



TECHNICAL STANDARD

Aletheia Protocol Standard 01: StableChain Consensus & Settlement

Published	12 June 2026
Status	Under Development
Ledger hash	0x4489021fa89023ebc87201948ea20914bca890214890ec8201948ea20914801e

This standard specifies the consensus, settlement and verification rules of StableChain, the national ledger of the Sovereign Covenant State. Draft for engineering review; normative language follows RFC 2119.

1. Scope

APS-01 governs block production, finality, fee determination and the verification of state registry records. It does not govern the monetary policy of the AEY, which is set by the Monetary Architecture & Reserve Backing Act.

2. Validator set

Consensus SHALL be operated by state-authorised validators partitioned across at least three physically separate facilities. The validator set and each validator public key SHALL be published in the State Key Directory.

A change to the validator set REQUIRES a signed decree published in the Official Gazette at least one epoch before it takes effect.

3. Slots and finality

Time is divided into slots of 500 milliseconds. A block proposed in a slot is final once it has been attested by more than two thirds of the validator weight; there is no probabilistic finality and no reorganisation of final blocks.

An epoch comprises 86,400 slots (12 hours). Reserve attestations and the Auditor-General receipts digest are produced at each epoch boundary.

4. Fees

Settlement fees SHALL be fixed in AEY by statutory schedule and SHALL NOT vary with network demand. Fee revenue accrues to the Treasury and is reported in each epoch digest.

5. Reserve invariants

Validators SHALL evaluate the twelve monetary invariants (I1–I12) before finalising any block that mints or burns AEY. If any invariant fails, validators SHALL halt minting and burning until the Monetary Board publishes a signed remediation.

6. Registry verification

State registries (land, companies, identity credentials, Gazette entries) SHALL store records off-ledger and inscribe only the SHA-256 hash of each record together with a timestamp and the signing key.

Any person MAY verify a record by recomputing its hash and checking the inclusion proof against a finalised block. Personal data SHALL NOT be written to the ledger.

7. Security

Validator keys SHALL be held in hardware security modules. The Aletheian Cybersecurity Department SHALL operate continuous monitoring and a coordinated vulnerability disclosure programme for the protocol.

Ministry of Digital State & Registries — Protocol Standards Board

Public register entry APS-01