# Veritas Consensus Protocol

**Abstract**

A consensus mechanism where voice equals risk. Participants stake capital to gain influence. Belief Decomposition aggregates opinions, Bayesian Truth Serum scores accuracy, and stake redistribution rewards truth-tellers.

## 1 Stake System

Influence in consensus is proportional to capital at stake.

### 1.1 Stake and Lock Definitions

Each participant maintains:

- **Global stake** $S_i$ = total at-risk capital across all markets
- **Per-market lock** $L_{i,m}$ = locked capital in market $m$

Lock amount = 2% of last buy amount in that market.

### 1.2 Solvency Invariant

Total stake must cover all lock requirements:

$$S_i \geq \sum_{\text{all markets}} L_{i,m} \tag{1}$$

### 1.3 Automatic Collateralization

On trade execution:

$$\text{Skim} = \max\left(0, \sum_m L_{i,m}^{\text{new}} - S_i\right) \tag{2}$$

Skim is collected atomically with the trade only when total lock requirement exceeds current stake.

### 1.4 Epistemic Weight

Voting weight in each market equals locked capital:

$$w_i = L_{i,m} \tag{3}$$

# 2 Belief Decomposition

Extracts shared knowledge from diverse opinions.

## 2.1 Input Requirements

Each participant provides:

- Belief $p_i$ (e.g., 0.7 for 70% confidence)
- Meta-prediction $m_i$ (prediction of population average)

## 2.2 Local Expectations Matrix

Calculate belief-prediction correlations:

$$w_{11} = \text{weighted avg}(p_i \times m_i \mid p_i = 1) \tag{4}$$

$$w_{21} = \text{weighted avg}(p_i \times m_i \mid p_i = 0) \tag{5}$$

## 2.3 Common Prior

Extract shared baseline before evidence:

$$\pi = \frac{w_{21}}{w_{21} + (1 - w_{11})} \tag{6}$$

## 2.4 Aggregate Belief

Combine beliefs with prior correction:

$$A = \frac{\prod_i p_i^{\hat{w}_i} / \pi^{\sum \hat{w}_i}}{\prod_i p_i^{\hat{w}_i} / \pi^{\sum \hat{w}_i} + \prod_i (1 - p_i)^{\hat{w}_i} / (1 - \pi)^{\sum \hat{w}_i}} \tag{7}$$

## 2.5 Certainty Measure

Agreement level from Jensen-Shannon divergence:

$$c = 1 - [H(A) - \sum_i \hat{w}_i H(p_i)] \tag{8}$$

where $H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$. High certainty amplifies redistribution.

# 3 Bayesian Truth Serum

Measures information contribution of each participant.

## 3.1 Score Formula

$$s_i = D_{\mathrm{KL}}(p_i \| \bar{m}_{-i}) - D_{\mathrm{KL}}(p_i \| \bar{p}_{-i}) - D_{\mathrm{KL}}(\bar{p}_{-i} \| m_i) \tag{9}$$

where $\bar{p}_{-i}$ and $\bar{m}_{-i}$ are leave-one-out aggregates excluding agent $i$.

Positive scores indicate informative, accurate contributions. Negative scores indicate noise.

## 3.2 Zero-Sum Property

Weighted scores sum to zero:

$$\sum_i w_i \times s_i = 0 \tag{10}$$

Creates natural winner and loser sets for redistribution.

# 4 Stake Redistribution

## 4.1 P90 Normalization

Compute 90th percentile scale factor:

$$k = \max(\text{P90}(|s_1|, |s_2|, \ldots, |s_n|), 0.1) \tag{11}$$

Normalize scores to $[-1, 1]$:

$$\hat{s}_i = \text{clamp}\left(\frac{s_i}{k}, -1, +1\right) \tag{12}$$

Prevents outliers from dominating redistribution.

## 4.2 Slashes and Rewards

For losers (negative scores):

$$\text{Slash}_i = c \times |\hat{s}_i| \times w_i \tag{13}$$

For winners (positive scores):

$$\text{Reward}_i = \frac{\text{your signal strength}}{\text{total signal strength}} \times \text{total slashed} \tag{14}$$

## 4.3 Bounded Risk

You can never lose more than your lock in any single market:

$$\text{Slash}_i \leq L_{i,m} \tag{15}$$

# 5 ICBS Prediction Markets

## 5.1 Market Structure

Each belief market has LONG and SHORT tokens. Traders buy LONG to express confidence, SHORT to express skepticism.

## 5.2 Inverse Coupling

When you buy LONG, SHORT gets cheaper.

When you buy SHORT, LONG gets cheaper.

This prevents pure hype spirals.

## 5.3 Market Prediction

The market's consensus forecast:

$$q = \frac{\text{LONG reserves}}{\text{LONG reserves} + \text{SHORT reserves}} \tag{16}$$

## 5.4 Settlement

At epoch end, compare market prediction $q$ to BD score $x$:

**If LONG was right** ($x > q$):

- LONG reserves grow by factor $x/q$
- SHORT reserves shrink by factor $(1-x)/(1-q)$

**If SHORT was right** ($x < q$):

- SHORT reserves grow
- LONG reserves shrink

Total value locked stays constant. No tokens minted or burned.

# 6 Game Theory

## 6.1 Nash Equilibrium

Rational traders buy LONG when they believe:

$$\mathbb{E}[\text{BD score}] > q \tag{17}$$

At equilibrium, the market prediction equals expected truth:

$$q = \mathbb{E}[x] \tag{18}$$

## 6.2 Optimal Strategy

Rational participants trade based on expected BD score relative to market prediction:

$$\mathbb{E}[x] > q \implies \text{buy LONG} \tag{19}$$

$$\mathbb{E}[x] < q \implies \text{buy SHORT} \tag{20}$$

$$\mathbb{E}[x] = q \implies \text{hold} \tag{21}$$

## 6.3 Sybil Resistance

Identity fragmentation provides no advantage. Total epistemic weight and expected rewards remain invariant under capital splitting:

$$\sum_{j \in \text{sybils}} w_j = w_{\text{original}}, \quad \sum_{j \in \text{sybils}} \mathbb{E}[\Delta S_j] = \mathbb{E}[\Delta S_{\text{original}}] \tag{22}$$

# 7 Protocol Lifecycle

## 7.1 Trade Execution

Agent buys tokens, triggering lock calculation ($L = 0.02 \times \text{amount}$). If total lock requirement exceeds current stake, skim is collected atomically. Lock replaces previous lock for that position.

## 7.2 Epoch Processing

Participants submit beliefs $p_i$ and meta-predictions $m_i$. BD computes aggregate $A$ and certainty $c$. BTS scores $s_i$ are calculated. P90 normalization applied. Stakes redistributed via certainty-weighted slashes and proportional rewards.

## 7.3 Position Closure

Agent sells tokens to zero balance. Lock $L_{i,m}$ is released. Excess stake becomes withdrawable:

$$\text{Withdrawable} = S_i - \sum_{m \in \text{active}} L_{i,m} \tag{23}$$

# 8 Key Properties

The protocol exhibits the following properties:

- **Proportional influence**: Epistemic weight directly proportional to capital at risk
- **Automatic collateralization**: Seamless stake management via conditional skimming
- **Bounded risk**: Maximum loss per market bounded by lock amount
- **Zero-sum dynamics**: Total stake preserved across redistribution
- **Incentive compatibility**: Nash equilibrium at truthful reporting
- **Sybil resistance**: No advantage from identity fragmentation