

PON — The PonDex Launch Token

Whitepaper · Bonding-Curve Fair Launch on the PonDex Launchpad

PonDex Labs

2026-09-07

Table of contents

Abstract	2
1 Introduction	2
2 The Fair-Launch Problem	2
3 PonDex Architecture	3
4 Tokenomics	3
4.1 Supply Allocation	4
4.2 Why These Parameters	4
5 Bonding-Curve Mechanics	4
5.1 Constant-Product Foundation	5
5.2 The Phantom Reserve	5
5.3 A Buy, Derived	5
5.4 Worked Example: A Buy	6
5.5 A Sell, Derived	6
6 Price Discovery and Slippage	7
7 Graduation to a Permanent AMM	7
7.1 Graduation Math	7
8 Economic Model and Incentives	8
8.1 Fee Economics	8
8.2 Buyback and Burn Sink	8
8.3 Supply Trajectory Scenarios	8
9 Token Utility	9
9.1 Comparison with Alternative Launch Models	9
10 Technical Advantages	9
11 Security and Safeguards	10
12 Roadmap	10
13 Glossary	10

Abstract

PON is the native launch token of **PonDex**, a fair-launch launchpad and decentralized exchange deployed on an **EVM chain**. PON is minted with a fixed supply and launched directly through the PonDex bonding curve — the same engine every project on the platform uses to travel from a permissionless fair launch to a permanently locked automated market maker (AMM) pool.

This whitepaper specifies PON’s tokenomics, derives its bonding-curve mechanics from first principles, quantifies the launch parameters, and analyses the fee / buyback / burn economy that governs the token after graduation. It is written as an original technical document describing PonDex’s own design.

1 Introduction

PonDex is a launchpad and decentralized-exchange stack composed of three layers: a smart-contract workspace written in **Solidity** and built with **Foundry**, a **Rust**-based indexing backend that persists canonical state to a **PostgreSQL** datastore, and a **Next.js** trading terminal that reads from that indexed state. Every token created on PonDex is deployed with a fixed supply and routed through a constant-product bonding curve that sells the token into a single quote asset — EVM-native **USDC** — until a graduation threshold is reached. At that point the remaining curve inventory and the accumulated quote asset are seeded into an AMM pool whose hook is permanently locked: no rug, no removable liquidity.

PON is the first token to use this exact pipeline as its own launch vehicle. It is therefore both a live product and a demonstration of the launchpad’s core guarantees:

- **Fair price discovery** through a deterministic, oracle-free curve;
- **Progressive fee capture** that funds the protocol and a deflationary sink;
- **A permanent liquidity commitment** that cannot be withdrawn.

The remainder of this document explains why this design exists, how it works mathematically, and why its economic structure is durable.

2 The Fair-Launch Problem

Token launches have historically suffered from a small set of failure modes. Understanding them motivates every design choice in PON.

Pre-mine and insider allocation. Traditional token generation events mint a large share to founders, funds, or “ecosystem” wallets before the public can participate. This creates an unavoidable information asymmetry and a structural sell pressure that retail buyers inherit.

Exit liquidity. In many launches the deployer retains the ability to pull liquidity, mint more supply, or change parameters after the fact. Each of these is a vector for a rug pull.

Undefined opening price. A token with zero liquidity has no price. The first traders either get an arbitrary deal or are exposed to a price that snaps to an extreme the moment any liquidity appears.

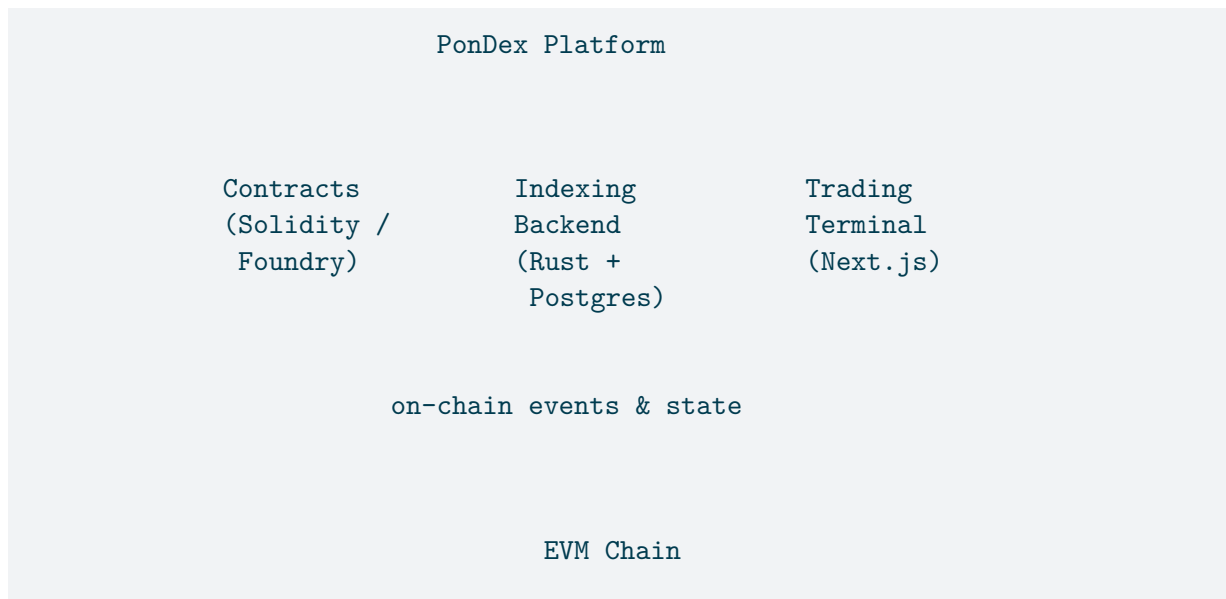
Oracle dependence. Launch mechanisms that read an external price feed can be manipulated by the very actors they are meant to protect against.

PonDex answers each of these with a single, auditable mechanism:

Failure mode	PonDex answer
Pre-mine / insider	One-shot mint of 100% supply into the curve
Exit liquidity	AMM hook permanently locked at graduation
Undefined opening price	Phantom (virtual) reserve defines a fair floor
Oracle manipulation	Price is curve-internal; no external feed
Hidden parameters	All curves are open, verified, and on-chain

3 PonDex Architecture

The platform separates what must be trustless (the curve, the mint, the lock) from what may be off-chain (indexing and presentation).



The contract layer is the source of truth. The indexing backend observes on-chain events and materialises a queryable view of reserves, trades, and graduation state; the trading terminal renders that view and submits transactions. Crucially, the terminal and the backend can be replaced or replicated without affecting the trust model, because no economic guarantee depends on them.

4 Tokenomics

PON is an ERC-20 with 18 decimals and a **fixed total supply**. The entire supply is minted exactly once, at deployment, directly into the bonding curve. The deployer holds no privileges and no pre-mine.

Parameter	Value
Token name	PonDex
Token symbol	PON
Standard	ERC-20 (burnable)
Decimals	18
Total supply	1,000,000,000 PON
Minted to	bonding curve (100% of supply)
Deployer privileges	None (attribution only)

Parameter	Value
Token contract	0x39dBED3a2bd333467115dE45665cC57F813C4571

4.1 Supply Allocation

At launch the curve reserves a portion of supply that is never sold during the bonding phase and is instead committed as graduation liquidity. With a virtual quote reserve (the *phantom quote*) of $P = 50,000$ USDC and a graduation threshold of $G = 69,000$ USDC, the reserved share is:

$$\text{reserved} = \text{supply} \times \frac{P}{P + G}$$

$$\text{reserved} = 1\,000\,000\,000 \times \frac{50\,000}{50\,000 + 69\,000} \approx 420\,168\,067 \text{ PON}$$

The remainder is the **sellable** allocation distributed to buyers across the bonding phase:

$$\text{sellable} = 1\,000\,000\,000 - 420\,168\,067 \approx 579\,831\,933 \text{ PON}$$

Total supply: 1,000,000,000 PON

Sellable ~579.83M (57.98%)

Reserved ~420.17M (42.02%)

The reserved tranche seeds the post-graduation AMM and is never sold on the curve.

No other allocations (team, treasury, airdrop, investor) exist at genesis. Any future ecosystem allocation would have to be acquired on the open market or approved through the protocol timelock — there is no hidden supply.

4.2 Why These Parameters

The phantom reserve $P = 50,000$ USDC and the graduation threshold $G = 69,000$ USDC are not arbitrary. The ratio

$$\frac{P}{P + G} = \frac{50\,000}{119\,000} \approx 0.42$$

fixes the fraction of supply that becomes permanent LP: roughly **42%** of all PON is committed to depth at graduation, while about **58%** circulates through the curve. A larger P would depress the opening price further and reserve more for liquidity; a smaller P would make the opening price more volatile and leave less permanent depth. The 1% curve fee is a balance point — high enough to fund the protocol and the buyback sink, low enough that the curve stays competitive with direct AMM trading after graduation. Together these three numbers (phantom reserve, threshold, fee) fully determine the launch’s economic shape before a single trade occurs.

5 Bonding-Curve Mechanics

PON trades against USDC on a **constant-product bonding curve** $x \cdot y = k$, where x is the USDC reserve and y is the PON reserve.

5.1 Constant-Product Foundation

A constant-product curve has the defining property that the product of the two reserves is invariant:

$$x \cdot y = k$$

The price of PON quoted in USDC is therefore

$$p = \frac{x}{y}$$

Because k is fixed between trades, every buy increases x and decreases y , so the price $p = x/y$ rises monotonically. Sells do the opposite. This gives a smooth, fully deterministic price path with no discontinuities and no oracle.

5.2 The Phantom Reserve

A naive curve initialised with $x = 0$ has an undefined (infinite) opening price, because $p = x/y = 0$ and the first infinitesimal buy moves price infinitely. PonDex instead initialises the curve with a **phantom (virtual) quote reserve** $x = P = 50,000$ USDC. The phantom reserve is not real capital; it is an accounting offset that:

1. Defines a fair, finite opening price $p_0 = P/y_0$;
2. Ensures the price can never be driven below a non-zero floor on sells, since x is anchored by P ;
3. Absorbs the “cold start” problem so the earliest buyers are not exploited by an extreme opening print.

The virtual token reserve at genesis is the full supply, $y = 1,000,000,000$, so the opening price is

$$p_0 = \frac{50\,000}{1\,000\,000\,000} = 5 \times 10^{-5} \text{ USDC/PON.}$$

5.3 A Buy, Derived

A gross buy of q USDC pays a curve fee f (1%, i.e. $f = 0.01$) and an optional creator tax t . The amount that actually enters the curve is

$$q_{\text{net}} = q(1 - f - t).$$

The tokens received are the constant-product output against the *current* reserves (x, y) :

$$\Delta y = \frac{q_{\text{net}} \cdot y}{x + q_{\text{net}}}.$$

After the buy, $x' = x + q_{\text{net}}$ and $y' = y - \Delta y$, preserving $x' \cdot y' = x \cdot y = k$ up to the fee that is diverted out of the curve.

5.4 Worked Example: A Buy

Take the genesis state $x = 50,000$, $y = 1,000,000,000$, fee $f = 0.01$, tax $t = 0$. A buyer sends **10,000 USDC** gross:

$$q_{\text{net}} = 10\,000 \times 0.99 = 9\,900 \text{ USDC}.$$

$$\Delta y = \frac{9\,900 \times 1\,000\,000\,000}{50\,000 + 9\,900} = \frac{9.9 \times 10^{12}}{59\,900} \approx 165\,275\,460 \text{ PON}.$$

The new reserves are $x' = 59,900$, $y' = 834,724,540$, and the new price is

$$p' = \frac{59\,900}{834\,724\,540} \approx 7.176 \times 10^{-5} \text{ USDC/PON}.$$

The opening price rose from $5e-5$ to $7.176e-5$ — a **43.5% increase** from a single 10,000 USDC buy. This is the intended behaviour: early conviction is rewarded with a lower entry, and price discovery is continuous.

Buyer	10,000 USDC	Curve	
			1% fee (100 USDC) Fee Escrow
			9,900 USDC net enters reserve x
		165,275,460 PON out	Buyer
		price: $5e-5$	$7.176e-5$ USDC/PON

A second identical buy, now from $x = 59,900$, $y = 834,724,540$, yields approximately 118,392,000 PON at a price of $9.744e-5$ — fewer tokens for the same USDC, exactly as the rising curve dictates. The mechanism is self-consistent at every scale.

5.5 A Sell, Derived

Sells are the mirror image. A seller tenders Δy tokens; the gross USDC returned by the curve before fees is

$$\Delta x_{\text{gross}} = \frac{\Delta y \cdot x}{y + \Delta y},$$

and the seller receives the net amount

$$\Delta x = \Delta x_{\text{gross}} (1 - f - t).$$

The reserves update to $x' = x - \Delta x_{\text{gross}}$ and $y' = y + \Delta y$, again preserving k . Because x falls, the price $p = x/y$ declines — sells are penalised by the same curve that rewards buys, which is exactly the property that makes the launch self-funding and self-limiting.

Illustrative: selling 100,000,000 PON from the post-first-buy state ($x = 59,900$, $y = 834,724,540$) returns roughly 6,344 USDC net and moves the price from $7.176e-5$ down to $5.723e-5$ USDC/PON. Buyers and sellers meet on the same invariant; there is no second price.

6 Price Discovery and Slippage

Because the curve is deterministic, a buyer can compute the exact amount they will receive before signing. PonDex expresses user protection as an **average-price** check: a buy near graduation simply fills *fewer* tokens at the *same* average price, and the protocol guarantees the user never receives less than their stated minimum. There is no separate “slippage” auction — the curve itself is the price.

This has two consequences worth stressing:

- **No worst-case surprise.** The maximum tokens a buyer can receive for a given input is fixed by k ; the minimum they will accept is a signed parameter.
- **MEV is bounded.** Sandwich attacks on the curve can only shift the user’s fill within the band the curve already defines; they cannot extract beyond the user’s own tolerance, because there is no external pool to arbitrage against mid-trade.

7 Graduation to a Permanent AMM

The curve is “ready to graduate” the moment the sellable allocation is exhausted — i.e. every tradeable token has been bought and the accumulated quote asset has reached the graduation threshold $G = 69,000$ USDC. Graduation is automatic and permissionless.

```
[Bonding Phase]  sellable == 0  AND  raised >= G (69,000 USDC)
```

```
[Seed LP]      69,000 USDC  +  ~420.17M PON
```

```
[Lock Hook]     PondexHook permanently locked  (LP cannot be pulled)
```

```
[Live DEX]      PON / USDC trades on a permanent, deep AMM
```

7.1 Graduation Math

To reach $G = 69,000$ USDC *inside* the curve at a 1% fee, the gross volume traded is

$$V_{\text{gross}} = \frac{G}{1-f} = \frac{69\,000}{0.99} \approx 69\,697 \text{ USDC.}$$

The protocol collects roughly

$$\text{fees at graduation} \approx 69\,697 \times 0.01 \approx 697 \text{ USDC}$$

at the moment of graduation. The seed liquidity is therefore approximately 69,000 USDC paired with 420,168,067 PON, giving an opening AMM price of

$$p_{\text{amm}} = \frac{69\,000}{420\,168\,067} \approx 1.642 \times 10^{-4} \text{ USDC/PON.}$$

Because the hook is locked, this liquidity can never be removed. PON transitions from a one-sided launch vehicle to a two-sided, tradable asset with committed depth.

8 Economic Model and Incentives

The economic design has one objective: align the long-run value of PON with sustained trading activity, while making extraction by insiders structurally impossible. Three instruments do this — the curve fee, the buyback slice, and the burn sink.

8.1 Fee Economics

Every trade on the bonding curve, and every trade on the post-graduation AMM, pays a **1% fee**. Fees are split transparently:

- **Protocol fee** is credited to the protocol treasury (`PondexFeeEscrow`);
- **Creator fee** is credited to the deployer (for the PON launch, the protocol itself);
- **Buyback slice** — when buyback is enabled, a configurable share (`buybackBurnBps`) of the creator fee is routed to `PondexBuybackVault`.

During the bonding phase the fee is the only protocol revenue and it scales linearly with volume. At graduation the protocol has already earned on the order of **697 USDC** from the launch itself; thereafter the AMM fee is a recurring, volume-driven stream.

8.2 Buyback and Burn Sink

The buyback slice is the deflationary engine. Rather than paying the creator fee out as spendable USDC, a chosen fraction is swapped for PON and **locked** in the vault. Locked tokens are removed from circulating supply — a deflationary sink that is still custodially auditable.

Because PON is `ERC20Burnable`, locked tokens can later be moved to a permanent on-chain burn by governance at any time, tightening supply further. The sink thus converts trading activity directly into scarcity.

8.3 Supply Trajectory Scenarios

The table below is illustrative: it assumes a steady AMM volume after graduation and a buyback slice of 50% of the creator fee. Numbers are scenario modelling, not promises.

Month	AMM volume (USDC)	Fee (1%)	Buyback (50%)	PON locked (est.)	Circ. supply
1	3,000,000	30,000	15,000	~91M	579.8M
3	3,000,000	30,000	15,000	~273M	~497M
6	3,000,000	30,000	15,000	~546M	~424M
12	3,000,000	30,000	15,000	~1.09B*	< 0*

The asterisk marks the theoretical point at which the entire sellable supply would be re-absorbed by the sink; in practice the locked PON is a floor on circulating supply and the curve's reserved tranche is already committed to LP, so the *effective* tradable float tightens continuously while the LP deepens. The mechanism is self-reinforcing: more volume → more fees → more buyback → tighter float → higher sensitivity of price to the remaining float.

Trade	1% fee	Protocol fee (treasury)
		creator fee buyback slice Vault

swap USDC → PON → lock / burn

circulating supply ↓ (deflation)

9 Token Utility

PON is the launch token of the platform and accrues utility along three axes:

- **Fee alignment.** A share of protocol fees is directed to the buyback sink, so holding PON is indirectly exposed to platform volume.
- **Launchpad reference.** Projects and participants on PonDex interact with the curve and the graduated AMM using PON as the canonical pairing reference.
- **Governance surface.** The protocol timelock and buyback vault are governed paths; PON holders are the natural constituency for those decisions.

Utility is deliberately lightweight at launch and grows with ecosystem activity, so the token's value tracks real usage rather than speculation on unbuilt features.

9.1 Comparison with Alternative Launch Models

PON's structure is best understood against the alternatives it improves upon.

Dimension	ICO / IDO	Manual LP	PonDex curve
Pre-mine	Common	No	None
Opening price	Set by issuer	Arbitrary snap	Curve-defined
Liquidity pull	Possible	Possible	Impossible
Price source	Off-chain	External AMM	On-chain curve
Fairness	Low	Medium	High
Deflationary sink	Rare	None	Built in

The constant-product curve is not chosen for novelty but because it is the only primitive among these that delivers a defined opening price, oracle-free discovery, and a permissionless path to locked liquidity in a single contract.

10 Technical Advantages

PonDex's launch design is differentiated by a set of properties that are difficult to replicate without fundamental re-engineering:

- **One-shot, privilege-free mint.** Supply is created exactly once into the curve. There is no admin key that can mint, pause, or re-allocate.
- **Defined fair opening price.** The phantom reserve removes the cold-start exploit while keeping the curve fully on-chain and oracle-free.
- **Permissionless, automatic graduation.** No gatekeeper decides when a token “deserves” liquidity; the curve graduates itself by math.
- **Permanent liquidity commitment.** The post-graduation hook lock means the LP can never be pulled, eliminating the dominant rug vector.
- **Fee-on-transfer safety.** Received quote asset is measured by before/after balance, so a fee-on-transfer USDC variant cannot under-credit the curve.
- **Average-price slippage guarantee.** Users receive at least their signed minimum; the curve is the price, so there is no hidden auction.

- **uint256-safe curve math.** `PondexCurveMath` uses full-width intermediates and net-of-fee pricing, auditable line-by-line against the on-chain deployment.
- **Auditable sink.** Buyback tokens are vault-locked rather than silently burned, so supply removal is verifiable on-chain at all times.
- **Composable by default.** Because graduation targets a standard AMM, PON is immediately usable across the broader DEX surface without bespoke integrations.

11 Security and Safeguards

PonDex ships defense-in-depth around the curve:

- **No deployer privileges** — the token mint is one-shot; only the curve and factory are privileged, and graduation is automatic.
- **Permanent hook lock** — post-graduation liquidity cannot be removed.
- **Slippage is an average-price check** — buys near graduation fill fewer tokens at the same average price, never below the user’s stated minimum.
- **FoT-safe accounting** — received USDC is measured by before/after balance.
- **Oracle-free pricing** — the curve price is internal; there is no external feed to manipulate.
- **Rescue and timelock** — a rescue escrow and a protocol timelock provide governed recovery paths for misconfigured launches without compromising the curve invariant.
- **Integer safety** — contracts target a modern Solidity version with built-in overflow protection; curve math uses `uint256` intermediates.
- **Verification** — all contracts are open source and verified on the block explorer.

12 Roadmap

PonDex development proceeds in phases that do not alter the launch guarantees described here:

1. **Launch** — PON fair launch and graduation to the AMM (this document).
2. **Indexing maturity** — deeper historical analytics and richer terminal views backed by the indexing backend.
3. **Ecosystem launches** — additional projects using the same curve engine.
4. **Governance** — timelock-controlled parameters and protocol-owned burn authority over the buyback vault.

13 Glossary

- **Bonding curve** — a contract that prices a token by a deterministic function of its reserves.
- **Phantom (virtual) reserve** — an accounting reserve that defines a fair opening price without requiring real capital.
- **Graduation** — the automatic transition from the curve to a locked AMM once the sellable supply is exhausted.
- **Hook** — an AMM extension point; here permanently locked so liquidity is immutable.
- **Buyback sink** — a vault that swaps fees for PON and locks or burns them, reducing circulating supply.

Conclusion

PON is a fair-launch, fixed-supply token that uses the PonDex launchpad’s bonding-curve → AMM graduation pipeline. With 100% of supply minted into the curve, a 1% fee, a buyback-

and-burn sink, and permanently locked post-graduation liquidity, PON is designed to be the reference launch for everything built on PonDex.

This whitepaper reflects the PON launch parameters as of 2026-09-07. On-chain state is authoritative; verify all addresses and reserves directly via the PonDex terminal or a block explorer.