KRYONIS SOVEREIGN SYSTEMS LIMITED

Proof-of-Physical-State

Verification Methodology

PoPS Consensus Specification

Three-Tier Data Architecture, Confidence Scoring, and Dispute Resolution

Biological Computing Control Standard (BCCS) — Document 03

Version 2.0 | April 2026

kryonislab.org | bccs.bio

1. Introduction

Proof-of-Physical-State (PoPS) is the consensus mechanism through which the BCCS protocol verifies biological state transitions on-chain. Unlike Proof-of-Work (computational puzzle) or Proof-of-Stake (capital lock), PoPS achieves consensus through multi-source physical evidence about the real-world state of biological assets.

This document specifies the verification methodology: how biological state data enters the protocol, how validators evaluate evidence, how consensus is reached, how disputes are resolved, and how economic incentives enforce truthful reporting.

2. Three-Tier Verification Architecture

A state transition is confirmed when at least 2 of 3 independent data tiers agree on the new state within a configurable evidence window (default: 72 hours). If only 1 tier submits, the transition enters “pending” state. If tiers conflict, the transition enters “disputed” state and triggers challenge resolution.

Tier	Source	Data Types	Automation
Tier 1	Satellite / Remote Sensing	Spectral imagery, synthetic aperture radar (SAR), thermal anomaly detection, NDVI vegetation indices. Sources: Sentinel-2, Landsat, Planet Labs, MODIS.	Automated pipelines
Tier 2	Ground Sensors / IoT	Soil moisture, air quality, water pH, biomass density, temperature, humidity. Semi-automated data feeds from distributed sensor networks.	Semi-automated
Tier 3	Physical Inspection	On-site human verification with photographic evidence, timestamped GPS coordinates, standardized reporting forms. Required for initial registration and disputed transitions.	Human-verified

2.1 Why Three Tiers

Single-source verification is architecturally insufficient for biological state. Satellite imagery captures surface appearance but not ecological function — a green canopy may conceal a dying ecosystem. Ground sensors provide continuous monitoring but cover limited areas. Physical inspection is high-confidence but expensive and infrequent. The three-tier model combines breadth (Tier 1), depth (Tier 2), and ground truth (Tier 3).

3. Verification Flow

The end-to-end verification flow proceeds as follows: a physical world event occurs (fire, growth, degradation, seasonal change). Sensor, satellite, or inspector captures evidence data. Data is submitted to the BCCS oracle contract on Base. The multi-source consensus check evaluates whether 2 of 3 tiers agree. If consensus is reached, the state transition is recorded on-chain, the BAIN ID State Checksum is updated, and the new verified state becomes queryable via the API. AI agents and institutions query the state and pay verification fees in $BCCS.

3.1 Evidence Submission Requirements

Tier	Required Evidence	Minimum Confidence
Tier 1	Spectral data with timestamp, satellite pass ID, coverage area, classification result	0.85

Tier 2	Sensor readings with device ID, calibration date, GPS coordinates, data range	0.80
Tier 3	Photographs with EXIF data, GPS coordinates, inspector credentials, standardized form	0.90

4. Confidence Scoring Model

Each verification submission receives a confidence score between 0.0 and 1.0. The composite confidence for a state transition is calculated as the weighted average of contributing tier scores. Default weights: Tier 1 (0.30), Tier 2 (0.30), Tier 3 (0.40). Physical inspection carries higher weight due to ground-truth authority.

A state transition is accepted when composite confidence exceeds the asset-class threshold. Default threshold: 0.75. Higher-value or higher-risk asset classes may require elevated thresholds configurable through protocol governance.

Confidence scores are recorded on-chain with each state transition and exposed via the API. Consumers can filter query results by minimum confidence level.

5. Validator Participation

Validators are licensed node operators who have activated an Infrastructure Access License and staked $50,000 worth of $BCCS into the oracle contract. Staking creates economic alignment — validators have direct financial exposure to the accuracy of their submissions.

Parameter	Value	Rationale
Minimum Stake	$50,000 in $BCCS	Economic barrier against Sybil attacks and false data
Lock Period	90 days from first submission	Prevents hit-and-run oracle manipulation
Unstaking Cooldown	14 days	Allows challenge window for recent submissions
Inactivity Penalty	1% per week after 30 days	Prevents stake-without-work free-riding

6. Slashing Conditions

Economic slashing enforces truthful reporting. All slashed $BCCS is permanently burned (sent to 0x000...dead), creating a deflationary mechanism proportional to network dishonesty.

Offense	Slash %	Evidence Required	Burned
False data submission	10%	Counter-evidence from 2+ validators	100% burned
Duplicate/copied data	5%	Hash collision detection	100% burned
Inactivity (30+ days)	1%/week	Automatic (no submission logged)	100% burned
Collusion (coordinated false data)	25%	Pattern analysis + counter-evidence	100% burned

Estimated annual burn rate from slashing: 0.1–0.5% of circulating supply, depending on network size and validator behavior. This creates structural deflation independent of query-driven buy-and-distribute mechanics.

7. Challenge and Dispute Resolution

Any licensed validator can challenge a pending state transition by submitting counter-evidence from at least 2 tiers. The challenge resolution process:

Step	Action	Timeline
1	Challenger submits counter-evidence with stake deposit (2% of own stake)	Within evidence window
2	Counter-evidence evaluated against original submission by validator network	48 hours
3	Consensus check: which evidence set achieves higher composite confidence	Automatic
4a	Challenger wins: original submitter slashed, challenger receives 50% of slash	Immediate
4b	Challenger loses: challenger's 2% deposit slashed and burned	Immediate

The economic design ensures that challenges are only initiated when the challenger has high confidence in counter-evidence. Frivolous challenges are penalized. Successful challenges are rewarded. This creates a self-correcting verification market.

8. Expected Error Rates and Limitations

No verification system achieves zero error. The PoPS methodology is designed to minimize Type I errors (false state change accepted) through multi-source consensus, and Type II errors (true state change rejected) through the challenge mechanism.

Error Type	Definition	Mitigation	Target Rate
Type I	False positive: incorrect state accepted	2-of-3 tier consensus + slashing	< 2%
Type II	False negative: correct state rejected	Challenge mechanism + bounties	< 5%
Latency	Delay between event and on-chain record	72h evidence window, Tier 1 automation	< 7 days

These are design targets. Actual error rates depend on validator quality, sensor coverage, and satellite revisit frequency. Error rates are published transparently per asset class as the network matures.

9. Future Extensions

The PoPS methodology is designed for extensibility. Planned enhancements include: AI-assisted anomaly detection for Tier 1 data (automated flagging of spectral anomalies), cross-asset correlation analysis (detecting ecosystem-level changes across adjacent BAIN IDs), dynamic confidence weighting (adjusting tier weights based on historical accuracy per region), and integration with emerging environmental monitoring infrastructure (drone networks, underwater sensors, atmospheric sampling).

KRYONIS Sovereign Systems Limited — Hong Kong | kryonislab.org | bccs.bio