, bounded monetary change, auditable governance, and battle-tested migration protocols for continuity across substrates and DA layers.

---

1. Overview and Motivation

1.1 Terminology

This section defines terminology and abbreviations used throughout the specification. Terms are intentionally precise so that subsequent sections can reference them without ambiguity.

Term	**Abbrev.**	**Definition**
Gauge	—	A weighted emissions bucket that directs new token issuance to specific purposes (e.g., Validators, Builders, Liquidity). The proportion of emissions each gauge receives is determined by validator vePRML voting.
Hardware Validator	HV	Validator with attested hardware that sequences transactions, proposes blocks, and participates in builder and attester committees. Eligible for the

Term	Abbrev.	Definition
		fixed per-block HV emission. Votes in governance via ve-positions like any participant. See Section 6 for more details on different types of yield and rewards validators can earn for network participation.
Network Validator	NV	Validator that performs verification, economic finality, and governance committee work. Votes in governance via ve-positions. NV rewards are routed from governance buckets rather than the fixed HV stream. See Section 6 for more details on different types of yield and rewards validators can earn for network participation.
Identity NFT	—	Soulbound identifier for a validator or governance participant. Aggregates ve-positions for quadratic weighting, carries reputation signals, and enforces per-entity caps in cohort selection.
Bond NFT	—	Transferable record of a delegated capital position to an HV or NV. Encodes class, size, term, and policy flags without transferring Identity.
vote-escrowed PRML	vePRML	Time-locked governance power derived from PRML. Votes in Bucket A and Bucket B per the authority map.

Term	Abbrev.	Definition
vote-escrowed BTC	veBTC	Time-locked governance power derived from PBTC. Votes in Bucket A only. Available from genesis once PBTC is locked.
veBTC binding	—	Optional association of a veBTC position with an HV Identity for benefits such as slower voting power decay and negotiated revenue sharing.
Auxiliary Proof-of-Work anchoring	AuxPoW	Settlement anchoring method that commits succinct L2 state to Bitcoin using merge-mined tag (See Section 14.1, #4 & #5) commitments on a compatible substrate.
Finality Anchor Commitment	FAC	Compact, per-epoch commitment that binds the aggregate HV signatures, the recursive zk-proof reference, and state metadata. Posted via AuxPoW merge-mined tags. The consistency and safety of the BTC bridge only required a single honest miner or honest minority hashrate to maintain its security which is a first of its kind solution for the BTC space.
Edgechain Verification Layer	—	Coordination layer that maintains validator registries, collects NV receipts and ΣHV aggregates, and prepares FACs for anchoring.

Term	Abbrev.	Definition
Builder Funding Proposal	BFP	A proposal for builder grants. Approved BFPs create vesting streams funded first from the Builder Gauge and secondarily from the DAO Treasury if needed.
Monetary Policy Proposal	MPP	Standard governance proposal for non-emergency parameter and program changes within pre-set bounds.
Treasury Parameter Proposal	TPP	Monthly governance mechanism that adjusts DAO financial parameters such as the BTC Vault share, rebase rates, and recycle ratios.
Emergency Monetary Policy Proposal	EMPP	Time-boxed, higher-threshold proposal class for constrained emergency actions such as limited Backstop deployment or oracle failover.
Veto Committee	VC	Standing safety layer with authority to block new or materially altered gauges during warm-up when explicit risk criteria are met. Defensive only.
Cohort Policy Initiative	CPI	Bounded, NV-led policy surface for HV cohort sizing, weights, and diversity caps within top-level thresholds approved by MPP.
Protocol-owned liquidity	POL	Treasury-owned LP positions that may participate in gauges under transparency and guardrail rules.

Term	Abbrev.	Definition
Backstop Vault	—	Reserve funded from the fixed emission slice. Deployable only through EMPP within strict caps and with replenishment priority.
BTC Vault	—	PBTC vault that receives a governed share of protocol revenue and distributes it pro-rata to PBTC depositors. Bucket A controls its parameters.
pUSD	—	Over-collateralized stablecoin primarily backed by PBTC with conservative liquidation, oracle redundancy, and crisis tooling.
Composability	—	As new successful DApps create their own ecosystems, liquidity is not fragmented but shared within the ecosystem through a shared gateway that settles the edgechain proofs in a batch, allowing for interoperability.

1.2 The Case for Bitcoin-Anchored Programmability

Bitcoin is the world's most secure settlement layer, but it was not designed to host high-throughput programmable finance. PrimeLayer brings programmability to Bitcoin without eroding its trust model by anchoring L2 state with AuxPoW merge-mined tags and executing smart contracts in a zkEVM. This preserves Bitcoin-aligned security while enabling modern DeFi primitives, DAO governance, and on-chain markets. The result is programmable finance that inherits Bitcoin's neutrality, hashpower, durability, and auditability.

1.3 The Problem with Blockspace Competition

Most Bitcoin L2s today directly compete for Bitcoin blockspace for settlement, which is both costly and brittle. It forces economic activity into the L1 mempool, amplifies fee volatility, and crowds out unrelated settlement. PrimeLayer avoids this by committing aggregated state under

merge-mined tag commitments rather than emitting full transactional detail to Bitcoin. This achieves verifiable anchoring without turning the L1 into an application bus, and it allows growth without bidding wars for blockspace.

1.4 Vision of a Hyper-bitcoinized Economy

In a hyper-bitcoinized world, BTC functions as the reserve asset backing credit, liquidity, and settlement. PrimeLayer's vision is to make BTC both sovereign and productive: BTC stays under a Bitcoin-anchored security umbrella while earning non-custodial yield and steering resource allocation. Institutions can hold PBTC – PrimeLayer's native wrapped Bitcoin token – to earn protocol revenue from the BTC Vault, and participate in governance through vote-escrowed BTC (veBTC) without surrendering keys to custodians or relying on opaque wrappers. Liquidity, market-making, and stable value emerge around BTC-denominated rails, with the protocol's gauges and bicameral governance allocating emissions and revenues toward the most valuable activity. This maintains Bitcoin's monetary primacy while enabling the financial expressivity demanded by modern markets.

1.5 Liquidity Incentives and Long-Term Economic Sustainability as a Core Principle

Unlike other protocols that rely on emissions-only to incentivize participation and sustainability, or DEX protocols that rely solely on fees extracted from DEX activity to support long-term sustainability, PrimeLayer differentiates itself in several ways to ensure long-term sustainability via multiple demand sinks and yield opportunities for network validators. Because PrimeLayer implements these concepts at a protocol level, the design affords the ability to support multiple sinks which serve as a deflationary mechanism, creating long-term economics very similar to Bitcoin.

Liquidity is a first principle of the protocol – creating long term incentives for expansion of the protocol in a sustainable way that transitions from emissions-only to eventually creating a self-serving emissions engine driven by real, protocol-generated revenue derived from multiple sources. Unlike other protocols, PrimeLayer creates multiple demand sinks that drive deflationary economics while also creating revenue generation opportunities at a protocol level that stem from a variety of sources that are all protocol-native. When coupling these concepts with the lockup mechanics and voting rights associated with locking up PRML or PBTC on the protocol, this creates a system that is self-sustaining over the long term.

1.6 PrimeLayer Objectives and Ethos

- **Security first:** Anchor state succinctly to Bitcoin using AuxPoW merge-mined tags. Keep L1 load minimal and verifiable.

- **No custodial yield:** BTC earns through protocol revenues and measured emissions, not through rehypothecation or trusted wrappers.

- **Clear separation of roles:** HVs build and attest blocks. NVs enforce economic finality and govern parameters.

- **Monetary boundedness:** A predictable infrastructure slice plus community-directed buckets reduce arbitrary issuance and create a path to sustainable, fee-driven yield.

- **Upgradeability without trust creep:** Type I-III migration protocols preserve user positions and system invariants across substrate or DA changes.

1.6 Economic Participation and Non-Custodial Yield

PrimeLayer offers two complementary participation paths anchored in Bitcoin:

- **veBTC – day-one governance and revenue influence:** Lock PBTC to mint veBTC and vote on the allocation of Bucket A: liquidity gauges, BTC Vault revenue share, and related levers earning them yield in a variety of tokens including direct PBTC, PRML, and tokens offered through bribe market participation (See Section 8 for more details). Binding veBTC to a Hardware Validator identity is optional, market-based, and beneficial: it slows voting power decay for the veBTC holder and shares HV-side revenue at a declared rate. HV identities compete for veBTC bonding by publishing revenue shares and performance, creating a transparent market that aligns BTC capital with high-quality block production.

- **BTC Vault – passive BTC yield from protocol revenues:** Deposit PBTC to receive a pro-rata stream of real protocol revenues when Vault conditions are met and active. This allows conservative holders to remain passive while still participating in upside as network usage grows.

- **vePRML – infrastructure and policy stewardship:** Lock PRML to vote across both buckets where appropriate, fund infrastructure, steer validator rewards, and govern treasury operations. Validators earn rewards both in native PRML, as PBTC from DAO Revenue and from participation in the bribe marketplace and various other sources based on how their voting power is allocated across the gauges system. HVs receive a direct cut of emissions for supporting network security on top of the rewards already available to NVs (see Section 6 for more details). HVs and NVs both participate in governance. The infrastructure slice provides predictable support for hardware operations, while bucket voting balances near-term liquidity needs with long-term sustainability.

Economic integrity is reinforced by operational rules that reward correctness and penalize waste. If an HV cohort produces an invalid block, the per-block subsidy is not paid and rolls forward to the next valid block, with the deferred amount split 50 percent to DAO revenue and 50 percent burned. This yields negative carry-on faults, aligning incentives for high-quality block production. Early liquidity is supported through gauge warm-ups and a 15 percent retroactive

early-LP bonus upon activation, while escrow accrued during a warm-up that ends in veto accrues to the DAO.

1.8 Plain-Language Summary

- PrimeLayer adds smart contracts to Bitcoin without asking Bitcoin to change.
- It anchors L2 state using merge-mined tags so the system inherits Bitcoin's security.
- Hardware Validators make the blocks. Network Validators provide finality and governance.
- Bitcoin holders can earn non-custodial yield: lock PBTC for veBTC voting or deposit PBTC in the BTC Vault to share protocol revenues.
- veBTC can bind to specific HV identities. HVs publish revenue shares, and veBTC holders who bind get slower vote-decay and aligned yield.
- Emissions are bounded and mostly directed by governance across two buckets. Rebasing is not part of this design.
- The protocol includes migration procedures so it can move to new anchoring or DA while preserving user positions.

---

2. Core Components

This section defines the roles, artifacts, and governance primitives used throughout the specification.

2.1 Gauges, Buckets, and Emission Directionality

2.1.1 Emission strata

PrimeLayer separates issuance into one fixed stratum and two governed strata.

- **Fixed allocation**: deterministic infrastructure funding is reserved for each epoch. Includes the per-block HV reward, Builder Grants envelope, and Backstop Vault envelope.

- **Governed allocation**: two buckets that route programmatic funding by on-chain vote.

Stratum	Share of epoch emission	Scope	Governance lane
Fixed allocation	25 percent	HV per-block reward, Builders, Backstop Vault	Immutable shares for HV; MPP ranges for Builders and Backstop within the 5 percent envelope.
Bucket A	37.5 percent	Liquidity programs, BTC Vault revenue, bribes routing	Bicameral vote: veBTC 50 percent, vePRML 50 percent.
Bucket B	37.5 percent	NV rewards, infrastructure programs, Treasury programs, Burn and Buyback gauges	vePRML only.

2.1.2 House weighting and vote aggregation in Bucket A

Votes in Bucket A are tallied within each house, then combined with an equal 50-to-50 weight. Within each house, voting power is aggregated per Identity NFT and transformed by a quadratic function to reduce dominance. Per-gauge voter caps limit concentration.

2.1.3 Gauge lifecycle, warm-up, and early liquidity signals

New gauges and materially altered gauges enter a **14-day warm-up**:

1. **Proposal**: anyone may propose a gauge with program metadata and risk notes.

2. **Warm-up escrow**: notional emissions are escrowed per epoch and do not stream to LPs during warm-up.

3. **Early-LP bonus window**: if the gauge activates, LP positions in the first 14 days after activation receive a **15 percent** emission boost.

4. **Activation or veto**: if activation criteria are met and no valid veto is filed, the gauge activates and **escrow is paid retroactively** to voters who supported it during warm-up using per-epoch vote snapshots. If vetoed, **100 percent of escrow routes to DAO revenue**.

2.1.4 Gauge catalog

- **Liquidity gauges**: route emissions to LP positions. PRML-paired pools may receive an amplification factor to deepen PRML routes without mandating them.
- **NV reward gauges**: route Bucket B emissions to NV-focused programs.
- **Builders and audits**: funded either from the fixed Builders envelope or Bucket B programs.
- **Burn gauge**: destroys PRML per vote within defined caps after all safety checks.
- **Buyback gauge**: authorizes Treasury buybacks that either retire PRML or warehouse it with transparent reporting.

2.2 Identity, Escrowed Voting Power, and Binding

2.2.1 Identity NFT and quadratic aggregation

An Identity NFT represents a participant or validator entity. All ve-positions bound to that identity are aggregated before applying quadratic weighting for vote calculations. This curbs vote concentration while preserving proportional influence for larger, long-duration locks.

2.2.2 vePRML and veBTC

- **vePRML**: time-locked PRML that confers voting rights in both buckets according to the authority map.
- **veBTC**: time-locked PBTC that confers voting rights in Bucket A. veBTC is available from genesis and requires no activation vote.

2.2.3 Binding veBTC to HV Identity

A veBTC holder may opt to bind a veBTC position to a specific HV Identity to align capital with high-quality hardware operation.

- **Benefits to veBTC holder**: voting power decays at half the standard rate while the binding is active and the HV remains in good standing.
- **Benefits to HV operator**: may advertise a transparent revenue share for delegated bindings, attracting veBTC capital.

- **Market discipline**: HVs publish their binding terms and performance metrics, creating a marketplace where veBTC seeks reliable operators. Capacity caps and cooldowns deter rapid rebinding churn.

Binding affects decay and, where defined, program multipliers. It does not change which domains a participant may vote in.

2.3 Committees, Sortition, and Quorums

2.3.1 Per-block HV cohort

Each block selects an HV **proposer**, a **builder committee**, and an **attester committee** using verifiable randomness. Selection weights incorporate stake, lock duration multiplier, hardware performance indicators, governance reputation, and diversity caps by operator and region. This reduces cartel risks and improves geographic and organizational dispersion.

- **Proposer**: sequences transactions into the candidate block and collects priority tips.
- **Builder committee**: competes to construct optimized blocks for the proposer.
- **Attester committee**: verifies correctness and participates in ΣHV aggregation.

2.3.2 NV functions and CPI scope

NVs provide verification receipts, participate in economic finality, and drive CPI proposals that tune cohort sizing, coefficient ranges, and dispersion caps within upper and lower bounds approved by MPP. This separates rapid, operational tuning from constitutional parameters.

2.3.3 Governance proposal classes and safety layers

- **MPP**: standard changes to parameters and programs within defined bounds.
- **EMPP**: constrained emergency actions with higher quorum and approval, strict scopes, and post-action audits.
- **Veto Committee**: defensive authority to block risky gauge activations during warm-up when explicit criteria are met. Vetoes are logged with reason codes and evidence.

2.4 Plain-Language Summary

- There are two kinds of validators. Hardware Validators run the heavy machines that make blocks, and Network Validators double-check results and help run governance. Both can vote, as long as they hold the right voting locks.
- Emissions are split into a fixed slice for core needs and two governed buckets. Liquidity and the BTC Vault are decided by both veBTC and vePRML together. Infrastructure and validator programs are decided by vePRML.
- New incentive programs go through a short waiting period. If a program activates, early supporters and voters get paid from the escrow that built up during the wait. If it is blocked for safety reasons, the escrow goes to the DAO.
- People who lock PBTC get veBTC voting power right away. They can optionally bind their voting power to a specific Hardware Validator to slow the voting power decay and share in that validator's success.
- Every block uses a small, randomly chosen group of Hardware Validators to propose, build, and attest. This spreads out power and makes the network harder to capture.

3.9 Plain-Language Summary

- Each epoch the system computes how many new tokens to create. A fixed slice always pays for hardware, builders, and an emergency reserve. The rest is split into two buckets that are directed by on-chain votes.
- Hardware Validators are selected by a weighted lottery to propose, build, and attest blocks. If they miss or produce a bad block, that block's reward is not paid. The withheld amount is held until the next good block, then half is burned and half goes to the DAO, and the pool is reset.
- Liquidity and the BTC Vault are decided together by veBTC and vePRML voters. Infrastructure and validator programs are decided by vePRML voters. New programs wait 14 days before paying out so safety checks can run. If a program activates, early voters and early LPs are rewarded; if it is vetoed, the held funds go to the DAO.
- BTC holders can lock PBTC to get veBTC and vote in Bucket A from day one. They can optionally bind veBTC to a specific Hardware Validator to slow the voting power decay and share in that validator's success.
- The stablecoin aims to stay healthy using conservative collateral ratios, liquidation rules, and redundant oracles. Emergency actions have higher voting thresholds and are time-limited.
- If the anchoring or data-availability layer needs to change, both the old and new paths run in parallel for a time, a checkpoint links them, and a unified index keeps everything easy to verify.

---

3. System Architecture – Components and Interactions

This section specifies components, trust boundaries, end-to-end data and value flows, emission and fee accounting identities, and containment mechanisms that limit blast radius during fault or migration events. Notation follows Section 3.

3.1 Subsystems and Trust Boundaries

3.1.1 Components

Subsystem	**Role**	**Primary artifacts**	**Trust boundary**	**Principal risks**	**Containments**
Bitcoin L1	Settlement root and public audit anchor	Block headers, PoW chain	External – trust in Bitcoin consensus	Short reorgs; delayed inclusion	Confirmation depth policy; anchor SLO tau_anchor
AuxPoW substrate	Merge-mined tag carrier for anchors	Merge-mined tag with FAC pointer	External – trust-minimized by overlap	Anchoring endpoint instability	Overlap N_overlap; cross-binding checkpoint chi_checkpoint; unified index I_index
Edgechain verification layer	Registry and anchor preparation	Validator registry root, NV receipts, Sigma_HV, FAC metadata	Internal – quorum based	Liveness shortfall; miscoordination	CPI tuning; cohort reselection; safety mode tau_safety
Execution - zkEVM	Deterministic state with succinct proofs	Blocks B_i, recursive proof pi_epoch	Internal – proof soundness	Prover stalls, latency spikes	Alternate provers; batching; epoch rollover

Subsystem	Role	Primary artifacts	Trust boundary	Principal risks	Containments
Validator layer	Block production and finality	HV proposer, builder committee, attester committee	Internal – threshold honesty	Invalid or missed blocks	Withheld-subsidy rule; Sigma_withheld; slashing; selection penalties
Governance layer	Parameterization and programs	MPP, EMPP, VC actions	Internal – bicameral checks	Capture attempts, oscillation	Quorums; thresholds; cooldown tau_cool; veto scope; Omega_veto.
DEX and gauges	Liquidity routing and emissions	Gauge configs, epoch snapshots	Internal – rule based	Misconfiguration, spam	Warm-up T_warmup; escrow E_escrow; veto to DAO; rho_escrow_veto
BTC Vault	PBTC revenue distribution	Vault shares, conversion ledger	Internal – policy based	Revenue volatility	Activation tau_vault_act; pause tau_vault_pause;
pUSD subsystem	Over-collateralized stablecoin	CR, auctions, oracle set	Internal – rule based	Oracle faults, liquidity gaps	Delta_oracle; tau_oracle; Gamma_EMPP; Backstop envelope.
Bridge connectors	Asset and message transport	Proof verifiers, timelocks	Mixed – proof-first design	Route stall or committee failure	Timeouts; challenges; staged deprecation
Observability	Transparency and audit	Dashboards, logs, attestations	Public	Telemetry blind spots	On-chain evidence bundles; public archives

3.1.2 Minimal trust stance

- Settlement anchoring uses merge-mined tag commitments on a compatible AuxPoW substrate so that Bitcoin remains the sole ultimate root. No single operator or lane is a critical dependency due to required overlap and cross-binding at cutover.
- Internal correctness is enforced by proofs and quorums. Incentives, slashing, and reward withholding discourage deviations. All exceptional actions are bounded by EMPP scope and produce verifiable evidence.

3.2 End-to-End Data and Value Flows

3.2.1 Execution and anchoring

1. **Transaction ingress** – users submit transactions to the execution mempool.

2. **HV assembly** – the selected proposer sequences transactions; the builder committee constructs candidate blocks; the attester committee validates.

3. **Proofing** – per-block proofs pi_i are aggregated into pi_epoch.

4. **NV verification and Sigma_HV** – NVs verify pi_epoch and emit receipts; HV attesters aggregate Sigma_HV for the epoch.

5. **FAC formation** – Edgechain binds state root, pi_epoch reference, Sigma_HV, and metadata M_epoch into the FAC.

6. **Anchor commit** – FAC is posted via merge-mined tag on the AuxPoW substrate. Observers read the tag from Bitcoin, fetch FAC, and validate pi_epoch and Sigma_HV.

3.2.2 Emission allocation

Per epoch t:

1. Compute E_epoch(t).
2. Reserve fixed slice S_fixed: HV per-block stream S_HV, Builders S_Build, Backstop S_Backstop.
3. Allocate Bucket A and Bucket B using within-house votes and the Bucket A house weights w_A = [0.5 veBTC, 0.5 vePRML].
4. Enforce validator floor V_floor across S_HV + NV distributions from Bucket B.
5. Apply gauge warm-up and safety interlocks – escrow E_escrow for warming gauges; withhold streaming until activation; if vetoed, route escrow to DAO.
6. Stream per-gauge emissions to recipients subject to caps and routing multipliers.

3.2.3 DAO revenue routing

Sources include:

- Gas base-fee routing per policy, priority tips excluded.
- DEX protocol fees not redirected to staked LP voters.
- Liquidation penalties and redemption fees from pUSD.
- Bridge connector fees.
- Withheld-subsidy release – when a valid block follows one or more invalid or missed slots, release Sigma_withheld as psi_DAO to DAO and psi_burn to burn.
- Veto disposition – escrow from vetoed warm-up gauges routed 100 percent to DAO.

Destinations include:

- Treasury programs in Bucket B.
- BTC Vault share alpha_vault in Bucket A after conversion rho_vault_fees to PBTC.
- Buyback and Burn gauges per allocation.

3.2.4 DEX and gauge streaming

- Staked LPs – receive emissions and fee redirection proportional to gauge vote snapshots and stake.
- Unstaked LPs – retain collected trading fees but receive no emissions.
- PRML-paired pools – may receive alpha_PRML amplification per policy, never bypassing validator or backstop invariants.

3.3 Accounting Identities and Safety Rules

3.3.1 Per-epoch allocation identity

Let E_epoch(t) be the epoch emission, then:

E_epoch(t) = E_fixed(t) + E_A(t) + E_B(t)

with

E_fixed(t) = S_HV(t) + S_Build(t) + S_Backstop(t) E_A(t) = S_A * E_epoch(t) E_B(t) = S_B * E_epoch(t)

Ordering and checks:

1. Reserve E_fixed(t) first.
2. Compute E_A(t), E_B(t).
3. Enforce validator floor – ensure S_HV(t) + NV_from_B(t) >= V_floor * E_epoch(t). If not, reallocate within Bucket B to validator distributions until satisfied.

4. Apply warm-up and veto logic before streaming.

3.3.2 Withheld-subsidy rule

For each block slot:

- If valid: pay E_block per cohort split (theta_P, theta_B, theta_A).
- If invalid or missed: Sigma_withheld := Sigma_withheld + E_block; cohort receives nothing.
- On the next valid block: send psi_burn * Sigma_withheld to burn and psi_DAO * Sigma_withheld to DAO revenue; set Sigma_withheld := 0; then pay the current E_block per cohort split.

3.3.3 DAO revenue and net issuance identities

DAO revenue per epoch t:

R_DAO(t) = R_gas(t) + R_dex(t) + R_liq(t) + R_bridge(t) + psi_DAO * Sigma_withheld(t_release) + R_veto(t)

Net issuance per epoch t:

E_net(t) = E_epoch(t) - B_total(t)

where B_total(t) includes Burn gauge output plus any withheld-release burn psi_burn * Sigma_withheld(t_release). Buyback-and-burn reduces circulating supply but does not change E_epoch(t).

3.4 Modularity and Fault Containment

3.4.1 Anchor and DA migrations

- Overlap – run old and new paths concurrently for N_overlap epochs.
- Cross-binding – publish a final overlap FAC that binds the last-old anchor to the first-new anchor using chi_checkpoint.
- Unified index – expose I_index for clients; post-cutover, the old path remains read-only for retrieval window R_retrieval.

3.4.2 Safety mode and EMPP

- Safety mode clamps parameters and freezes risky surfaces for tau_safety after approved triggers.

- EMPP actions are limited to a predefined set, require higher quorum and approval, are time-boxed, and produce on-chain post-action audits.

3.4.3 Connector containment

- Proof-first verification is preferred; interim committees use timelocks and challenges.
- Stalled routes revert to safing states through timeouts and challenge outcomes, preventing asset lock-in.

3.4.4 Oracle containment

- Medianization with deviation bound delta_oracle and heartbeat tau_oracle.
- Breaches cause automatic freezes on sensitive paths and may qualify for EMPP stabilization.

3.4.5 Gauge containment

- New or materially altered gauges must pass warm-up and VC review before streaming.
- On veto, escrow disposition is rho_escrow_veto to DAO; on activation, escrow is paid retroactively to warm-up voters by snapshot.

3.5 Plain-Language Summary

- Every epoch ends with a compact record posted to Bitcoin that proves the state updates were valid. This record is small and easy to verify.
- Hardware Validators make blocks in small, randomly chosen groups. If they miss or submit a bad block, that block's reward is held back. When the next good block arrives, half of the held amount is burned and half goes to the DAO.
- New tokens are divided into a fixed part for running the network and two voted parts. Liquidity and the BTC Vault are decided by both veBTC and vePRML together. Infrastructure and validator programs are decided by vePRML.
- New programs spend two weeks in a waiting period. If approved, the escrow from that period is paid back to early voters, and early liquidity gets a short bonus. If a program is vetoed, that escrow goes to the DAO instead.
- The system can change its anchoring or data provider without stopping. Both old and new run in parallel for a while, a special checkpoint links them, and a single index keeps everything consistent for users and explorers.

---

4. Validator Economy NV, HV, vePRML, veBTC, Bond NFTs

This section specifies validator roles, selection and reward mechanics, governance parity, identity and delegation artifacts, and fault handling. Notation and symbols match Section 3.

4.1 Roles and Responsibilities

Hardware Validator (HV). Runs attested hardware, sequences transactions, proposes blocks, participates in builder and attester committees, and aggregates signatures. Receives the per-block infrastructure reward from the fixed slice S_HV. Holds governance rights through vePRML and, where applicable, veBTC like any participant.

Network Validator (NV). Verifies proofs, emits verification receipts, participates in CPI policy, finality, and governance committees. NV rewards are routed from Bucket B programs; NVs do not share in the per-block HV stream by default.

Governance parity. Voting rights are determined by ve-positions, not validator class. Any identity holding vePRML participates in Bucket A and Bucket B per their authority, and any identity holding veBTC participates in Bucket A via w_A = [0.5 veBTC, 0.5 vePRML].

4.2 HV Cohort Selection and Sortition

Each block selects a proposer, a builder committee of size b, and an attester committee of size a by verifiable randomness. The selection weight for HV i is:

W_i = f(stake_i, M_dur_i, HardwareScore_i, GovernanceScore_i, history_i),

subject to anti-concentration:

- cap_entity = 20% maximum of a cohort that any single operator may hold,
- cap_region = 30% maximum of a cohort from any single region.

CPI proposals set coefficient ranges for f(.) and the bounds for a, b, cap_entity, cap_region within top-level policy.

Committee roles

- **Proposer:** sequences and finalizes the winning block; receives priority tips.

- **Builder committee:** supplies optimized block candidates.
- **Attester committee:** validates the block; participates in Sigma_HV aggregation.

4.3 NV Finality and Governance

NVs verify pi_epoch, issue signed receipts to the Edgechain verification layer, and staff governance and risk committees. CPI scope includes adjusting a and b within bounds, setting per-entity and per-region caps, and tuning coefficient corridors for f(.). NVs participate in Bucket B leadership and, with vePRML, in Bucket A per w_A.

4.4 Identity and Bond NFTs

Identity NFT. A soulbound identifier used to aggregate ve-positions for quadratic weighting, carry validator reputation and slashing history, and enforce anti-concentration in sortition.

Bond NFT. A transferable delegation record that binds capital to an HV or NV without transferring Identity. Fields include class, size, M_dur, and policy flags. Redelegation preserves Identity and reputation continuity while moving capital support.

veBTC binding (optional). A veBTC position may bind to an HV Identity to align capital with operator quality:

- Voting decay slows to delta_bind = 0.5 * delta_base while the binding is valid and the HV is in good standing.
- An HV may advertise rho_HV (for example 5% to 15%) as the revenue share required for delegated bindings; k_bind caps bound volume; tau_rebind enforces a cooldown after unbinding.
- Binding affects decay and any program multipliers where defined. It does not expand voting domains beyond Bucket A for veBTC.

4.5 Rewards, Slashing, and Reputation

4.5.1 Per-block HV reward

Let E_block be the nominal HV reward unit for a block derived from S_HV and E_epoch. If a block is valid, split E_block by the policy vector (theta_P, theta_B, theta_A) with sum(theta) = 1:

- Proposer share: theta_P * E_block
- Builder committee share: theta_B * E_block (split per builder rules)

- Attester committee share: theta_A * E_block (split among attesters)

Priority tips are paid to the proposer and are not part of E_block.

4.5.2 Withheld-subsidy rule

If a block is invalid or missed:

- Do not pay E_block to the cohort.
- Add E_block to Sigma_withheld.

When the next valid block lands:

- Burn psi_burn * Sigma_withheld and route psi_DAO * Sigma_withheld to DAO revenue,
- Set Sigma_withheld = 0,
- Then pay the current E_block by (theta_P, theta_B, theta_A).

This enforces negative carry on faults while preserving emission accounting.

4.5.3 Validator floor and NV distributions

Per epoch, enforce:

S_HV + NV_from_B >= V_floor * E_epoch,

where NV_from_B denotes Bucket B distributions earmarked for NV programs and validator support. If the inequality is not met, reallocate within Bucket B to validator programs until it holds, before any gauge streaming.

4.5.4 Slashing and penalties

- **Safety faults.** Double-signing, fraud-equivalent evidence. Penalties include stake slash, exclusion from cohorts for a defined window, and reputation impact on W_i.

- **Liveness faults.** Chronic failure to meet U_rho. Penalties include reduced W_i, temporary loss of cohort eligibility, and reduced reward multipliers where defined.

- **Binding impacts.** When an HV is slashed beyond a threshold, bound veBTC loses binding benefits until the holder unbinds or the HV regains good standing. rho_HV applies only while binding is active.

4.5.5 Reputation surfaces

HardwareScore and GovernanceScore are updated by uptime, attestation quality, response latency, proposal participation, and incident history. These scores feed W_i and may modulate reward multipliers within policy bounds.

4.6 Plain-Language Summary

- There are two validator roles. Hardware Validators make blocks and get a fixed reward per block. Network Validators help confirm results and shape policy. Both can vote if they hold the right governance locks.
- Each block picks a small set of Hardware Validators at random to propose, build, and attest. This spreads out power.
- If a block is bad or missed, the reward for that block is held back. When the next good block arrives, half of the held amount is burned and half goes to the DAO, and the pool is reset.
- A strict rule makes sure validators as a group get at least half of all emissions when you add the fixed block rewards and the programs funded for validators.
- Voting power can come from PRML locks or PBTC locks. PBTC voters can also choose to bind to a specific Hardware Validator. Binding slows vote decay and can share in that validator's success, but it does not change where the voter is allowed to vote.
- Delegations are handled by Bond NFTs so capital can move without losing identity or reputation history.

---

5. Emission Allocation and Distribution

This section formalizes the per-epoch allocation sequence, the fixed infrastructure slice, the two governed buckets, vote aggregation and weighting, streaming semantics, and the safety interlocks that precede any distribution. Notation and symbols follow Section 3.

5.1 Fixed Allocations vs Governance-Directed Buckets

5.1.1 Allocation order per epoch t

1. Compute epoch emission E_epoch(t) using the path in Section 13.2.

2. Reserve fixed slice E_fixed(t) = S_HV(t) + S_Build(t) + S_Backstop(t).

3. Compute governed shares E_A(t) = S_A * E_epoch(t), E_B(t) = S_B * E_epoch(t).

4. Enforce validator floor Ensure S_HV(t) + NV_from_B(t) ≥ V_floor * E_epoch(t). If not satisfied, reallocate within Bucket B toward validator support until the inequality holds.

5. Apply gauge lifecycle and safety interlocks Warm-up T_warmup, escrow E_escrow, VC veto window, per-gauge caps and identity weighting.

6. Stream per-gauge emissions Release to eligible recipients according to epoch snapshots, after all checks and only for activated gauges.

5.1.2 Fixed allocation (infrastructure)

Envelope	Symbol	Share of total	Governance	Purpose
HV per-block reward	S_HV	20%	Constitutional	Pays HV proposer; builder; attester. committees per slot via E_block and theta vector.
Builders	S_Build	2% to 4%	MPP within [2,4]	Client maintenance; audits; tooling; core R&D.
Backstop Vault	S_Backstop	1% to 3%	MPP within [1,3]	Crisis liquidity and stability interventions; EMPP-gated and replenishment-prioritized.

Notes • S_Build + S_Backstop = 5% of total. • HV rewards are an infrastructure bonus for running hardware; they do not reduce governance rights nor directly fund Bucket programs.

5.2 Bucket A – Liquidity and BTC Vault

5.2.1 Scope and house composition

- **Scope:** liquidity gauges, PRML-paired pool incentives, BTC Vault revenue share, bribe routing to voters.

- **House composition**: votes combined as w_A = [0.5 veBTC, 0.5 vePRML] after within-house aggregation.

5.2.2 Within-house aggregation and quadratic weighting

For each house H ∈ {veBTC, vePRML}:

- Aggregate all ve positions bound to the same Identity NFT.
- Apply quadratic weighting: weight_i(H) = (power_i(H))^(alpha_bound) for bound identities and (power_i(H))^(alpha_unbound) for unbound positions.
- Enforce per-voter per-gauge cap: no voter may assign more than cap_gauge of total voting power to a single gauge.

- House total for a gauge g: W_H(g) = sum over identities of weight_i(H, g).

Combined score: W_A(g) = 0.5 * W_veBTC(g) + 0.5 * W_vePRML(g).

Per-gauge share in Bucket A: share_A(g) = W_A(g) / sum over all gauges in A of W_A(.).

5.2.3 PRML-paired amplification and routing rebate

- PRML-paired pools may receive an amplification factor alpha_PRML within MPP bounds.
- Optional routing rebate R_route on PRML-leg volume can be enabled; it does not count toward validator floor enforcement and cannot impair S_Backstop replenishment targets.

5.2.4 BTC Vault distribution

- A governed fraction alpha_vault of DAO revenue is directed to the BTC Vault.
- Revenue conversion follows rho_vault_fees and is distributed to PBTC depositors pro-rata per epoch once tau_vault_act conditions are met.
- Vault may be paused under tau_vault_pause in safety mode or via EMPP within allowed scope.

5.3 Bucket B – Infrastructure, Treasury, Burn and Buyback Gauges

5.3.1 Scope and authority

- **Scope:** NV rewards and validator programs, infrastructure operations, Treasury programs, Burn gauge, Buyback gauge, additional Builders if needed.

- **Authority**: vePRML only; within-house weighting and per-gauge cap rules from 6.2.2 apply.

5.3.2 Validator floor enforcement

Before any Bucket B streaming:

S_HV(t) + NV_from_B(t) ≥ V_floor * E_epoch(t).

If not satisfied, reallocate within Bucket B toward validator programs (NV rewards and necessary support) until the inequality holds. Only after the floor is met may non-validator programs stream.

5.3.3 Burn and Buyback gauges

- **Burn gauge.** Destroys a governed share of Bucket B after all floor and safety checks. Cap B_rate per epoch applies.

- **Buyback gauge.** Authorizes Treasury to purchase PRML subject to K_buy caps and execution rails. Purchased PRML is either retired to the burn sink or warehoused with transparent inventory. Buybacks affect circulating supply but not E_epoch.

5.3.4 Treasury and POL

- Treasury programs and POL must declare targets, caps, and conflict-mitigation rules.
- POL may stake in gauges but is subject to transparency, caps, and warm-up like any participant.

5.4 Early-LP Bonus and Gauge Warm-Up Rules

5.4.1 Warm-up and escrow

- New or materially modified gauges enter warm-up for T_warmup = 14 days.
- During warm-up, notional emissions accumulate in E_escrow per epoch; no streaming to LPs occurs.

5.4.2 Activation and retroactive payouts

- On activation, release E_escrow retroactively to voters who backed the gauge during warm-up, pro-rata to their per-epoch snapshot weights.
- Apply the early-LP bonus beta_early = +15% for LP positions during the first 14 days after activation. This boost is multiplicative on their emission share from the activated gauge.

5.4.3 Veto disposition

- If vetoed during warm-up or review, route 100% of E_escrow to DAO revenue. No payments are made to LPs or voters for that gauge's warm-up period.
- Re-submission requires a new warm-up and fresh voting.

5.4.4 Bribes and delays

- Bribes to gauge voters are permitted within guardrails.
- Bound identities may claim bribes without delay; unbound identities observe a claim delay Delta_bribe.

5.4.5 Safety ordering

Per epoch, for each gauge g:

1. Verify warm-up status and veto outcome.
2. If activated: include g in the streaming set with beta_early applied where eligible.
3. If vetoed: exclude g; add its E_escrow to DAO revenue.

5.5 Plain-Language Summary

- Each epoch starts by deciding how many new tokens to issue, then sets aside a fixed slice for hardware, builders, and an emergency reserve. The rest is split into two buckets that are decided by on-chain votes.
- Bucket A funds liquidity and the BTC Vault. People with veBTC and vePRML each control half of this bucket. Bucket B funds validators and infrastructure and is controlled by vePRML.
- Voting uses identity-aware math so one entity cannot easily dominate. Voters cannot put all their weight on one program.
- New programs wait for two weeks. During that time, the system holds back their potential rewards in an escrow. If the program goes live, the escrow pays back to the voters who supported it, and early LPs get a short bonus. If the program is vetoed, the escrow goes to the DAO.
- A strict rule keeps at least half of all emissions going to validators when you add the fixed hardware rewards and the validator programs in Bucket B.
- PRML-paired pools can get a small boost to encourage healthy routing, and the DAO can run buybacks or burns when it makes sense, all within caps and safety checks.

---

6. DAO Security and Governance Resilience

This section defines the governance surfaces, proposal classes, voting mechanics, warm-up and veto processes, emergency procedures, treasury safety rails, and the evidence and accountability requirements that make changes auditable and bounded. All notation follows Section 3.

6.1 Bicameral Governance Model

6.1.1 Houses and authority

- **House P (vePRML).** Authority over all governance domains, including Bucket B and participation in Bucket A per w_A.

- **House B (veBTC).** Authority only in Bucket A. No authority in Bucket B.

- **Bucket composition.** Bucket A is combined by w_A = [0.5 veBTC, 0.5 vePRML] after within-house aggregation. Bucket B is vePRML-only.

6.1.2 Within-house aggregation and anti-capture controls

- **Identity aggregation.** Voting power is summed across ve-positions bound to the same Identity NFT, then transformed by a quadratic exponent:
    - Bound identities: exponent alpha_bound (default 0.50).
    - Unbound positions: exponent alpha_unbound (default 0.45).

- **Per-gauge cap.** A single voter may not allocate more than cap_gauge of their total effective power to any one gauge.

- **Cooling.** A governance cooldown tau_cool applies after major changes to avoid oscillation.

6.1.3 Quorums, thresholds, and constitutional surfaces

- **Standard changes (MPP).** Quorum Q_MPP per house, approval T_MPP per house. Cross-house composition applies for Bucket A resolutions.

- **Constitutional surfaces.** Changes to S_HV, V_floor, house scopes, or anchor migration semantics require constitutional handling (elevated bounds and explicit audit artifacts). Such changes cannot be enacted by EMPP.

- **Override thresholds.** Where an override is permitted (for example, veto appeal), it uses a strictly higher approval threshold T_override > T_MPP and may require both houses when impacts cross domains.

6.2 Monetary Policy Proposals and Emergency Procedures

6.2.1 Monetary Policy Proposal (MPP)

- **Scope**: Parameter and program changes within published bounds: gauge parameters, Builders and Backstop sub-bands within the fixed 5 percent envelope, alpha_PRML bounds, R_route, alpha_vault, cohort coefficient corridors, oracle bounds (delta_oracle, tau_oracle), and similar.

- **Process:**
    - Submit proposal with rationale, parameter deltas, safety analysis, and monitoring plan.
    - Satisfy Q_MPP and T_MPP in the relevant house(s).
    - Apply tau_cool where applicable.

- **Evidence**: On-chain metadata must include parameter diffs, bound checks, and dashboard links for ex-post monitoring.

6.2.2 Emergency Monetary Policy Proposal (EMPP)

- **Scope (enumerated and narrow):**
    - Backstop release within S_Backstop caps.
    - Oracle failover: freeze minting, switch feeds, adjust delta_oracle and tau_oracle within emergency bounds.
    - Safety mode: temporary clamps on streaming or connector throughput.
    - No authority to alter S_HV, V_floor, house scopes, or constitutional surfaces.

- **Process:**
    - Elevated quorum Q_EMPP and supermajority T_EMPP.
    - Time-boxed effect window; automatic sunset if not re-ratified.
    - Mandatory post-action report with measured impacts and a replenishment plan (for example, Backstop top-up schedule).

- **Guardrails:**
    - Serial EMPP on the same surface escalates thresholds or requires constitutional treatment.
    - All EMPP artifacts are logged on-chain and referenced by FAC metadata for durable audit.

6.3 Veto Committee and Gauge Lifecycle

6.3.1 Veto Committee (VC)

- **Composition and threshold.** Five members, threshold Omega_veto = 4 of 5.

- **Jurisdiction.** Defensive authority during warm-up only. VC may block a new or materially altered gauge if explicit risk criteria are met:
    - Validator floor risk: S_HV + NV_from_B would fall below V_floor.
    - Treasury/Backstop solvency risk: S_Backstop or Builders sub-bands would breach policy corridors.
    - Oracle integrity risk: dependency on a feed outside delta_oracle or heartbeat tau_oracle.
    - Cross-domain encroachment: a gauge that effectively alters house scopes or constitutional surfaces.

- **Transparency.** Each veto must include a reason code, evidence bundle, and recommended remediation.

6.3.2 Gauge lifecycle and outcomes

- **Warm-up.** All new and materially altered gauges enter warm-up for T_warmup. Notional emissions accrue to E_escrow each epoch; no streaming occurs.

- **Activation.** If activation conditions are met and no valid veto is filed, the gauge activates. E_escrow is paid retroactively to warm-up voters using per-epoch snapshots; early-LP bonus beta_early applies to LP positions during the first 14 days after activation.

- **Veto.** If vetoed, E_escrow is routed 100 percent to DAO revenue as rho_escrow_veto. The gauge may be resubmitted, restarting warm-up.

- **Appeal.** Proposers may submit an override MPP with higher approval T_override and Q_MPP per house. If passed, the gauge re-enters warm-up.

6.4 Warm-Up Escrow and Activation Delay

6.4.1 Parameters and identities

- **Warm-up window**: T_warmup = 14 days.

- **Escrow accumulator**: E_escrow per epoch.

- **Disposition**: activation → retro payout to warm-up voters; veto → 100 percent to DAO.

6.4.2 Safety ordering and streaming

Per epoch and per gauge:

1. Check warm-up status and VC outcome.
2. If activated: include in streaming set; apply beta_early to eligible LP positions for 14 days following activation.
3. If vetoed: route E_escrow to DAO; do not stream; clear E_escrow.

6.5 Treasury, Backstop Vault, and Recapture

6.5.1 Treasury transparency

- Budgets and actuals must be published per epoch for Builders, Bucket A, Bucket B, Burn, Buyback, and Vault shares.
- Buyback execution logs must include spend notional, units acquired, average execution price, and final disposition (burn vs warehouse).

6.5.2 Backstop deployment and replenishment

- Backstop draws occur only via EMPP within S_Backstop caps.
- Replenishment has priority in subsequent epochs until coverage targets are restored.
- Post-event audits check that replenishment occurred and that gauges did not impair Backstop recovery.

6.5.3 Recapture and clawback

- If misconfiguration or abuse is demonstrated, DAO may recapture funds from future streams or direct clawbacks via MPP, respecting legal and technical feasibility.
- Veto-reverted E_escrow and certain penalties automatically route to DAO revenue and may be earmarked for Backstop replenishment.

6.6 Plain-Language Summary

- Two houses share power. veBTC and vePRML together control the liquidity bucket, and vePRML alone controls the infrastructure bucket. Voting uses identity-aware math that makes it hard for one whale to dominate.

- Normal changes go through a standard proposal. Emergency changes require higher turnout and support, do less, and expire quickly unless renewed. Every emergency action is logged and reviewed.
- New programs must wait 14 days before paying out. During that time, a Veto Committee can block unsafe programs. If a program goes live, early voters and early liquidity are rewarded. If it is blocked, the set-aside funds go to the DAO.
- The DAO's finances are transparent. The emergency Backstop is tightly controlled and must be refilled after use. If a program misbehaves or was misconfigured, the DAO can claw back future funds.

---

7. BTC Participant Yield Layer – PBTC, veBTC, Gauges, BTC Vault

This section specifies the non-custodial BTC participation path. It defines PBTC bonding and veBTC voting, describes how Bucket A directs liquidity gauges and BTC Vault distributions, formalizes optional veBTC binding to Hardware Validator identities, and adds veBTC participation in the bribe market. All symbols follow Section 3.

7.1 PBTC Bonding and veBTC Mechanics

7.1.1 Bonding flow

1. Deposit BTC into the protocol bonding contract.
2. Mint PBTC at 1:1, held by the user on PrimeLayer.
3. Lock PBTC to mint veBTC with lock duration in [0, tau_lock].
4. Vote in Bucket A with veBTC. Voting is live at genesis.
5. Optionally provide PBTC or PBTC–PRML liquidity and stake LP positions in Bucket A gauges.

No external custodian holds BTC; PBTC is programmatically redeemable subject to standard bridge and settlement rules.

7.1.2 veBTC properties

Property	Symbol(s)	Definition
Lock duration	tau_lock	Maximum lock length; determines duration multiplier M_dur for voting power.
Voting scope	—	Bucket A only; co-governance with vePRML via w_A = [0.5 veBTC, 0.5 vePRML].
Weighting	alpha_bound, alpha_unbound	Identity-aggregated ve transformed by quadratic exponent; bound identities use alpha_bound, unbound use alpha_unbound.
House composition	w_A	Bucket A combines house results equally.
Rebinding cooldown	tau_rebind	Minimum wait time between HV binding changes (see 8.3).

7.1.3 PBTC in liquidity gauges

PBTC can be supplied to liquidity pools and staked into Bucket A gauges. Staked LPs receive:

- Emissions according to epoch snapshots.
- Fee redirection to the voters of the gauge (see Section 6).
- PRML-paired amplification alpha_PRML for PBTC–PRML pools within bounds.

Unstaked LPs retain trading fees but receive no emissions.

7.2 BTC Vault Operation and Yield Policy

7.2.1 Governance lane and purpose

- BTC Vault parameters and distributions are governed in **Bucket A** through the bicameral vote w_A.
- The Vault provides a BTC-denominated, passive yield path to PBTC depositors by streaming a governed share of protocol revenue.

7.2.2 Distribution identity and accounting

Per epoch t:

- DAO revenue is R_DAO(t) (see Section 4).
- Vault share is alpha_vault * R_DAO(t) after conversion per rho_vault_fees to PBTC.
- Per-depositor payout is proportional to the depositor's share of total PBTC deposited at epoch close.

Activation and safety:

- Activation requires tau_vault_act criteria to be met.
- Pause may be invoked under tau_vault_pause or EMPP rules if stress conditions or oracle faults occur.
- The Vault publishes per-epoch ledgers for inflows, conversions, and pro-rata distributions.

7.3 Binding veBTC to HV Identity – Market and Decay Benefits

7.3.1 Binding model

A veBTC position may bind to a specific HV Identity to align governance capital with high-quality hardware operation.

- Decay benefit: bound veBTC uses delta_bind = 0.5 * delta_base while binding is valid and the HV remains in good standing.
- Revenue sharing: an HV may advertise a required share rho_HV (for example 5% to 15%) applied to the veBTC-side yield attributable to the binding relationship.
- Capacity limit: each HV declares k_bind, the maximum veBTC capacity it will accept for binding.

Binding affects decay and, where defined, program multipliers. It does not change voting scope.

7.3.2 Market operation

1. HVs publish offers {rho_HV, k_bind, performance metrics}.
2. veBTC holders select an HV and initiate a binding transaction.
3. Binding becomes effective after standard finality; rebinding requires waiting at least tau_rebind.

7.3.3 Risk and enforcement

If an HV's reputation or hardware performance falls below policy thresholds, or if it is slashed above a defined severity, binding benefits pause. The veBTC holder may unbind and rebind elsewhere after tau_rebind elapses. Binding never expands house authority; it modifies decay only.

7.3.4 Yield composition identity (informative)

For a PBTC participant P in epoch t:

Yield_P(t) = Emissions_share_P(t) + Fee_share_P(t) + Bribe_share_P(t) + Vault_share_P(t) + Binding_share_P(t) − Program_fees_P(t)

where:

- Emissions_share_P(t) is the share from active gauges for staked LP,
- Fee_share_P(t) is redirected trading fees to voters for the chosen gauge,
- Bribe_share_P(t) is the share of bribes eligible to P's voting identity (see 8.4),
- Vault_share_P(t) is alpha_vault * R_DAO(t) distributed pro-rata to PBTC depositors,
- Binding_share_P(t) is any negotiated rho_HV flow from delegated binding.

7.4 Bribe Market Participation

7.4.1 Overview

Bribes are voluntary incentives paid by protocols or counterparties to voters of a specific gauge to attract voting weight. Both veBTC and vePRML voters in Bucket A are eligible to receive bribes on gauges they support, subject to identity and safety rules.

7.4.2 Eligibility and claim rules

- **Eligibility:** any Identity that cast votes on gauge g in epoch t is eligible for the bribe attached to g in epoch t, pro-rata to their effective vote weight.

- **Claim timing:** bound identities may claim bribes without delay; unbound identities are subject to a claim delay Delta_bribe.

- **Transparency:** each bribe specifies funding source, amount, vesting or lockup if any, and the epoch of record for eligibility.

7.4.3 Accounting and safety

- Bribes do not count toward validator floor enforcement and must not impair S_Backstop replenishment targets.
- Bribe programs cannot bypass warm-up, veto, or per-gauge cap rules and must adhere to disclosure standards.
- Escrowed emissions for warming gauges are distinct from bribes; bribes are paid per the bribe contract terms, while emissions escrow E_escrow follows the activation or veto outcomes in Section 6.

7.4.4 Interaction with veBTC binding

- Binding does not change bribe eligibility or scope; it affects vote decay only.
- Where specified by policy, binding may confer a small multiplier on Bribe_share_P(t) for bound identities to further align long-term BTC governance with high-reliability operators; any such multiplier must remain within explicit bounds and may be set to 1.0 by default.

7.5 Plain-Language Summary

- You can put BTC to work without a custodian. Deposit BTC to mint PBTC, lock it for veBTC, and vote on where liquidity and BTC Vault revenue go.
- Staking PBTC or PBTC–PRML LP in a gauge earns program emissions, and PRML-paired pools can receive a modest boost.
- The BTC Vault sends a governed portion of protocol revenue to PBTC depositors each epoch, after converting it to PBTC. It can be paused if markets are stressed.
- You can optionally bind your veBTC to a specific Hardware Validator. Your voting power fades more slowly, and you can agree on a revenue share with that operator.
- As a voter, you can also earn bribes offered by protocols to attract votes to their gauges. Bound voters can claim immediately; unbound voters wait for a short delay. Bribes follow strict transparency and safety rules and cannot undermine validator funding or the emergency reserve.

---

8. pUSD Stablecoin – Collateralization, Liquidations, Backstop Alignment

This section defines the over-collateralized pUSD stablecoin, its risk controls, liquidation mechanics, oracle discipline, and the DAO Backstop's role in crisis response. Parameters and symbols follow Section 3.

8.1 Collateralization and Health Metrics

8.1.1 Collateral set and valuation

- **Primary collateral**: PBTC.

- **Valuation**: Collateral value is computed from medianized oracle prices subject to deviation and heartbeat bounds (delta_oracle, tau_oracle). If bounds are breached, minting and redemptions can freeze under EMPP until integrity is restored.

8.1.2 Health identities

- **Collateral ratio**: CR = value(collateral) / debt.
- **Minimum collateral**: CR_min per asset; minting requires CR ≥ CR_min.
- **Warning band**: CR_warn > CR_liq triggers user alerts, fee nudges, or partial deleveraging incentives.
- **Liquidation threshold**: CR_liq, where CR < CR_liq moves a position into liquidation.

8.1.3 Stability charges and fees

- **Mint and redemption fees**: policy-set to maintain target spreads and fund operations.
- **Liquidation penalty**: pi_liq charged on liquidated debt to compensate keepers and the system for risk.
- **Queueing and throttles**: L_queue caps redemptions per 24 h to avoid run dynamics.

8.2 Mint, Redeem, and Liquidation Mechanics

8.2.1 Mint and redeem

- **Mint**: user deposits PBTC into a pUSD vault, receives pUSD up to CR_min, paying any mint fee.
- **Redeem**: user repays pUSD to unlock PBTC plus accrued fees, subject to L_queue and safety mode if active.

8.2.2 Liquidation pipeline

When CR < CR_liq:

1. **Seizure window**: position enters liquidation; a liquidation amount is computed to restore CR ≥ CR_min (partial liquidation preferred to reduce cascade).
2. **Auction**: Dutch or batch auction sells seized PBTC for pUSD. Keepers bid pUSD to retire debt plus pi_liq; residual PBTC, if any, is returned to the user.
3. **Settlement**: proceeds retire the liquidated debt; penalties and fees are routed to DAO revenue; any shortfall moves to Stability tooling (9.3).

Keeper incentives. Priority access, fee rebates, and minimum tick sizes are tuned to promote rapid, orderly auctions across market regimes.

8.3 Stability Tooling and DAO Backstop Integration

8.3.1 Stability Pool

- **Purpose**: a pooled liquidity facility that can absorb liquidations by automatically swapping pUSD for PBTC at a discount, reducing auction latency and slippage during stress.

- **Funding**: voluntary deposits of pUSD and, by governance, designated Treasury tranches; rewards sourced from liquidation penalties and protocol incentives.

- **Risk controls**: per-epoch contribution and withdrawal limits; circuit breakers aligned with oracle guards.

8.3.2 Backstop Vault and emergency use

- **Funding**: S_Backstop sourced from the fixed slice each epoch (1% to 3%).

- **Deployment**: under EMPP only, within capped amounts and time-boxed windows, the Backstop may:
    - Provide pUSD (or approved assets) to the Stability Pool or auctions to maintain orderly deleveraging.
    - Purchase PBTC or BTC at a discount from distressed liquidations when market depth is insufficient.

- **Hyper-bitcoinized alignment:** In systemic stress, the Backstop can opportunistically **acquire BTC at a discount** using pUSD or other approved reserves. This is consistent with the thesis that BTC becomes the global unit of account. By buying PBTC or BTC below fair value:
    - The DAO **stabilizes the system** by absorbing sell pressure.
    - The DAO **accumulates BTC** in periods of fear, consistent with long-term conviction.
    - When conditions normalize, the DAO has options:
        - **Hold** the BTC as a strategic reserve backing protocol solvency under a BTC-centric regime.
        - **Distribute** a governed portion to the BTC Vault to amplify PBTC depositor yield.

        - **Realize gains** by selling a portion back into the market to **replenish the Backstop** and, if authorized, retire pUSD debt or reduce net issuance via burns.
    - This creates a flywheel where crisis-time purchases support market functioning and, over a full cycle, are expected to **generate surplus** that strengthens the reserve, reduces long-run risk, and reinforces the hyper-bitcoinized thesis.

8.3.3 Oracle integrity and EMPP triggers

- **Deviation guard**: if any primary price deviates beyond delta_oracle, or heartbeats exceed tau_oracle, minting may freeze and auctions switch to conservative modes.

- **EMPP eligibility**: Gamma_EMPP enumerates actions such as oracle failover, temporary fee hardening, CR_min elevation, and limited Backstop releases. All actions are logged and require post-action replenishment plans.

8.3.4 Accounting identities

Let Debt(t) be total outstanding pUSD debt; let Collateral(t) be the fair value of pledged collateral; let R_DAO(t) be DAO revenue.

- **System collateralization**: SysCR(t) = Collateral(t) / Debt(t).

- **Backstop coverage**: Cov_backstop(t) = Backstop_balance(t) / Debt(t).

- **Backstop change**: Backstop_balance(t+1) = Backstop_balance(t) + S_Backstop(t) + Gains_backstop(t) − Deploy_backstop(t) − Replenish_outflows(t).

- **Discount purchase accounting**: when the DAO acquires PBTC at discount d and later realizes it at price uplift u: Gains_backstop ≈ quantity * (u − d) − costs, with governance deciding the split across replenishment, burns, Vault distributions, or Treasury.

8.4 Plain-Language Summary

- Gas emissions and network subsidy are used to stabilize liquidity risks such as liquidation/margin calls of CDP. As the network achieves more activity and adoption the USD CDP becomes more robust to market volatility and black swan events.
- pUSD is created by locking PBTC. You can borrow pUSD up to a safe collateral ratio. If your position falls below the liquidation line, part of your collateral is sold to repay your debt.
- Prices come from multiple sources and must stay within bounds. If the feeds look unreliable, the system can freeze minting and switch to safer modes until it is fixed.

- There is a Stability Pool and a Backstop reserve. The pool absorbs liquidations quickly, and the Backstop can be released in small, well-defined amounts during emergencies.
- In panics, the DAO can buy PBTC or BTC at a discount. That helps the market stabilize and lets the DAO accumulate BTC cheaply. Later, when BTC recovers, the DAO can sell some for a gain, refill the Backstop, and optionally boost Vault payouts or reduce issuance. This matches the long-term view that BTC becomes the global unit of account.
- Redemption limits and fees slow runs, while conservative parameters and audits keep the system transparent and predictable.

---

9. Bridge Operations and Decentralization Roadmap

This section specifies cross-domain messaging and asset transport and defines the **governed** path from a **Federated Bridge** to a **Semi-Federated Bridge** and finally to a **Fully Decentralized zk Garbled-Circuit (ZK-GC) Bridge**. Stage transitions are **not automatic**. Quantitative and qualitative thresholds are **readiness indicators** that inform a Monetary Policy Proposal (MPP). Actual cutovers occur **only by DAO approval** with bicameral voting, warm-up visibility, overlap, and explicit change control. All notation follows Section 3.

9.1 Security Model and Objectives

Objectives

1. Minimize trust beyond Bitcoin and PrimeLayer proofs.
2. Maintain liveness with bounded failure modes and safe exits.
3. Record verifiable public evidence for every cross-domain state change.
4. Evolve by governed stages without breaking safety or auditability.

Anchoring. Bridge checkpoints, connector state roots, and proof hashes are referenced in the Finality Anchor Commitment (FAC) anchored to Bitcoin via AuxPoW merge-mined tags, providing durable public audit.

Core parameters

Symbol	**Meaning**	**Notes**
c	Committee size (route-specific)	Stage-dependent: c1, c2.
t	Signature threshold	Stage-dependent: t1, t2 $t \le c$.

Symbol	Meaning	Notes
tau_anchor	Target time to publish FAC	Aligns route SLOs to epoch cadence.
tau_committee	Timelock before committee attestations finalize	Stage-dependent: tau_committee1, tau_committee2.
tau_challenge	Challenge window for disputes	Stage-dependent: tau_challenge1, tau_challenge2.
L_route	Per-route capacity and rate limits	Stage-dependent: L1, L2, L3.
S_proof	Proof SLO for zk verification	Stage III parameter.
N_overlap	Overlap epochs during stage cutover	Required at every cutover.
chi_checkpoint	Cross-binding checkpoint at cutover	Binds last-old to first-new.
I_index	Unified event index across mechanisms	Single canonical index for clients.

9.2 Stage I – Federated Bridge (FB)

Trust model. A route-specific committee signs off on source-chain events. Attestations are subject to a timelock and public challenge. No proof requirement.

Default per-route parameters

Name	Symbol	Default (illustrative)
Committee size	c1	7 or 9
Threshold	t1	5 of 7 or 7 of 9
Timelock	tau_committee1	12 to 24 h
Challenge window	tau_challenge1	24 to 72 h

Name	Symbol	Default (illustrative)
Capacity limits	L1	conservative per-asset and per-route caps

Flow

1. Source emits event E. Committee members sign attestation A(E).
2. After tau_committee1, A(E) is queued.
3. If no valid challenge arrives within tau_challenge1, execute E on destination.
4. Persist E, A(E), challenges, and outcomes on-chain with content-addressed references.

Controls and evidence

- Threshold keys with on-chain proofs of rotation.
- Public dashboards for signer availability, median attestation time, challenge outcomes.
- MPP controls L1 and committee composition. EMPP may pause a route within narrow scope.

Governed cutover readiness indicators (non-binding)

- c1 and t1 stability across K epochs.
- Zero or low dispute rates and successful challenge handling.
- Demonstrated operator rotation without liveness loss.
- Monitoring SLOs met relative to tau_anchor.

Cutover trigger. An **MPP** proposes moving a route from Stage I to Stage II, citing the indicators above. The DAO decides; if approved, the cutover proceeds with N_overlap and chi_checkpoint. No automatic promotion.

9.3 Stage II – Semi-Federated Bridge (SFB)

Trust model. Hybrid proof-first. Where feasible, events are verified by zk or light-client proofs; a reduced committee remains as fallback for sub-claims or routes not yet covered by proofs.

Default per-route parameters

Name	Symbol	Target (illustrative)
Proof availability ratio	PAR	≥ 80% of events proven
Committee size	c2	5 or 7
Threshold	t2	4 of 5 or 5 of 7

Name	Symbol	Target (illustrative)
Timelock	tau_committee2	6 to 12 h
Challenge window	tau_challenge2	≥ tau_committee2 + margin
Capacity limits	L2	higher than L1, governed by SLOs

Dual track flow

- **Proof path**: Source provides proof P of event E against state root H. Verifier checks P; if valid, execute E without committee.

- **Fallback path**: Committee produces A(E); apply tau_committee2 and tau_challenge2; execute if unchallenged.

Monitoring and discipline

- PAR must be measured per route; L2 increases only if PAR and safety SLOs hold across multiple epochs.
- Committee dependency shrinks; signer churn increases; all rotation is evidenced on-chain.

Governed cutover readiness indicators (non-binding)

- PAR sustained above target with multiple independent provers.
- Verifier circuits stable, audited, and within S_proof.
- Clean challenge history and dispute tooling tested.
- Bridge accounting reconciled across both paths.

Cutover trigger. An **MPP** proposes moving a route from Stage II to Stage III, including circuit audit references, prover diversity, S_proof performance, and incident history. The DAO decides; if approved, the cutover proceeds with N_overlap and chi_checkpoint. No automatic promotion.

9.4 Stage III – Fully Decentralized ZK Garbled-Circuit Bridge (ZK-GC)

Trust model. All route-critical verification is performed by zk proofs. Committees are removed from finality. Complex source logic is encoded as a garbled-circuit or zk-VM program; a succinct proof attests to correct evaluation.

Default per-route parameters

Name	Symbol	Target (illustrative)
Proof SLO	S_proof	≤ tau_anchor / 2
Prover diversity	k_provers	≥ 3 independent implementations
Capacity limits	L3	governed by proof throughput and headroom
Fallback	—	none for finality; read-only audits only

Flow

1. Build circuit C for verifying event E under finalized root H.
2. Evaluate C on witness W to produce proof P_zk.
3. Verify P_zk on destination; if valid, execute E.
4. Persist {E, H, circuit hash, P_zk hash} and operator metadata on-chain; reference in FAC.

Governed downgrade path. If S_proof or prover diversity degrades, a route may **downgrade** to Stage II by **MPP**, with N_overlap and chi_checkpoint to preserve auditability. No implicit fallback.

9.5 Operator Roles and Rotation

Role	Responsibility	Evidence
Relayer	Transport proofs, headers, or attestations	Delivery receipts; latency logs
Prover	Produce P or P_zk within S_proof	Proof artifacts; keyed transcripts
Observer	Detect censorship, stalls, or equivocation; file challenges	Challenge txs; incident reports

Keying uses threshold cryptography where applicable. Rotations are scheduled and evidenced on-chain. Emergency rotations follow MPP or EMPP rules with public incident logs.

9.6 Route Safety, Limits, and Circuit Breakers

- **Caps (L_route)**: Each stage sets per-asset and per-route caps. Increasing caps requires that stage SLOs be met for multiple epochs with zero unresolved incidents. Caps never auto-increase; changes require **MPP**.

- **Timelocks and challenges**: Stages I and II enforce tau_committee and tau_challenge; Stage III relies solely on proof verification for finality.

- **Safety mode**: Under EMPP triggers, reduce caps, pause specific routes, or enforce proof-only processing; all actions time-boxed and audited.

9.7 Fees, Revenues, and Accounting

Fee types

- Toll fees per asset and route.
- Proof fees for heavy circuits (Stages II–III).
- Refunds for canceled or successfully challenged transfers.

Revenue identity. Connector revenue contributes to DAO income:

R_DAO(t) = R_gas(t) + R_dex(t) + R_liq(t) + R_bridge(t) + psi_DAO * Sigma_withheld(t_release) + R_veto(t),

where R_bridge(t) aggregates route tolls and proof fees net of refunds.

9.8 Governed Stage Cutovers and Evidence

Not automatic. Stage changes are **never automatic**. Readiness indicators justify an **MPP** that proposes the cutover plan, parameters, and safety instrumentation. Approval requires the appropriate quorums and thresholds and may be classified as constitutional when surfaces include anchoring, circuit keys, or house scopes.

Cutover procedure:

- **N_overlap** epochs with both mechanisms active for the route.
- **chi_checkpoint** that binds last-old to first-new evidence.
- **I_index** exposes a single canonical event index to clients.
- **R_retrieval** guarantees legacy path retrievability for audits.

Public evidence. Each executed event records source chain id, block height, event id, proof or attestation hash, operator ids, and outcome. Bundled archives include proofs, transcripts, challenges, and rotation attestations, with content-addressed references and FAC pointers.

9.9 Plain-Language Summary

- The bridge becomes more trust-minimized in three stages, but it never switches automatically. The community votes to move stages when clear readiness signals are met.
    1. **Federated**: a group of signers approves transfers with a delay and a public challenge window.
    2. **Semi-federated**: most transfers use cryptographic proofs; a smaller signer group only covers what proofs cannot yet handle.
    3. **ZK-GC**: all important checks are proven with zero-knowledge. There is no signer group to trust for finality.
- If conditions worsen, the DAO can vote to step back to a safer stage while keeping full auditability.
- Every step leaves a permanent trail tied to Bitcoin so anyone can verify what happened. Fees from bridging help fund the protocol and can be directed to programs by governance.

---

10. Infrastructure Continuity and Migration Protocol – Types 1 to 3

This section defines the governed procedures for changing anchoring routes or data-availability lanes without loss of state, balances, or auditability. Migrations are deterministic, produce public evidence, and do not require user action. Bitcoin remains the settlement root at all times via AuxPoW merge-mined tag commitments carrying Finality Anchor Commitments (FACs). Symbols follow prior sections.

10.1 Overview and Objectives

Objectives

1. Preserve liveness, safety, and auditability under routine upgrades or adverse conditions.
2. Ensure Bitcoin remains the settlement root and FAC verification remains public and non-interactive.
3. Guarantee continuity of state and balances for validators, PBTC, pUSD, gauges, Treasury, and Vaults.

4. Require governed approvals for every cutover; no automated migrations.

Key symbols

- N_overlap – number of epochs with both old and new paths active in parallel.
- chi_checkpoint – cross-binding checkpoint that cryptographically binds last-old to first-new anchor.
- I_index – unified FAC/event index presented to clients across overlap and after cutover.
- R_retrieval – policy for legacy-path retrievability and archival availability.
- tau_anchor – target anchor publication SLO; used to align overlap timing.

Governance

- Standard cutovers are authorized by a Monetary Policy Proposal (MPP) with readiness evidence, overlap plan, and explicit exit criteria.
- Emergency cutovers (when safety or liveness is at risk) may be authorized by an Emergency Monetary Policy Proposal (EMPP) limited to the narrow actions enumerated here, with time-boxing and mandatory post-action audits.

10.2 Type 1 – Anchor Shift Migration

Scope: Switch the anchoring route or tag namespace carrying the FAC pointer while keeping execution, validator registries, and data-availability (DA) unchanged.

Typical triggers:

- Reliability or cost improvements in a new merge-mined tag route.
- Policy or format changes in tag indexing that do not alter trust assumptions.
- Operational SLO breaches on the current anchoring endpoint.

Execution plan:

1. **Dual anchor** – publish each FAC to both old and new anchor routes for N_overlap epochs.
2. **Canonical pointer** – FAC metadata advertises both anchors during overlap.
3. **Index handover** – publish a deterministic mapping from old anchor indices to new anchor indices; expose I_index to clients.
4. **Cross-binding** – at the final overlap epoch, emit chi_checkpoint that binds last-old to first-new anchor.
5. **Decommission** – after exit criteria are met, mark the old route read-only; retain R_retrieval to guarantee historical fetch.

Invariants:

- Bitcoin remains the settlement root; FAC format and verification are unchanged.
- No user action; validators, PBTC/pUSD, gauges, and Treasury balances persist 1 to 1.
- Execution semantics, NV/HV registries, and DA lane are untouched.

Governance:

- **MPP** with overlap schedule, dashboards, test vectors, failure rollback, and explicit success metrics.

10.3 Type 2 – Full Infrastructure Migration

Scope: Migrate the anchoring substrate and any dependent verification infrastructure (and, if specified, DA lane) to a new environment while preserving all state and audit trails.

Typical triggers:

- Sustained instability or unacceptable economics on the current substrate.
- Strategic realignment to a superior AuxPoW substrate.
- Material protocol upgrades that require a different substrate environment or proof plumbing.

Execution plan:

1. **Parallel commit** – post each FAC to both current and target substrates for N_overlap epochs; maintain both DA references if DA also changes.

2. **Unified index** – expose I_index that resolves to either path during overlap and to the new path post-cutover.

3. **Cross-binding** – include chi_checkpoint in the final overlap FAC that binds last-old anchor to first-new anchor.

4. **State continuity** – export and import the following, pinning each hash in FAC metadata at snapshot epoch s:
    - Validator registry root and slashing ledger at s.
    - CPI parameters and cohort policy at s.
    - Gauge registry and E_escrow ledgers at s.
    - Treasury, Vault, PBTC/pUSD supplies and reserves at s.

5. **Decommission** – mark the legacy path read-only; guarantee R_retrieval for historical queries.

Invariants:

- Bitcoin remains the settlement root via AuxPoW; FAC verification stays public and non-interactive.
- No re-execution of application state; all balances and program ledgers persist.
- Bridging connectors are synchronized to the new path using the same overlap and checkpointing.

Governance:

- **MPP** with elevated thresholds for critical infrastructure changes, or **EMPP** when immediate safety or liveness requires urgent cutover.
- Public dry-run, overlap monitoring, and signed post-cutover audit.

10.4 Type 3 – DA-Only Migration

Scope: Change the data-availability lane while leaving anchoring and execution semantics unchanged.

Typical triggers:

- DA cost, throughput, or censorship-resistance improvements.
- Regulatory or geographic constraints on existing DA providers.
- Move to a modular DA network with better guarantees.

Execution plan:

1. **Dual DA** – publish proof artifacts and witnesses to both old and new DA lanes for N_overlap epochs.
2. **FAC references** – FAC metadata carries content-addressed pointers to both DA lanes during overlap.
3. **Availability checks** – enforce that both DA lanes satisfy availability proofs for the same epochs throughout overlap; abort cutover if gaps are detected.
4. **Switch** – after chi_checkpoint and satisfied exit criteria, set the canonical DA pointer to the new lane; retain R_retrieval for the legacy lane.

Invariants:

- Anchoring route, execution semantics, and validator registries remain unchanged.
- FAC format and verification rules are stable; only data retrieval pointers change.

Governance:

- **MPP** with DA benchmarks, overlap length, retention policy for legacy DA, and post-cutover retrievability audits.

10.5 Migration Types – Summary Table

Type	Scope	Typical triggers	Execution path	Governance	Invariants
Type 1 – Anchor Shift	Change FAC anchoring route/tag namespace only	Reliability/cost; tag format or index changes	Dual anchor for $N_{overlap}$ → canonical pointer and I_{index} → $chi_{checkpoint}$ → legacy read-only with $R_{retrieval}$	MPP	Bitcoin root unchanged; FAC format unchanged; execution and DA untouched; no user action.
Type 2 – Full Infrastructure	New substrate and dependent verification infra (optionally DA)	Sustained instability; strategic realignment; major upgrades	Parallel commit on both substrates → unified I_{index} → $chi_{checkpoint}$ → export/import snapshot hashes → legacy read-only	MPP (elevated) or EMPP if urgent	Bitcoin root unchanged; public verification; state and balances preserved; connectors synchronized.
Type 3 – DA-Only	Replace or relocate DA lane only	Cost/throughput/censorship improvements; regulatory constraints	Dual DA publication for $N_{overlap}$ → FAC dual pointers → availability proofs → switch pointer → legacy retained per $R_{retrieval}$	MPP	Anchoring and execution unchanged; FAC format stable; audit retrievability guaranteed.

10.6 Evidence, Monitoring, and Exit Criteria

Evidence bundles. Each migration publishes hash-addressed bundles containing: snapshot epoch s; registry roots; gauge and escrow ledgers; Treasury and Backstop balances; connector states; FAC indices; and DA object manifests. Bundle hashes are referenced in FAC metadata during overlap and at cutover.

Monitoring:

- Anchor SLOs: tau_anchor adherence on both paths.
- Consistency checks: FAC equivalence and index mapping integrity.
- DA availability proofs: dual lane retrieval and parity hash checks.
- Post-cutover audits: retrieval from the new path and read-only legacy path within R_retrieval.

Exit criteria:

- No consistency failures across N_overlap.
- All evidence bundles posted and verifiable.
- Public dashboards green for anchor cadence, availability, and index mapping.
- Governance confirmation that exit criteria are met before decommissioning legacy paths.

10.7 Plain-Language Summary

- There are three governed ways to change the network's plumbing without breaking anything.
    1. **Anchor Shift:** moves only the way we post checkpoints to Bitcoin.
    2. **Full Infrastructure:** moves the anchoring substrate and related plumbing and can include data-availability if needed.
    3. **DA-Only:** changes where the proof data are stored and fetched.

- In all cases, the system runs the old and new setups together for a while and posts a special checkpoint that links them. A single index lets users and apps follow along as if nothing changed.

- These moves are **never automatic**. They require a **Monetary Policy Proposal** and, in rare emergencies, an **Emergency Monetary Policy Proposal**. The plan, the safety checks, and the results are all published so anyone can verify that nothing was lost.

---

11. Tokenomics – Allocation, Vesting, Long-Run Supply, EIP-1559 Fees

This section specifies the initial distribution and vesting disciplines, the per-epoch allocation sequence, burn and buyback controls, the validator floor, the EIP-1559-style PRML fee model, and long-run issuance accounting. Notation matches Section 3 (plain text symbols).

11.1 Initial Allocation and Vesting Schedules

11.1.1 Allocation categories at genesis

Category	**Objective**	**Mechanism**	**Governance lane**
Community and ecosystem	User growth, grants, partnerships, retroactive rewards	Program budgets with warm-up, escrow, VC review	Bucket A or Bucket B (per scope)
Validator alignment	Seed HV and NV participation and reliability	Bond NFTs, cohort bootstrap, performance incentives	Bucket B
Builders and core contributors	Client maintenance, audits, public goods	Cliff/linear vesting with transparency dashboards	S_Build envelope + Bucket B programs
Treasury reserve	Strategic initiatives, market ops, matching	Time-locked tranches released by MPP	Bicameral if cross-bucket effects
Backstop pre-fund (optional)	Accelerate early reserve	One-time deposit, EMPP-bounded use, replenishment priority	EMPP-bounded
Burn gauge reserve	Reduce net issuance within corridor	Burn gauge stream with cap B_rate, floor-first ordering	Bucket B
Treasury buyback program	Market stabilization or float policy	Buyback program with caps K_buy, rails, reporting	Bicameral MPP; warm-up applies

Notes • No rebasing; remove any rebase buffer, credits, or solvency indices. • Any non-vested stream must pass warm-up, escrow, and VC review; veto routes escrow to DAO revenue.

11.2 Per-Epoch Allocation and Safety Order

11.2.1 Allocation order (epoch t)

1. Compute emission E_epoch(t+1) = E_epoch(t) * g(phi, mu(t)) within corridor; ensure annual emission >= Emin.
2. Reserve fixed slice E_fixed(t) = S_HV(t) + S_Build(t) + S_Backstop(t).
3. Compute governed shares E_A(t) = S_A * E_epoch(t), E_B(t) = S_B * E_epoch(t).
4. Enforce validator floor Require S_HV(t) + NV_from_B(t) >= V_floor * E_epoch(t). If false, reallocate inside Bucket B toward validator programs until true.
5. Apply gauge lifecycle and safety interlocks Warm-up T_warmup, escrow E_escrow, VC window, per-gauge cap cap_gauge, identity-aware weighting (alpha_bound, alpha_unbound).
6. Stream activated gauges Release per-gauge streams for t; apply beta_early to eligible LP positions during first 14 days after activation.

11.2.2 Fixed allocation (infrastructure)

Envelope	**Symbol**	**Share of total**	**Governance**	**Purpose**
HV per-block reward	S_HV	20%	Constitutional	Pays HV proposer/builder/attester via E_block and theta_P, theta_B, theta_A.
Builders	S_Build	2% to 4%	MPP in [2, 4]	Client maintenance; audits; tooling; R&D.
Backstop Vault	S_Backstop	1% to 3%	MPP in [1, 3]	Crisis liquidity; EMPP-bounded deployment; replenishment priority.

S_Build + S_Backstop = 5% of total.

11.3 Burn Gauge and Treasury Buybacks

11.3.1 Burn gauge (Bucket B)

- **Lane:** Bucket B (vePRML).
- **Ordering:** executes only after validator floor and backstop checks.
- **Cap:** B_rate per epoch limits burnable portion of E_B.
- **Accounting:** B_gauge(t) contributes to B_total(t).
- **No redirect:** burn gauge cannot forward to recipients or Treasury.

11.3.2 Treasury buyback program

- **Lane:** bicameral MPP; warm-up and VC visibility apply.
- **Funding:** Treasury balances or approved stables; never from E_epoch.
- **Modes:** buyback-and-burn (retire to burn sink) or buyback-and-warehouse (hold as Treasury inventory).
- **Rails:** K_buy caps, price bands, slippage bounds, daily limits; may not breach V_floor or delay backstop replenishment.
- **Reporting:** per-epoch publish notional spent, units acquired, avg price, disposition.

11.4 PRML EIP-1559 Fee Model

The PRML fee market uses a base fee per gas that adjusts with demand plus a priority tip. Base fees are partially or fully burned; tips pay the HV proposer by default. Non-burned base-fee portions flow to Treasury (R_gas) within policy bounds.

11.4.1 Parameters (add to Section 3)

Symbol	Meaning	Governance
F_n	Base fee per gas in block n	MPP sets F_0 and bounds
G_target	Target gas per block	MPP sets initial and bounds
D_bf	Base-fee change denominator	MPP sets (for example, 8)
F_min	Base-fee floor	MPP sets floor
eta_tip	Proposer share of priority tips	MPP (default 1.0)
gamma_fee	Burn share of base fee	MPP in [0, 1] (1.0 = full burn)

11.4.2 Base-fee update rule

For block n with gasUsed_n:

F_{n+1} = max(F_min , F_n * (1 + (gasUsed_n − G_target) / (G_target * D_bf)))

Gas limit per block = 2 * G_target.

11.4.3 Per-block flows and epoch aggregation

Per block n in epoch t:

- Base-fee component = F_n * gasUsed_n • Burn: gamma_fee(t) * F_n * gasUsed_n → burn • Treasury: (1 − gamma_fee(t)) * F_n * gasUsed_n → R_gas(t)

- Priority tips = tip_n * gasUsed_n • Proposer: eta_tip(t) * tip_n * gasUsed_n → HV proposer revenue (outside E_epoch) • Treasury (optional): (1 − eta_tip(t)) * tip_n * gasUsed_n → R_gas(t) or burn per policy

Epoch sums:

B_fee(t) = sum over n in epoch t of [gamma_fee(t) * F_n * gasUsed_n] R_gas(t) = sum over n in epoch t of [(1 − gamma_fee(t)) * F_n * gasUsed_n + (1 − eta_tip(t)) * tip_n * gasUsed_n]

R_gas(t) is part of R_DAO(t) and is routed by governance (for example, to Bucket A Vault share alpha_vault, Treasury, or programs) after floor and backstop checks.

11.5 Long-Run Issuance and Net Supply

11.5.1 Dampened issuance corridor

- E_epoch(t+1) = E_epoch(t) * g(phi, mu(t)) within bounds.
- phi is MPP-tunable within a narrow corridor; mu(t) includes bounded indicators (utilization, participation).
- Annual emission never falls below Emin; combined with V_floor this sustains validator budgets.

11.5.2 Net issuance identity

Let B_withheld(t) be withheld-release burn (from invalid/missed blocks), and B_fee(t) the base-fee burn.

B_total(t) = B_gauge(t) + B_fee(t) + B_withheld(t) E_net(t) = E_epoch(t) − B_total(t)

Buyback-and-burn reduces circulating supply but does not change E_epoch(t).

11.5.3 Floor-first and backstop-first ordering

Per epoch:

1. Reserve S_HV, S_Build, S_Backstop.
2. Compute E_A, E_B; enforce V_floor.
3. Execute burn gauge within B_rate.
4. Execute buybacks within K_buy rails.
5. Count B_fee(t) from fees into B_total(t).
6. Apply withheld-release burns from Sigma_withheld per Sections 4 and 5.

11.5.4 Transparency and audits

Publish per epoch: E_epoch, B_total, B_gauge, B_fee, B_withheld, E_net, S_HV, NV_from_B, S_Build, S_Backstop, per-gauge streams, alpha_PRML usage, R_route, R_gas, buyback activity. Reference all fee-burn proofs and buyback transactions in FAC metadata.

11.6 Plain-Language Summary

- New tokens are created on a smooth schedule that can be tuned within safe limits and never drops below a minimum. First, the protocol pays for hardware validators, builders, and the emergency reserve. Then it splits the rest into two buckets the community votes on.
- Validators always receive at least half of total emissions when you combine the fixed hardware stream with validator programs from Bucket B.

- A Burn gauge can destroy part of the bucket allocation to lower net issuance, but only after security and reserves are fully funded. The Treasury can buy back tokens under strict caps and either burn them or hold them, with full reporting.
- PRML fees use an EIP-1559 model. Each block has a base fee that mostly burns by default and a tip that pays the block producer. If governance chooses, part of the base-fee flow can go to the Treasury within tight bounds and without harming validator funding or the Backstop.
- Every epoch reports exactly how much was minted, how much was burned, how much went to validators, and what funded the Treasury or the BTC Vault.

---

12. Security and Auditing – Controls and Observability

This section defines the enforceable invariants, monitoring surfaces, audit evidence, incident processes, and operational protections that together provide defense in depth and durable public accountability. Notation follows Section 3.

12.1 Control Surfaces and Mandatory Invariants

Security is expressed first as protocol-level inequalities and orderings that must hold **before** any per-gauge streaming occurs. Violations are unrepresentable in state transitions.

12.1.1 Protocol invariants

- **Validator floor.** For every epoch t: S_HV(t) + NV_from_B(t) ≥ V_floor * E_epoch(t) Enforced prior to any non-validator program streaming.

- **Backstop continuity.** S_Backstop accrues in the 1% to 3% corridor every epoch. After any EMPP deployment, replenishment priority applies until coverage targets are restored.

- **Gauge warm-up and veto.** New or materially changed gauges are escrowed for T_warmup. If vetoed, route 100% of E_escrow to DAO revenue; if activated, pay E_escrow retroactively to warm-up voters per epoch snapshots and apply beta_early to eligible LPs for 14 days after activation.

- **Invalid-block withheld-subsidy rule.** If a block is invalid or missed, withhold E_block and add to Sigma_withheld. On the next valid block, burn psi_burn * Sigma_withheld

and send psi_DAO * Sigma_withheld to DAO revenue; set Sigma_withheld = 0; then pay the current cohort split (theta_P, theta_B, theta_A).

- **Burn ordering and caps.** Burn gauge executes only after validator floor and Backstop checks. Per-epoch burn is capped by B_rate.

- **Buyback ordering and rails.** Treasury buybacks cannot impair validator floor or Backstop replenishment. Execution follows price bands, slippage rails, and daily caps K_buy; warm-up and VC visibility apply where a gauge-like program stream is used.

- **House scopes.** Bucket A is governed by w_A = [0.5 veBTC, 0.5 vePRML]. Bucket B is governed by vePRML only. No program may indirectly alter house scopes.

12.1.2 Governance procedure discipline

- **Monetary Policy Proposal (MPP).** Required for parameter changes within published corridors, gauge additions, Builders and Backstop sub-band adjustments, alpha_PRML bounds, R_route, alpha_vault, CPI corridors, and oracle bounds (delta_oracle, tau_oracle). MPPs must include rationale, parameter diffs, bound checks, safety analysis, and monitoring plans.

- **Emergency Monetary Policy Proposal (EMPP).** Eligible only for enumerated emergency actions: Backstop release within caps, oracle failover, temporary clamps, safety-mode entry (tau_safety). Requires elevated quorum Q_EMPP and approval T_EMPP, is time-boxed, and mandates post-action reports and replenishment plans.

- **Constitutional surfaces.** Changes to S_HV, house scopes, V_floor, anchoring semantics, or circuit keys are constitutional and require heightened treatment with explicit evidence bundles.

12.2 Monitoring and Public Observability

The system publishes machine-readable and human-auditable telemetry designed to verify invariants and detect anomalies early.

12.2.1 Epoch and issuance dashboards

Per epoch t, publish:

- E_epoch(t), B_total(t), E_net(t)
- S_HV(t), NV_from_B(t), S_Build(t), S_Backstop(t)
- Bucket A and Bucket B per-gauge streams; alpha_PRML usage; R_route usage
- Warm-up queues, E_escrow levels, veto decisions with reason codes; beta_early applications

- Buyback executions: notional, units, average price, disposition
- Validator floor attestation that S_HV + NV_from_B ≥ V_floor * E_epoch

12.2.2 Anchoring health and proofs

- Anchor SLOs vs tau_anchor, missed-anchor alarms, proof sizes, verification latency, Sigma_HV participation.
- Dual-path monitoring during migrations: overlap progress (N_overlap), cross-binding success (chi_checkpoint), unified index I_index parity, R_retrieval tests.

12.2.3 Validator telemetry and reputation

- Uptime U_rho, attestation success rates, proposer inclusion latency, slash events, redelegation flows (Bond NFTs), and per-epoch updates to HardwareScore and GovernanceScore.

12.2.4 Treasury and vault transparency

- Builders spend, Backstop accrual and deployments with replenishment schedule, Treasury inflows (R_DAO breakdown), Vault conversions (rho_vault_fees) and per-depositor payouts, inventory for buyback-and-warehouse.

12.3 Audit Domains and Evidence Artifacts

Audits combine formal verification where feasible, programmatic checks, and durable public artifacts.

Domain	**Scope**	**Primary evidence**	**Cadence**
Core contracts	Bonding; gauges; vesting; Vault; Treasury; Backstop	Formal specs; unit and property tests; third-party audits; on-chain invariant checks	Pre-deploy and continuous.
Proof and anchoring	pi_epoch validity; Sigma_HV aggregation; FAC contents, retrieval via AuxPoW tags	Verifier traces, FAC indices, overlap parity checks, DA availability proofs	Per epoch, extra during N_overlap.

Domain	Scope	Primary evidence	Cadence
Economics and issuance	E_epoch; V_floor;burn, buyback, vault	Machine-readable ledgers, Merkle receipts for per-gauge streams, validator floor attestations	Per epoch.
Oracles	Deviation and heartbeat adherence; failovers	Signed deviation logs, medianization proofs, feed rotation records	Continuous, event-driven.
Governance	MPP and EMPP logs; VC vetoes	On-chain metadata; quorums; approvals; veto reason codes; post-action audits	Per action.
Bridge	Proof transcripts; committee attestations; challenges	Event records; challenge outcomes; operator rotation proofs	Route-specific.

Evidence persistence Evidence bundles are content-addressed and linked from FAC metadata so third parties can reconstruct histories without privileged access.

12.4 Incident Response and Recovery

12.4.1 Response stages

1. **Detect**: automated alerts or observer reports trigger triage.

2. **Stabilize**: enter safety mode tau_safety, clamp caps, pause affected gauges or routes, prepare EMPP if required.

3. **Recover**: deploy Backstop within caps, rotate keys or committees, adjust parameters within bounds, resume normal operation.

4. **Review**: publish post-action audit with full timeline, parameter deltas, costs, and replenishment outcomes.

12.4.2 EMPP boundaries and accountability

- Elevated Q_EMPP and T_EMPP, explicit scope, time-boxing, and automatic sunset.
- Repeated EMPP use on the same surface escalates requirements or triggers constitutional review.
- Post-EMPP reports must reconcile Backstop usage, vault and treasury impacts, and parameter reversion.

12.5 Key Management and Operational Separation

- **Threshold keys** for route committees (where applicable), treasury signers, and other sensitive roles; rotation schedules with on-chain proofs of rotation.

- **Separation of duties** for deployment, monitoring, treasury execution, and VC operations.

- **Least privilege** access controls; emergency break-glass keys are timelocked and disclosed.

12.6 Migration Verification and Exit Tests

During Types 1–3 migrations:

- **Overlap checks**: both paths must meet tau_anchor; missing anchors are flagged.

- **Cross-binding**: verify chi_checkpoint binds last-old to first-new; I_index returns consistent results.

- **Retrievability**: historical artifacts remain accessible per R_retrieval; DA parity checks succeed.

- **Exit**: only after all checks pass and evidence bundles are posted does the MPP mark legacy path read-only.

12.7 Formal Checks and Machine-Readable Attestations

Before any gauge streams in epoch t:

1. Validate: S_HV + NV_from_B ≥ V_floor * E_epoch.

2. Confirm S_Backstop accrual within policy corridor; if depleted by EMPP, confirm replenishment priority.
3. Verify E_block withheld processing: if Sigma_withheld > 0 and a valid block landed, apply psi_burn and psi_DAO, reset Sigma_withheld = 0.
4. Enforce burn cap B_rate and ordering after floor and backstop checks.
5. Validate alpha_PRML and R_route usage do not cause 1) or 2) to fail.
6. Confirm warm-up and veto outcomes; if vetoed, route E_escrow to DAO; if activated, compute retro payouts and apply beta_early windows.
7. Record a signed attestation object for 1–6 and include its hash in the epoch ledger.

12.8 Plain-Language Summary

- The rules that keep the system safe are hard coded as checks that must pass before any program gets paid. Validators always get enough funding, and the emergency reserve fills every epoch.
- If a block is bad, its reward is not paid. The held amount is processed later: half burned, half to the DAO.
- New programs spend two weeks in a waiting period. If they pass review, early voters and liquidity are rewarded. If they are blocked, the money goes to the DAO.
- All decisions and payments are logged and auditable. Anyone can see how much was created, burned, and paid out, and they can rebuild the history from the anchors posted to Bitcoin.
- In an emergency, a stricter vote can authorize narrow, time-limited actions. Those actions are logged and must be followed by a public report and a plan to restore normal settings.
- When the network changes its anchoring or data provider, both old and new run in parallel for a while, a special checkpoint ties them together, and the old path remains readable so nothing is lost.

---

13. References and Appendices

This section lists the canonical sources that ground the design, followed by formal appendices for equations, glossary, and figure or table identifiers. References include DOIs or canonical links where available. Notation matches the rest of this document.

13.1 References

Bitcoin, AuxPoW, and anchoring

1. Nakamoto, S. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.” https://bitcoin.org/bitcoin.pdf
2. Namecoin Project. “Auxiliary Proof-of-Work (AuxPoW) and Merge Mining.” https://www.namecoin.org/docs/merged-mining/
3. Syscoin Core Team. 2020. “Syscoin 4.0 Whitepaper.” https://syscoin.org/whitepaper.pdf
4. Syscoin Core Team. 2025. “Bitcoin-Backed Sidechain Bridges: zk-Light Clients and Economic Challenges for Secure Finality.” https://syscoin.org/btc_bridge.pdf
5. Syscoin Core Team. 2025. “Syscoin 5.0.0 Release Notes.” https://github.com/syscoin/syscoin/blob/master/doc/release-notes/release-notes-5.0.0.md#4-auxpow-tags

Ethereum, EVM, and fee markets

6. Wood, G. 2014–2024. “Ethereum: A Secure Decentralised Generalised Transaction Ledger - Yellow Paper.” https://ethereum.github.io/yellowpaper/paper.pdf
7. Buterin, V., et al. 2021. “EIP-1559: Fee market change for ETH 1.0 chain.” https://eips.ethereum.org/EIPS/eip-1559

Zero-knowledge proofs and recursive composition

8. Bowe, S., Grigg, J., Hopwood, D. 2019. “Halo: Recursive Proof Composition without a Trusted Setup.” IACR ePrint 2019/1021. https://eprint.iacr.org/2019/1021
9. Gabizon, A., Williamson, Z., Ciobotaru, O. 2019. “PLONK: Permutations over Lagrange-bases for Oecumenical Non-interactive Arguments of Knowledge.” IACR ePrint 2019/953. https://eprint.iacr.org/2019/953
10. Zcash Foundation and ECC. 2020–2024. “Halo 2 and Recursive Proofs - Docs and Explainers.” https://github.com/zcash/halo2
11. Yin, M., et al. 2021. “zk-SNARKs for Beginners.” arXiv:1906.07221. https://arxiv.org/abs/1906.07221

Garbled circuits and verifiable computation

12. Yao, A. C. 1986. “How to Generate and Exchange Secrets.” 27th FOCS, 162-167. https://doi.org/10.1109/SFCS.1986.25
13. Beaver, D. 1990. “Foundations of Secure Interactive Computing.” CRYPTO’90. https://doi.org/10.1007/3-540-38424-3_34
14. Dziembowski, S., Kazana, T., Nielsen, J. 2019. “Proofs of Secure Computation.” arXiv:1903.02819. https://arxiv.org/abs/1903.02819
15. “BitVM + Garbled Circuits Bridge for Bitcoin+ (zkSYS) – Technical Descriptor v0.” 2025. [internal whitepaper PDF]

Verifiable randomness, voting, and public goods funding

16. Micali, S., Rabin, M. O., Vadhan, S. 1999. “Verifiable Random Functions.” 40th FOCS, 120-130. https://doi.org/10.1109/SFFCS.1999.814584
17. Lalley, S. P., Weyl, E. G. 2018. “Quadratic Voting: How Mechanism Design Can Radicalize Democracy.” AEA Papers and Proceedings 108, 33-37. https://doi.org/10.1257/pandp.20181002
18. Buterin, V., Hitzig, Z., Weyl, E. G. 2018. “A Flexible Design for Funding Public Goods.” arXiv:1809.06421. https://arxiv.org/abs/1809.06421

Data availability, light clients, and fraud or DA proofs

19. Al-Bassam, M., Sonnino, A., Buterin, V. 2018. “Fraud and Data Availability Proofs - Maximising Light Client Security.” arXiv:1809.09044. https://arxiv.org/abs/1809.09044
20. Boneh, D., et al. 2020. “Compiling MPC to SNARKs for Efficient and Scalable Zero-Knowledge Proof Systems.” IEEE S&P. https://doi.org/10.1109/SP40000.2020.00058

Oracle networks and liquidation designs

21. Ellis, S., Juels, A., Nazarov, S. 2017. “Chainlink: A Decentralized Oracle Network.” https://link.smartcontract.com/whitepaper
22. Maker Foundation. 2020. “The Maker Protocol - Multi-Collateral Dai.” https://makerdao.com/en/whitepaper/
23. Liquity AG. 2021. “Liquity Protocol - Technical Documentation.” https://docs.liquity.org/

Additional background

24. Ben-Sasson, E., et al. 2014. “Scalable Zero Knowledge via Cycles of Elliptic Curves.” CRYPTO’14. https://doi.org/10.1007/978-3-662-44381-1_15
25. Pass, R., Shi, E. 2017. “Thunderella: Blockchains with Optimistic Instant Confirmation.” EUROCRYPT 2018. https://doi.org/10.1007/978-3-319-78375-8_24

Internal or partner documents provided for implementation detail are cataloged in the project repository with content hashes and stable identifiers.

13.2. Variables and Constants – Master Tables

This section enumerates canonical parameters and identities used across the specification. Unless otherwise noted, values are initialized at genesis and may be adjusted only through the governance process stated in the “Governance” column. Symbols are unique and case sensitive.

13.2.1 Emission and Decay Parameters

Symbol	Name	Default or Bounds	Governance	Notes
E0	Initial annual emission	set at genesis	MPP within corridor	Annual reference used to derive per-epoch emission.
lambda	Annual decay factor	bounded corridor	MPP within corridor	Dampening on issuance; applied in the epoch path g(.).
Emin	Annual emission floor	nonzero > 0	Constitutional or narrow MPP	Protects long-run validator funding.
T_epoch	Epoch length	7 days	Fixed	Basis for per-epoch emission.
E_epoch(t+1)	Epoch emission path	E_epoch(t) * g(phi, mu(t))	Derived	g(.) is a bounded dampening function; phi is a governance-tunable dampening scalar; mu(t) are bounded macro indicators (utilization, participation).
phi	Dampening scalar (for g)	corridor per policy	MPP within corridor	Used only in the emission path g(.).
S_fixed	Fixed allocation share (of total)	25%	MPP only for sub-bands	Split into HV, Builders, Backstop envelopes.

Symbol	Name	Default or Bounds	Governance	Notes
S_A	Bucket A share (of total)	37.5%	Fixed	Liquidity and BTC Vault governance.
S_B	Bucket B share (of total)	37.5%	Fixed	Infrastructure and treasury governance.
S_HV	HV fixed share (of total)	20%	Constitutional	Per-block reward stream for HV cohorts.
S_Build	Builders envelope (of total)	2% to 4%	MPP within [2,4]	Fixed-band within the 5% infra slice.
S_Backstop	Backstop envelope (of total)	1% to 3%	MPP within [1,3]	Complements Builders to sum 5%.
alpha_PRML	PRML-pair multiplier	1.25x	MPP within bounds	Amplification factor for PRML-paired pools.

Equation notes • Epoch path: E_epoch(t+1) = E_epoch(t) * g(phi, mu(t)), subject to annual emission >= Emin. • Allocation order each epoch: Fixed → Buckets → Validator floor checks → Gauge warm-up and safety interlocks → Streaming.

13.2.2 Validator Bonding, Cohort Selection, and Vesting

Symbol	Name	Default or Bounds	Governance	Notes
a	Attester committee size	32 (range 16–64)	CPI within MPP bounds	Members contribute to Sigma_HV and fault detection.

Symbol	Name	Default or Bounds	Governance	Notes
b	Builder committee size	5 (range 3–9)	CPI within MPP bounds	Compete to construct blocks for proposer.
W_i	Cohort weight for HV i	f(stake, M_dur, HardwareScore, GovernanceScore, history)	CPI coefficients	VRF-weighted selection with anti-concentration caps.
cap_entity	Per-entity cohort cap	20%	CPI within bounds	Limits the share any single operator can hold.
cap_region	Per-region cohort cap	30%	CPI within bounds	Improves geographic dispersion.
E_block	Nominal per-block HV reward unit	derived from S_HV and E_epoch	Derived	Base unit for the cohort split.
theta_P, theta_B, theta_A	Proposer, Builder, Attester split	policy vector, sum(theta) = 1	TPP within bounds	Determines intra-cohort reward allocation.
Sigma_withheld	Withheld pool on invalid or missed blocks	0 at genesis	Automatic	Accumulates unpaid E_block units.
psi_burn	Burn share of Sigma_withheld	50%	Fixed	Applied at next valid block before cohort split.
psi_DAO	DAO share of Sigma_withheld	50%	Fixed	Routed to DAO revenue on release.
U_rho	Uptime target	95% rolling	CPI within bounds	Rewards and selection weights may use bonuses above target.

Symbol	Name	Default or Bounds	Governance	Notes
M_dur	Lock duration multiplier	bounded slope	MPP within bounds	Used in W_i and certain reward programs.

Block validity rule If a block is invalid or missed, E_block for that slot is withheld and added to Sigma_withheld. On the next valid block, release Sigma_withheld as psi_burn * Sigma_withheld to burn and psi_DAO * Sigma_withheld to DAO revenue, then set Sigma_withheld = 0.

13.2.3 Governance Epochs, Thresholds, and Cooldowns

Symbol	Name	Default or Bounds	Governance	Notes
Q_MPP	MPP quorum per house	policy range	MPP	Minimum participation to consider valid.
T_MPP	MPP approval	simple majority of participants	MPP	Per house unless bicameral combination is required.
Q_EMPP	EMPP quorum	higher than Q_MPP	MPP	Elevated participation for emergency actions.
T_EMPP	EMPP approval	supermajority	MPP	Elevated approval threshold.
tau_cool	Governance cooldown after major changes	policy window	MPP	Prevents rapid oscillations.
w_A	Bucket A house weights	[0.5 veBTC, 0.5 vePRML]	Fixed	Combined after within-house vote aggregation.
alpha_bound	Quadratic exponent – bound identities	0.50	Fixed	Applied to Identity-aggregated ve.

Symbol	Name	Default or Bounds	Governance	Notes
alpha_unbound	Quadratic exponent – unbound positions	0.45	Fixed	Harsher curve to deter sybil splitting.
cap_gauge	Per-gauge voter cap	30%	MPP	Max of a voter's total influence assignable to a single gauge.
Delta_bribe	Bribe claim delay for unbound identities	>= 7 days	MPP	Bound identities claim without delay.

13.2.4 BTC Yield and Vault Parameters

Symbol	Name	Default or Bounds	Governance	Notes
alpha_vault	Share of protocol revenue to BTC Vault	policy corridor	MPP in Bucket A	Streams PBTC-denominated yield to depositors.
tau_vault_act	BTC Vault activation criteria	policy checklist	MPP in Bucket A	Preconditions for turning on distributions.
tau_vault_pause	BTC Vault pause criteria	policy checklist	EMPP within scope	Safety stop during exogenous stress.
rho_vault_fees	Fee conversion policy	transparent schedule	MPP in Bucket A	Conversion path to PBTC prior to distribution.

13.2.5 Stablecoin Parameters and Risk Limits

Symbol	Name	Default or Bounds	Governance	Notes
CR_min	Minimum collateral ratio	per-asset policy	MPP	Health must satisfy CR >= CR_min to mint.
CR_warn	Warning threshold	policy margin	MPP	Triggers alerts and soft nudges.
CR_liq	Liquidation threshold	less than CR_min	MPP	Positions below are liquidated.
pi_liq	Liquidation penalty	policy range	MPP	Paid by under-collateralized positions.
L_queue	Redemption queue limit	quantity per 24 h	MPP	Smooths redemptions, avoids run dynamics.
delta_oracle	Oracle deviation bound	basis-points band	MPP	Automatic freeze or failover if exceeded.
tau_oracle	Oracle heartbeat	policy interval	MPP	Required update cadence.
Gamma_EMPP	Stability EMPP triggers	enumerated set	Fixed scope via MPP	Defines emergency actions allowed in EMPP for stability.

Stablecoin health CR = value(collateral) / debt. Minting requires CR >= CR_min. Liquidation begins when CR < CR_liq. Oracles use medianization and bounds (delta_oracle, tau_oracle).

13.2.6 Bridge and Migration Parameters

Symbol	Name	Default or Bounds	Governance	Notes
tau_anchor	Target anchor publication SLO	policy interval	MPP	Maximum acceptable time to publish FAC.
N_overlap	Migration overlap epochs	policy range	MPP	Dual-path period for anchor or DA migration.
chi_checkpoint	Cross-binding checkpoint	required	Fixed	Binds last-old to first-new anchor at cutover.
R_retrieval	Legacy retrievability window	retained per policy	MPP	Ensures access to historical artifacts post-cutover.
I_index	Unified FAC index	enabled	Fixed	Single canonical index across overlap and post-cutover.

13.2.7 Activation, Warm-Up, and Safety Mode

Symbol	Name	Default or Bounds	Governance	Notes
T_warmup	Gauge warm-up window	14 days	Fixed	No emissions stream during warm-up.
E_escrow	Warm-up escrow accumulator	per-epoch	Automatic	Holds notional emissions until activation or veto.
beta_early	Early-LP bonus on activation	+15%	TPP within bounds	Applies to LP positions during

Symbol	Name	Default or Bounds	Governance	Notes
				first 14 days after activation.
rho_escrow_veto	Escrow disposition on veto	100% to DAO	Fixed	No payments to LPs or voters if vetoed.
tau_safety	Safety mode duration	policy window	EMPP	Hardening window with constrained actions.
Omega_veto	Veto committee threshold	4 of 5	MPP	Defensive authority during warm-up only.

Activation payouts on activation, E_escrow is paid retroactively to warm-up voters using per-epoch vote snapshots. Early-LP bonus applies to LP positions during the first 14 days after activation. If vetoed, E_escrow routes 100% to DAO revenue.

13.2.8 Tokenomics and Supply Controls

Symbol	Name	Default or Bounds	Governance	Notes
B_rate	Burn gauge cap per epoch	policy cap	MPP	Max portion of Bucket B allocable to burn.
K_buy	Buyback budget cap	policy cap	MPP or TPP	Treasury buybacks with reporting and rails.
R_route	Routing rebate rate for PRML legs	0.05% default	MPP	Optional fee rebate for PRML-leg routes.

Symbol	Name	Default or Bounds	Governance	Notes
V_floor	Validator emissions floor (of total)	>= 50%	Fixed	Enforced across HV fixed plus NV Bucket B distributions.
tau_lock	Max ve lock duration	policy max	MPP	Upper bound for vePRML and veBTC locks.
delta_base	Standard vote decay	linear to 0	Fixed function	Applies to all unbound ve positions.
delta_bind	Bound veBTC vote decay	0.5 * delta_base while valid	TPP within bounds	Applies only to veBTC bound to an HV identity in good standing.
rho_HV	HV revenue share for delegated binding	0% to 25% typical	Market within TPP caps	Visible offer that attracts veBTC bindings.
k_bind	HV binding capacity	operator-declared	MPP caps	Maximum total veBTC bound to an HV.
tau_rebind	Rebinding cooldown	7 days	MPP	Prevents rapid churn and gaming.

13.3 Appendix A – Formulas and Identities

This appendix collects the core identities for reference. Symbols match Section 3.

A.1 Emission path

E_epoch(t+1) = E_epoch(t) * g(phi , mu(t))

- phi is the dampening scalar within a bounded corridor.
- mu(t) are bounded macro indicators such as utilization and validator participation.

- Annual emission never falls below Emin.

A.2 Allocation order per epoch

1. Reserve fixed: S_HV, S_Build, S_Backstop.
2. Compute buckets: E_A = S_A * E_epoch, E_B = S_B * E_epoch.
3. Enforce validator floor: S_HV + NV_from_B >= V_floor * E_epoch.
4. Apply warm-up and veto.
5. Stream per-gauge emissions.

A.3 Validator floor

S_HV(t) + NV_from_B(t) >= V_floor * E_epoch(t)

A.4 Withheld-subsidy rule

If block invalid or missed: withhold E_block and add to Sigma_withheld. On next valid block: burn psi_burn * Sigma_withheld and send psi_DAO * Sigma_withheld to DAO; set Sigma_withheld = 0; then pay cohort split for current E_block.

A.5 Base-fee update (EIP-1559 style)

F_{n+1} = max(F_min , F_n * (1 + (gasUsed_n − G_target) / (G_target * D_bf)))

- Base-fee burn per block n: gamma_fee * F_n * gasUsed_n.
- Proposer tips per block n: eta_tip * tip_n * gasUsed_n.

A.6 Net issuance

B_total(t) = B_gauge(t) + B_fee(t) + B_withheld(t) E_net(t) = E_epoch(t) − B_total(t)

A.7 Collateralization thresholds

CR = value(collateral) / debt Mint if CR >= CR_min Liquidate when CR < CR_liq

A.8 Bridge revenue contribution

R_DAO(t) = R_gas(t) + R_dex(t) + R_liq(t) + R_bridge(t) + psi_DAO * Sigma_withheld(t_release) + R_veto(t)

13.4 Appendix B – Glossary of Terms

- **Attester committee** – HV subset that verifies a candidate block and participates in Sigma_HV.

- **AuxPoW anchoring** – posting FAC pointers as merge-mined tag commitments on a Bitcoin-aligned substrate.
- **Backstop Vault** – reserve funded every epoch from S_Backstop, deployed only by EMPP, with replenishment priority.
- **Bond NFT** – transferable delegation record that binds capital to a validator without moving Identity.
- **Bucket A** – governed share S_A for liquidity and BTC Vault, co-governed by veBTC and vePRML at w_A = [0.5, 0.5].
- **Bucket B** – governed share S_B for validators, infrastructure, Treasury, Burn and Buyback gauges, governed by vePRML.
- **Builder committee** – HV subset that constructs block candidates.
- **E_block** – nominal per-block reward unit for HV cohorts, split by theta_P, theta_B, theta_A.
- **FAC** – Finality Anchor Commitment binding state root, proof reference, Sigma_HV, and metadata; posted via AuxPoW tag.
- **Identity NFT** – soulbound identifier that aggregates ve positions and carries reputation for quadratic weighting and selection caps.
- **NV** – Network Validator performing verification, finality, and committee duties.
- **PBTC** – protocol-native representation of bonded BTC for use on PrimeLayer.
- **pUSD** – over-collateralized stablecoin primarily backed by PBTC.
- **POL** – protocol-owned liquidity, governed like any LP position and subject to warm-up.
- **Proposer** – HV that sequences a block, earns priority tips, and participates in cohort rewards.
- **Sigma_HV** – aggregate HV signatures over the verified epoch's blocks.
- **Stability Pool** – DAO-governed pool that absorbs liquidations using pUSD under policy.
- **veBTC** – vote-escrowed PBTC that co-governs Bucket A only.
- **vePRML** – vote-escrowed PRML that governs Bucket B and co-governs Bucket A.
- **Veto Committee** – defensive body that can block risky gauges during warm-up under explicit criteria.
- **VRF sortition** – verifiable random selection of per-block HV committees.

13.5 Appendix C – Tables and Diagram Identifiers

Use these stable identifiers to link figures and tables in the production PDF or web build.

Tables

- T-1 – Emission allocation order and invariants
- T-2 – Governance quorums, thresholds, cooldowns
- T-3 – Validator cohort and reward parameters
- T-4 – Bucket A and B gauge catalogs and caps
- T-5 – BTC Vault parameters and revenue ledger fields

- T-6 – Stablecoin collateral, liquidation, oracle bounds
- T-7 – Bridge stage parameters and cutover checklist
- T-8 – Treasury programs, buyback and burn caps
- T-9 – Observability and evidence bundle fields

Diagrams

- D-1 – Execution to anchoring: tx → block → pi_epoch → FAC
- D-2 – HV cohort: proposer, builder, attester roles
- D-3 – Gauge lifecycle: proposal → warm-up → escrow → activation or veto
- D-4 – Emission flows: fixed slice and buckets with validator floor
- D-5 – BTC Vault flow: DAO revenue → conversion → PBTC distribution
- D-6 – pUSD liquidation pipeline and Stability Pool
- D-7 – Bridge stages: FB → SFB → ZK-GC with overlap and checkpoints
- D-8 – Migration Type 1 to 3 flows and evidence

13.6 Plain-Language Summary

- The references show where the core ideas come from: Bitcoin for settlement, EVM and EIP-1559 for execution and fees, zk proofs and garbled circuits for verification, and established designs for liquidations, oracles, and voting.
- The appendices collect the main formulas and definitions in one place so that engineers and reviewers can check the math and vocabulary quickly.
- Figure and table identifiers make it easy to keep the visuals in sync with the text and to cross-reference them during review and implementation.

13.7 Document Status and Parameter Finalization

This Bluepaper is a living technical specification. Structures and invariants are intended to be stable, while specific parameter values, ceilings, and corridors are designated by on-chain governance and will be reflected in the forthcoming Whitepaper and in the genesis parameter registry. Where discrepancies arise between this document and the on-chain registry, the on-chain configuration prevails. Any change to constitutional surfaces requires an MPP with elevated thresholds or, where permitted, an EMPP within its narrow scope, followed by public evidence and audit reporting.