OracleX: A Proof-of-Behavior Protocol for Decentralized Prediction Ecosystems

Dr. Elias
eliasoraclex@gmail.com

Abstract

A purely peer-to-peer version of a prediction information system would allow information to be aggregated directly from one party to another without going through a centralized institution to provide liquidity or adjudicate outcomes. Existing Decentralized Prediction Markets (DPMs), while providing part of the solution, lose their main benefits as an information discovery machine [4] if a fragile incentive mechanism is still required to attract liquidity and ensure honest participation. We term this ”The Oracle Paradox.”

This paper proposes a solution to this paradox using a ”Proof-of-Behavior” (PoB) protocol. The network utilizes a dual-token algorithmic stability model (OEX/USDX) to bind user prediction behavior with staking-based mining. This mechanism ensures that only sustained, high-quality participation is incentivized, thereby systematically resolving the conflict between liquidity incentives and information veracity.

1. Introduction

Commerce on the Internet, such as polling or expert forecasting, has come to rely almost exclusively on trusted third parties to organize, incentivize, and publish results. While this system works well enough for most cases, it still suffers from the inherent weaknesses of the trust-based model [1]. Centralized institutions inevitably incur high costs to incentivize participants, and their processes lack transparency, making outcomes susceptible to manipulation.

Decentralized Prediction Markets (DPMs) attempt to solve this problem, but mainstream DPMs currently face four major bottlenecks:

1. **Liquidity Crisis:** Insufficient trading depth, leading to inefficient price discovery.
2. **Incentive Gap:** Singular incentive models (i.e., profit from correct predictions alone), lacking a sustainable system for user engagement.
3. **Value Disconnect:** Difficulty in securely and reliably feeding off-chain event outcomes onto the chain.
4. **Centralized Governance:** Decision-making power is concentrated among a few entities.

What is needed is a prediction system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party [1].

In this paper, we propose a solution to the DPM incentive gap and liquidity problem using a peer-to-peer network and a ”Proof-of-Behavior” (PoB) protocol. This system generates computational proof of incentives for time-based prediction behaviors through an algorithmically stable dual-token model. The system is secure as long as participants find it more profitable to follow the rules (i.e., provide high-quality predictions) than to attack the system.

2. Core Components

We define a decentralized prediction ecosystem as a closed-loop system driven by two core tokens: OEX and USDX.

- **OEX:** The core equity token of the system. Its total supply is fixed. OEX serves as the cornerstone for network governance and for accessing incentives.
- **USDX:** The stable medium of exchange within the system, pegged to 1 USDT. USDX is used for the denomination and settlement of all prediction activities, mitigating the volatility of the broader crypto market.

USDX cannot be purchased directly; it must be minted by staking OEX. This mechanism creates a mandatory link between the core equity (OEX) and the liquid medium of exchange (USDX).

3. Proof-of-Behavior (PoB) Protocol

The solution we propose begins with a ”behavioral protocol mining” mechanism. This is a novel consensus mechanism intended to quantify and incentivize high-quality information contributions, rather than incentivizing pure computational power consumption like Proof-of-Work (PoW) [2].

3.1 Protocol Logic

The operational logic of the protocol is as follows:

- **Staking and Minting:** A user must first stake OEX. Concurrently, the system mints USDX according to a specific ratio (see Section 4.1).
- **Proof of Valid Behavior:** The user must complete at least one prediction action daily (e.g., selecting ”Yes” or ”No” for an event). This action is considered ”Proof of Valid Behavior” and is a prerequisite for activating mining incentives.

- **Dynamic Yield:** The system's incentive (newly released OEX) is not fixed. The yield rate is dynamically adjusted based on the user's prediction accuracy, participation frequency, and transaction volume.
- **Unstaking:** If a user wishes to redeem their staked OEX, they must return the full amount of USDX they minted. The returned USDX is then burned to maintain system equilibrium.

3.2 Mining Algorithm

A user's daily mining yield R_D is determined by their staked amount S_A and the final daily yield rate R_F:

$$R_D = S_A \cdot R_F$$

The final daily yield rate R_F is a composite of a base yield rate R_B and a dynamic adjustment factor A_D:

$$R_F = \text{max}(0, R_B + A_D)$$

3.2.1 1. Base Yield Rate (R_B)

R_B depends on the user's staking period T_P (e.g., 1 to 360 days) and undergoes exponential decay based on the total amount of tokens already mined M_D, smoothly controlling inflation.

$$R_B = R_{B0}(T_P) \cdot e^{-\alpha \cdot (M_D / M_{\text{max}})}$$

Where $R_{B0}(T_P)$ is the initial base rate determined by the staking period (e.g., $R_{B0} = 0.011$ for $T_P = 360$), α is the decay speed coefficient, and M_{max} is the total OEX mining pool supply.

3.2.2 2. Dynamic Adjustment Factor (A_D)

A_D is the direct feedback for the quality of the user's behavior, fluctuating within the range $[-0.002, +0.002]$. It is determined by a composite score S_C:

$$A_D = 0.002 \cdot (2 \cdot S_C - 1)$$

S_C is the weighted score of user behavior, with a range of $[0, 1]$:

$$S_C = W_{Acc} \cdot S_{Acc} + W_{NT} \cdot S_{NT} + W_{VF} \cdot S_{VF}$$

Where:

- S_{Acc}: Prediction accuracy score.
- S_{NT}: Prediction frequency (number of times) score.
- S_{VF}: Prediction volume score.
- W: The corresponding weight coefficients, where $\sum W_i = 1$.

This design ensures that incentives (OEX mining) flow only to participants who provide valid behavior (active participation and high-quality predictions). It systematically links ”providing liquidity” (staking OEX) with ”providing high-quality information” (prediction behavior), solving the ”incentive gap.”

4. Algorithmic Minting and Stability Mechanisms

To ensure the long-term robustness of this dual-token system and prevent systemic collapse from extreme market volatility, we have designed several algorithmic safeguard mechanisms.

4.1 Dynamic Minting

The minting of USDX from staked OEX is not a fixed ratio. The value of USDX minted is determined by a dynamic ratio, ratio:

$$\text{Value}_{\text{USDX\_Minted}} = \text{ratio} \cdot \text{Value}_{\text{OEX\_Staked}}$$

The ratio is algorithmically controlled within the range $[0.1, 0.5]$ to prevent over-leveraging:

$$\text{ratio} = \text{min}(0.5, \text{max}(0.1, 0.3 \times \text{adjust}))$$

The adjustment coefficient, adjust, is a multi-parameter function that responds to market health:

$$\text{adjust} = K \times \left(\frac{M_A}{N_M}\right)^{w_1} \times \left(\frac{P_A}{N_P}\right)^{w_2} \times (1 + \text{Prem}_B)^{w_3} \times \left(\frac{V_B}{N_V}\right)^{w_4}$$

Where:

- K: A governance-controlled parameter.
- M_A, P_A: The circulating market cap and price of OEX.
- Prem_B, V_B: The market premium and trading volume of USDX.
- N: Normalization factors for each parameter.
- w: The weight for each factor (e.g., $w_1 = 0.2, w_2 = 0.3, w_3 = 0.3, w_4 = 0.2$).

This mechanism allows the supply of USDX to be elastically adjusted based on market demand and system health.

4.2 Soft Liquidation

In traditional DeFi protocols, when collateral value becomes insufficient, the system triggers a ”Hard Liquidation,” forcibly auctioning the user’s collateral [1]. This often leads to market panic and cascading liquidations.

We propose a ”Soft Liquidation” solution:

1. **Trigger Condition:** Activates when the collateralization ratio $CR_t < CR_{\text{min}}$ (e.g., 100%).

   $$CR_t = (C_t \cdot P_t)/D$$

   Where C_t is the amount of staked OEX, P_t is the price of OEX, and D is the amount of USDX minted.

2. **Core Intervention:** The system will **automatically suspend the issuance of PoB mining yields** (ΔC_t) to the user.

3. **Automatic Repair:** The suspended yields are automatically diverted into the user's staking account, increasing the collateral C_t.

   $$C_{t+1} = C_t + \Delta C_t$$

   This process continues until CR_t is restored to a safe threshold.

This mechanism avoids the market panic associated with forced liquidations and helps stabilize the price by reducing the selling pressure of OEX during a market downturn (as yields are passively locked).

4.3 Hybrid Anchor

To guarantee the stability of USDX, we employ a hybrid anchor mechanism combining algorithmic adjustment and reserve backing.

1. **Algorithmic Adjustment:** Manages the supply and demand of USDX at the market level via the Dynamic Minting mechanism (Section 4.1).

2. **Central Reserve Fund (CRF):** The protocol maintains a ”Central Reserve Fund” (CRF), analogous to a central bank, composed of fiat-backed stablecoins (e.g., USDT).

3. **Redemption Backstop:** The CRF serves as the last line of defense. In extreme scenarios, the system utilizes the CRF to guarantee a hard redemption of USDX for USDT, thereby establishing market trust and preventing a de-pegging panic.

5. Network Operation

The steps to run the network are as follows:

1. New users stake OEX and mint USDX according to the dynamic ratio.

2. Users participate in various prediction events on the platform using USDX.

3. Users complete the ”behavioral protocol” at least once daily to submit their ”Proof of Valid Behavior.”

4. The system calculates the weight of each user's PoB via the algorithm (Section 3.2) and broadcasts OEX incentives.

5. When prediction events conclude, winners who used USDX are rewarded, and the protocol collects a service fee.

6. A portion of the protocol fees will be used to buy back OEX from the secondary market and burn it, creating a deflationary mechanism.

6. Incentive

By convention, the protocol incentive consists of two parts, analogous to Bitcoin’s block rewards and transaction fees [1].

1. **OEX Mining Incentive:** As described in Section 3, this is the primary incentive in the protocol’s early stages, rewarding participants who provide high-quality behavioral proofs. This is analogous to Bitcoin’s block reward, used for network bootstrapping and security.

2. **Transaction Fee Incentive:** The protocol collects a fee (e.g., 5%) from the winning pool of all prediction events. As the OEX mining incentive decays exponentially (see Section 3.2 formula), transaction fees will gradually become the primary source of network revenue.

A portion of these fees will be used to buy back and burn OEX. This mechanism ensures the system has a continuous incentive and deflationary force even after the OEX mining phase concludes, guaranteeing long-term economic sustainability.

7. Governance and Arbitration

One of the core challenges for decentralized prediction is the resolution of real-world event outcomes, known as the ”Oracle Problem.” This protocol employs a ”Wager-Based Governance” mechanism for arbitration.

1. **Optimistic Resolution:** An event creator first submits an outcome. This outcome is subject to a challenge period.

2. **Initiating a Dispute:** Any user who disagrees with the outcome can stake a certain amount of OEX to initiate a dispute.

3. **DAO Arbitration:** Once a dispute is initiated, the DAO is activated. All DAO nodes (parties not involved in the event) who have staked OEX will vote on the outcome.

4. **Economic Penalties:** The vote result is final. The losing party (whether the creator or the challenger) will forfeit their staked OEX, which is then distributed to the winning party and the participating DAO nodes.

This mechanism uses game theory and economic stakes to incentivize honest resolutions and arbitration, making an attack on the oracle prohibitively expensive.

8. Conclusion

We have proposed a system for decentralized prediction that does not rely on trust. We started with a dual-token model, which provides control over the medium of exchange (USDX) and system equity (OEX), but is incomplete without a method to prevent the ”tragedy of the commons” (i.ie., no one being incentivized to provide liquidity and truthful information).

To solve this, we proposed a peer-to-peer network using a ”Proof-of-Behavior” (PoB) protocol to record a public, valued history of predictions [5]. As long as honest nodes (participants) find it more economically advantageous to follow the rules than to attempt to subvert the system, the system’s value-discovery function is robust. The network unifies liquidity incentives and information incentives into a single mechanism, providing a viable solution to ”The Oracle Paradox.”

References

[1] Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. (https://bitcoin.org/bitcoin.pdf)

[2] Back, A. 2002. Hashcash - a denial of service counter-measure. (http://www.hashcash.org/papers/hashcash.pdf)

[3] Dai, W. 1998. b-money. (http://www.weidai.com/bmoney.txt)

[4] Hayek, F.A. 1945. The Use of Knowledge in Society. *The American Economic Review, 35*(4), 519-530.

[5] Haber, S. and Stornetta, W.S. 1991. How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99-111.

[6] Massias, H., Avila, X.S., and Quisquater, J.J. 1999. Design of a secure timestamping service with minimal trust requirements. *In 20th Symposium on Information Theory in the Benelux*.

[7] Merkle, R.C. 1980. Protocols for public key cryptosystems. *In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society*, 122-133.