TOKEN0: A Fair-Launch Quadratic Bonding Curve Protocol

Anonymous

tokenzer0.xyz

Abstract

We present TOKEN0, a novel fair-launch token mechanism on Ethereum that implements a quadratic bonding curve as the sole price discovery mechanism. The protocol eliminates information asymmetry through mathematical price determinism, requiring no trusted third parties, no team allocation, and no presale. All ETH reserves are permanently locked in the bonding curve contract, creating a mathematically guaranteed price floor that responds proportionally to circulating supply. We demonstrate how quadratic price functions, symmetric mint/burn mechanics, and on-chain reserve management create a provably fair token issuance system where all participants interact with identical economic conditions regardless of entry timing. The protocol operates autonomously through immutable smart contract logic deployed on Ethereum mainnet.

---

1 Introduction

Decentralized finance has evolved substantially since the introduction of programmable smart contracts on Ethereum. However, the majority of token launches continue to exhibit structural inequalities that systematically disadvantage retail participants. Presale rounds, team allocations, and investor unlocks create asymmetric information environments where early access determines economic outcome independent of market participation quality.

The tragedy of the commons in token economics manifests as follows: individual rationality incentivizes early exit, collectively producing price deterioration that harms all remaining holders. Traditional token models dependent on external liquidity pools require trusted market makers and introduce manipulation vectors through concentrated liquidity positions.

We propose TOKEN0, a deflationary bonding curve protocol where the price function is entirely determined by circulating supply. The protocol implements three core principles: (1) zero privileged access — all participants interact with an identical price curve from genesis; (2) deterministic pricing — price at any supply level is mathematically fixed and publicly verifiable before any transaction; and (3) guaranteed liquidity — ETH reserves locked in the curve provide immediate burn redemption at any point in time without relying on external counterparties.

The remainder of this paper is structured as follows. Section 2 develops the mathematical model. Section 3 describes the protocol mechanics. Section 4 analyzes economic properties and incentive alignment. Section 5 addresses security considerations. Section 6 concludes.

2 Mathematical Model

2.1 Price Function

TOKEN0 employs a quadratic bonding curve, where the instantaneous spot price is a function of circulating supply s:

$$P(s) = K \times s^2$$

where $K = 1 \times 10^{-12}$ is the curve constant and $s \in [0, S_{max}]$ with maximum supply S_{max} = 1,000,000 TOKEN0. The quadratic form ensures that price appreciation accelerates as supply increases, creating stronger holding incentives at higher supply levels.

2.2 Reserve Function

The ETH reserve required to back a supply of s tokens is the integral of the price function over the supply interval [0, s]:

$$R(s) = \int_0^s P(t)\,dt = K \times s^3 / 3$$

This function defines the total ETH locked in the contract at any supply level. The reserve function is strictly monotone increasing, guaranteeing that every token minted adds ETH to the reserve and every token burned removes ETH proportionally.

2.3 Mint Cost

The gross ETH cost to mint Δs tokens when current supply is s is given by the definite integral of the price function over the minting interval:

$$C_{mint}(s, \Delta s) = R(s + \Delta s) - R(s) = K/3 \times [(s + \Delta s)^3 - s^3]$$

After applying a protocol fee $\phi = 1\%$, the net ETH required from the user is $C_{mint} / (1 - \phi)$. The fee is retained in the reward pool and does not enter the bonding curve reserve.

2.4 Burn Return

The gross ETH returned when burning Δs tokens from current supply s is:

$$C_{burn}(s, \Delta s) = R(s) - R(s - \Delta s) = K/3 \times [s^3 - (s - \Delta s)^3]$$

The net ETH received after fee deduction is $C_{burn} \times (1 - \phi)$. This guarantees that the burn return is always fully collateralized by the reserve, irrespective of market conditions or external liquidity.

2.5 Price at Maximum Supply

At full supply S_{max} = 1,000,000 TOKEN0, the spot price and total reserve are:

$$P(S_{max}) = 1 \times 10^{-12} \times (10^6)^2 = 1.0 \text{ ETH per token}$$

$$R(S_{max}) = 1 \times 10^{-12} \times (10^6)^3 / 3 \approx 333{,}333 \text{ ETH}$$

3 Protocol Mechanics

3.1 Mint Operation

A user initiates a mint by specifying an ETH amount and a recipient address. The contract computes the corresponding Δs via Newton-Raphson iteration on the inverse of the reserve function, since no closed-form inverse exists for the cubic. The protocol fee is deducted from the gross ETH input, and the remaining ETH is added to the bonding curve reserve. TOKEN0 tokens are minted to the recipient address and total supply is incremented accordingly.

3.2 Burn Operation

A user initiates a burn by specifying a TOKEN0 quantity and a recipient ETH address. The contract computes the reserve release using the burn formula, deducts the protocol fee, destroys the specified TOKEN0 balance, decrements total supply, and transfers net ETH to the recipient. Both operations are atomic and revert in their entirety if any condition is not satisfied.

3.3 Slippage and Tolerance

Because token price is supply-dependent, concurrent transactions within the same block may produce price slippage. The protocol applies a default 0.5% slippage tolerance, reverting any transaction whose effective price deviates beyond this threshold from the quoted price at transaction submission time.

3.4 Fee Distribution

Protocol fees accumulate in an on-chain reward pool segregated from the bonding curve reserve. Fee distribution mechanics are encoded in the smart contract and execute without governance intervention. The separation of fee pool and reserve ensures that protocol revenue cannot dilute the burn collateralization guarantee.

4 Economic Properties

4.1 Fair Launch Guarantee

TOKEN0's fair launch properties derive directly from the mathematical structure of the bonding curve. No tokens are pre-minted. The genesis supply is zero, and the genesis price approaches zero as $s \to 0$. There is no team allocation, no investor round, and no privileged minting address. Every participant from the first buyer to the one-millionth interacts with the identical price function under identical contract conditions.

4.2 Guaranteed Price Floor

The reserve function R(s) provides a mathematically guaranteed price floor at every supply level. For any supply s, a holder can burn their position and receive $C_{burn}(s, \Delta s)$ ETH unconditionally. This floor is not subject to market liquidity conditions, counterparty availability, or oracle pricing — it is a direct consequence of the reserve invariant enforced by the contract.

4.3 Incentive Alignment

The quadratic price function creates natural incentive alignment between early and late participants. Early buyers acquire tokens at lower prices but face lower absolute returns per unit supply growth. Late buyers pay higher prices but benefit from the steeper portion of the price curve. Neither cohort possesses structural advantages unavailable to the other beyond timing, which is publicly observable.

4.4 Deflationary Pressure

Each burn operation permanently destroys TOKEN0 and reduces circulating supply, moving the spot price to a lower point on the curve for subsequent transactions. Asymmetric fee application — where fees are collected on both mint and burn operations but do not re-enter the curve — creates a small but persistent deflationary pressure relative to a zero-fee curve, as the fee-adjusted burn return is marginally below the theoretical curve value.

5 Security Considerations

5.1 No Administrative Privileges

The TOKEN0 contract contains no administrative functions, upgrade proxies, or owner keys. Once deployed, the curve constant K, maximum supply, and fee rate are permanently fixed. No party can pause the contract, modify parameters, or extract reserves outside of the burn mechanism available to all token holders.

5.2 Reserve Invariant

The contract enforces the reserve invariant at every state transition: the ETH balance of the curve contract must equal R(s) within floating-point tolerance at all times. Any transaction that would violate this invariant is reverted. This prevents reserve undercollateralization regardless of external market conditions.

5.3 Front-Running Considerations

Quadratic bonding curves are theoretically susceptible to sandwich attacks, where an adversary front-runs a large mint by minting ahead of it and immediately burning after. TOKEN0 mitigates this through the slippage tolerance mechanism, which bounds the maximum price impact any single transaction may accept. Additionally, the protocol fee applied to both legs of a sandwich attack makes the strategy unprofitable for fee amounts exceeding the price impact captured.

5.4 Oracle Independence

TOKEN0 requires no external price oracles. All pricing is derived entirely from the on-chain supply state. This eliminates oracle manipulation vectors present in externally-priced systems and removes any dependency on third-party data providers.

6 Conclusion

We have presented TOKEN0, a fair-launch bonding curve protocol that provides mathematically guaranteed pricing, symmetric participant access, and unconditional burn liquidity without relying on external market makers, oracles, or governance. The quadratic price function $P(s) = K \times s^2$ determines all economic parameters from a single immutable constant, eliminating discretionary decision-making from the protocol's operation.

The protocol's properties — zero pre-mine, zero team allocation, guaranteed reserve collateralization, and deterministic pricing — address the core structural failures of traditional token launches. TOKEN0 demonstrates that a fully fair token issuance mechanism can be implemented with minimal contract complexity through careful selection of the bonding curve primitive.

Future work may explore adaptive fee structures that respond to supply utilization, multi-asset reserve compositions, and integration with on-chain governance for protocol fee redistribution. The base curve mechanism, however, is intentionally immutable and requires no further modification to fulfill its core function.

Contract Address (Ethereum Mainnet)	0x7b171987Fc3d994ccd9fA8B73d0F3B03C2F1BB7d
Website	tokenzer0.xyz
Max Supply	1,000,000 TOKEN0
Curve Constant (K)	1 x 10^-12
Protocol Fee	1%

Table 1: TOKEN0 Protocol Parameters

The curve is the protocol. The protocol is the law.