

Governance

Calyx is designed not just as a protocol, but as an **open trust infrastructure**. Governance ensures that verifiers, entities, and stakeholders operate within clear, transparent rules that safeguard credibility and prevent misuse.

1. Verifier Accreditation

- **Eligibility** – Only accredited verifiers (auditors, certification bodies, qualified experts) can mint BUDS.
- **Onboarding** – Each verifier must complete KYC/AML checks and sign the Calyx Verifier Agreement.
- **Tiered Permissions** – Verifiers may operate at different levels (e.g., Tier 1: company-level audits, Tier 2: system-wide audits).
- **Revocation** – Misuse, negligence, or conflict of interest may result in suspension or removal of verifier status.

2. Protocol Updates

- **Open Specification** – The Arc™, Matrix™, and Attribution Ledger formulas are public and versioned on GitHub.
- **Proposal Process** – Any participant can propose changes via a **Calyx Improvement Proposal (CIP)**.
- **Consensus** – Protocol-level changes require review and approval by a governance council (see below).
- **Backward Compatibility** – Once minted, BUDS remain valid; formula updates affect only new issuance.

3. Governance Council

- **Composition** – Representatives from verifiers, technical maintainers, and ecosystem partners.
- **Mandate** – Approve or reject CIPs, accredit new verifier categories, and oversee security audits.
- **Transparency** – Council decisions and rationales are published openly on-chain and in governance forums.

4. Attribution & Lineage Rules

- **Propagation** – Proof may propagate across entities, but attribution must always be preserved.

- **No Double Counting** – Governance enforces that a verification cannot be claimed by multiple entities independently.
- **Lineage Ledger** – Maintained immutably on-chain to guarantee provenance.

5. Dispute Resolution

- **Challenge Mechanism** – Any entity may challenge a verification if evidence contradicts the claim.
- **Verifier Review** – The original verifier must respond within a set timeframe.
- **Council Arbitration** – If unresolved, the Governance Council rules on validity; outcomes are final and recorded on-chain.

6. Security Oversight

- **Audits** – Independent security and math audits of the protocol occur regularly.
- **Bug Bounties** – Open program for researchers to report vulnerabilities.
- **Incident Response** – Clear escalation paths for technical or procedural failures.

7. Incentive Alignment

- **Verifiers** – Earn BUDS and reputation for every trusted verification.
- **Entities** – Gain compounded BUDS when proofs align.
- **Ecosystem** – Shared incentives reduce the temptation to misreport and reward long-term credibility.