# ELPIS

PROTOCOL

## YELLOW PAPER

*Technical Specification*

Version 1.0 | January 2025

Formal definitions, parameters, and algorithms

elpistruth.org

# Contents

# 1. Notation and Definitions

## 1.1 Symbols

| Symbol | Definition |
|---|---|
| `C` | Content item (submission) |
| `S_c` | Stake amount for content C (in satoshis) |
| `R_c` | Self-assessed relevance score [1.00, 10.00] |
| `P(A\|C)` | Probability of accuracy for content C [0.00, 1.00] |
| `V_c` | Viewership volume for content C |
| `O_i` | Oracle i |
| `T_o` | Track record score for oracle O [0.00, 1.00] |
| `t_pub` | Publication timestamp (Unix epoch) |
| `t_settle` | Settlement timestamp (Unix epoch) |

## 1.2 Content Types

**RESOLVABLE:** Content with determinable ground truth. Settles at t_settle when evidence emerges.

**PERSISTENT:** Content that never formally settles. t_settle = ∞. Earns indefinitely based on viewership.

# 2. Protocol Parameters

## 2.1 Staking Parameters

| Parameter | Value | Notes |
|---|---|---|
| `MIN_STAKE` | 1 sat | User-defined minimum |
| `MAX_STAKE` | No limit | Market-determined |
| `RELEVANCE_MIN` | 1.00 | Lowest relevance tier |
| `RELEVANCE_MAX` | 10.00 | Highest relevance tier |

***Note:*** *All stakes settle via Lightning Network. Users may deposit/withdraw via fiat on-ramps; internal accounting uses satoshis.*

## 2.2 Settlement Parameters

| Content Type | Delay | Trigger |
|---|---|---|
| Breaking News | 24-48 hrs | Evidence + time threshold |
| Investigation | 7-30 days | Evidence + complexity factor |
| Prediction | Variable | Event occurrence |
| Persistent/Evergreen | ∞ | Never settles |

## 2.3 Revenue Distribution Parameters

| Recipient | Share | Type |
|---|---|---|
| `CONTRIBUTOR_SHARE_MIN` | 40% | Dynamic floor |
| `CONTRIBUTOR_SHARE_MAX` | 60% | Dynamic ceiling |
| `ORACLE_SHARE` | 10% | Fixed |
| `PLATFORM_SHARE` | Remainder | 30-50% (inverse of contributor) |

# 3. Core Algorithms

## 3.1 Probability Aggregation

Oracle assessments are aggregated using weighted average based on track record:

$$P(A|C) = \Sigma \, [ \, P\_i(A|C) \times T\_i \times S\_i \, ] \, / \, \Sigma \, [ \, T\_i \times S\_i \, ]$$

Where P_i is oracle i's probability assessment, T_i is oracle i's track record score, and S_i is oracle i's stake on the assessment.

## 3.2 Contributor Payout Calculation

For accurate content that passes settlement:

$$\text{Payout\_c} = (\text{V\_c} \, / \, \text{V\_total}) \times \text{Revenue\_pool} \times \text{Contributor\_share}$$

Where V_c is viewership for content C, V_total is total platform viewership, Revenue_pool is total platform revenue for the period, and Contributor_share is the dynamic share (40-60%) based on aggregate relevance.

## 3.3 Oracle Track Record Update

After each settlement, oracle track records update using exponential moving average:

$$\text{T\_new} = \alpha \times \text{Calibration\_score} + (1 - \alpha) \times \text{T\_old}$$

Where α = 0.1 (learning rate) and Calibration_score measures how close P(A|C) was to actual outcome (0 or 1).

## 3.4 Staker Settlement

Public stakes resolve as follows:

- If ACCURATE: SUPPORT stakers split OPPOSE stakes proportionally
- If INACCURATE: OPPOSE stakers split SUPPORT stakes proportionally
- Platform takes small fee from winning pool (configurable, default 2%)

$$\text{Winner\_payout} = (\text{My\_stake} \, / \, \text{Total\_winning\_stakes}) \times \text{Losing\_pool} \times (1 - \text{fee})$$

# 4. Data Structures

## 4.1 Content Object

```
{   id: UUID,   type: "RESOLVABLE" | "PERSISTENT",   contributor: Address,   stake:
Satoshis,   relevance_self: Float[1.00-10.00],   content_hash: SHA256,
timestamp_pub: UnixEpoch,   timestamp_settle: UnixEpoch | null,   status: "LIVE" |
"SETTLED_ACCURATE" | "SETTLED_INACCURATE",   viewership: Integer,
oracle_assessments: [OracleAssessment],   public_stakes: [PublicStake] }
```

## 4.2 Oracle Assessment Object

```
{   oracle_id: Address,   content_id: UUID,   probability: Float[0.00-1.00],
confidence: Float[0.00-1.00],   stake: Satoshis,   timestamp: UnixEpoch }
```

## 4.3 Public Stake Object

```
{   staker: Address,   content_id: UUID,   position: "SUPPORT" | "OPPOSE",   amount:
Satoshis,   timestamp: UnixEpoch }
```

## 4.4 Oracle Object

```
{   id: Address,   track_record: Float[0.00-1.00],   total_assessments: Integer,
total_stake_won: Satoshis,   total_stake_lost: Satoshis,   registered_at: UnixEpoch }
```

# 5. Security Model

## 5.1 Attack Vectors and Mitigations

| Attack | Mitigation |
|---|---|
| Spam submissions | Minimum stake requirement creates economic cost |
| Oracle collusion | First defector captures bounties; permissionless entry |
| Wealthy attacker | Asymmetric cost: lies cost more to maintain than truth |
| Sybil attack | Track record accumulation is slow; multiple identities don't help |
| Viewership gaming | Bot detection; viewership quality metrics; cost of fake views |

## 5.2 The Thermodynamic Floor

All attacks ultimately require acquiring Bitcoin, which requires energy expenditure. The cost of sustained misinformation campaigns is denominated in joules. At sufficient scale, even nation-states face resource constraints.

**Truth is Lindy. True claims cost nothing to defend because reality defends them. The asymmetry favors honesty over time.**

# 6. Appendix

## 6.1 Glossary

- **Lindy Effect:** The longer something has survived, the longer it's expected to survive.
- **Thermodynamic Security:** Security derived from real-world energy expenditure that cannot be faked or reversed.
- **Calibration:** When an oracle says 70%, it should be right approximately 70% of the time.
- **Settlement:** The moment when a claim's accuracy is determined and stakes are resolved.
- **Viewership Volume (VV):** The aggregate attention a piece of content receives, used to determine merit-based payouts.

## 6.2 Version History

v1.0 (January 2025): Initial specification release.

elpistruth.org