PANTHEON

Technical Whitepaper

Distribution engineering Infrastructure

Written by Paul Mak

Version 1.2 | May 2026

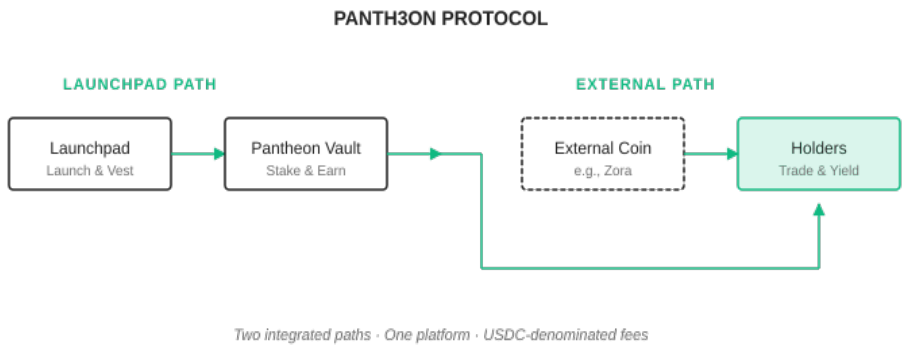
CONFIDENTIAL

SECTION 01

Introduction

Pantheon is a worlds first distribution engineering primitive, built to foster stronger, value rich, resilient token economies. Its infrastructure consists of three integrated applications that together form a complete lifecycle for scalable creator economies, capital routing and deterministic behavioural outcomes.

The third application is to be launched at a later date so this paper will focus on the initial two:
1. A unique Launchpad for token creation, human capital exposure, and price discovery, and the
2. Index vault for capital aggregation, yield generation, value routing and data rich feedback loops.



System Overview · Two integrated paths, one platform

1.1 System Overview

Launchpad App. Handles optional private presales with prorata oversubscription, token deployment with structured allocation, public sale with Merkle-protected anti-sniper window, graduation to Uniswap V4, vesting via Sablier, and investor claims.

Vault Staking App. Enables holders of any compatible Base-native creator coin to stake, earn yield from project-funded reward pools, and trade through atomic on-chain swaps. Supports existing coins like Zora alongside tokens launched through the Pantheon Launchpad.

1.2 Network and Dependencies

Parameter	Value
Chain	Base Mainnet (Chain ID: 8453)
Numeraire	USDC (0x8335…2913)
AMM Protocol	Uniswap V4 (post-graduation and external pools)
Vesting Protocol	Sablier LockupLinear V1.1

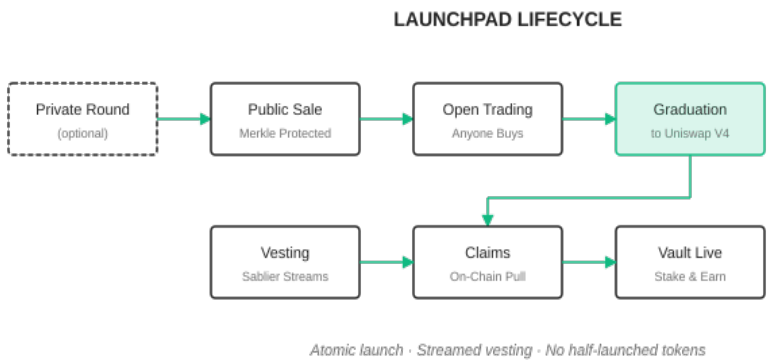
Staking Contracts	StakingVault.sol, TokenLock.sol, ProjectTokenConfig.sol
Token Standard	ERC-20
Smart Contract Audit	Salus Security (Feb 2026) — 12 findings, 11 resolved
External Token Support	Zora Creator Coins (CoinV4 hook architecture)

PART ONE

Launchpad Lifecycle

How tokens move from creation to market.

The Pantheon Launchpad operates a multi-stage lifecycle that takes a creator token from optional private commitment through public sale with anti-sniper protection, graduation to permanent DEX liquidity, and long-term vesting.



Launchpad Lifecycle · Atomic launch with streamed vesting

2.1 Private Presale (Optional)

Creators may run a private presale before public launch. Whitelisted wallets commit USDC on-chain to a receiving address on Base mainnet. Each commitment is validated by a Supabase Edge Function that performs on-chain verification.

Private rounds support oversubscription. When total committed USDC exceeds the raise target, prorata allocation applies — each investor receives tokens proportional to their commitment relative to the total committed. Private investor allocations are streamed via Sablier post-graduation, preventing early dumping on public sale buyers.

2.2 Public Sale with Sniper Protection

The public sale opens with a Merkle-tree-enforced protected window. During this initial phase, only wallets included in a pre-published whitelist may participate. The whitelist can be any size the entire set is compressed into a single Merkle root stored on-chain, and each buyer provides a proof at purchase time that is verified in a single check.

After the protected window expires, the sale opens to anyone. The mechanism is designed for anti-bot protection of the early window, not for ongoing gatekeeping. Bots cannot drain the sale in the first minutes; legitimate participants get a fair entry.

2.3 Token Launch and Allocation

The Creators tokemn deployment is atomic, the token contract, the liquidity pool, and the Sablier vesting streams are created in a single transaction. If any component fails, the entire launch rolls back.

Allocations are distributed across the categories defined in Section 3. Creator and platform allocations are streamed via Sablier with configurable cliff and linear vesting periods; neither party can dump on the public market. We foster clear blue sky trading.

2.4 Graduation to Uniswap V4

Once configured sale parameters are met, the token graduates to a permanent Uniswap V4 pool on Base. From this point forward, anyone can buy or sell the token through the Pantheon app, with all trades routing through the Universal Router.

2.5 Sablier Vesting Streams

After graduation, vesting streams are created in a batch transaction using Sablier V1.1 LockupLinear. Stream IDs are extracted from the receipt and persisted to the database for claims tracking. All vesting data is read directly from Sablier contracts on-chain.

2.6 Claims

Investors access the claims page to view their allocations, cliff countdowns, vesting progress, and claimable amounts. All data is sourced directly from Sablier on-chain. Pantheon holds no custody and cannot block claims.

2.7 Post-Graduation Trading

The token trades on its Uniswap V4 pool. Swaps execute via the Universal Router using a bundled command sequence with built-in slippage protection. Price discovery is continuous through V4's concentrated liquidity. A 1% platform fee is collected in USDC on every swap applied at the input side on buys and the output side on sells and all fees captured by and burn the creator coin for 5y in the Pantheon lock contract.

SECTION 03

Token Configuration

Configurable supply model and allocation parameters.

Tokens launched via the Pantheon Launchpad use a fixed-supply model with structured allocation. Both the total supply and the allocation breakdown are configurable per launch, creators tune these parameters to their specific economic design when initiating their token sale.

The categories below illustrate the typical structure available to creators. Specific percentages and durations are illustrative ranges, not fixed protocol requirements.

3.1 Allocation Categories

Category	Typical Range	Mechanism
Creator Treasury	Fixed 6m + 12m	Sablier stream
Platform Fee	Fixed protocol fee	Sablier stream to platform treasury wallet
Private Investors	Configurable	Prorata Sablier streams per wallet
Marketing / Operations	Configurable	Distributed per launch configuration
LP / Liquidity	Configurable	Seeds permanent Uniswap V4 pool

Total allocations across all categories sum to 100% of fixed supply. Creators design the breakdown that fits their economic model, small treasury / large community distribution, weighted private round, marketing-heavy launches, and other variants are all supported.

3.2 Vesting Parameters

Cliff and linear vesting durations are configurable per allocation category. The pattern is consistent across all parties: tokens vest on-chain via Sablier streams, and no party can bypass the schedule. Common configurations include:

- Multi-month cliffs followed by linear vesting for creator treasuries
- Cliffs aligned to product or market milestones for private investors
- Immediate or short-cliff streaming for platform fees and operational allocations

All vesting is enforced at the smart contract level via Sablier. Once a launch is configured and executed, the streams cannot be retroactively altered.

3.3 Private Round Mechanics

Private rounds support oversubscription. When total committed USDC exceeds the raise target, prorata allocation is applied. Each investor receives tokens proportional to their commitment relative to total committed:

```
allocationRatio = raiseTarget / totalCommitted
```

All private investor allocations are Sablier-streamed with cliff and linear vesting. Investors cannot sell their tokens during the cliff period, and any liquidation before vesting completes is mathematically impossible. This protects public sale buyers from being sold into by private participants.

PART TWO

Staking Mechanics

Single-term vault staking with monthly yield distribution.

4.1 Staking Model

Every vault implements a single mandatory staking term - typically six months with optional auto-restake. Staking uses a reward-per-share accounting model that ensures claim-order independence: the order in which stakers claim does not affect anyone's allocation.

4.2 Delayed Rewards

Rewards are anchored to real calendar months using fixed UTC boundaries. A user who stakes in Month A earns no rewards in Month A. Rewards begin accruing from Month B and become claimable at the end of Month B. This anchors yield to discrete, predictable epochs rather than continuous per-second accrual.

4.3 Early Unstake Penalties

Early unstaking applies a flat 10% penalty on staked principal only. Rewards from completed months are never penalized. The month in which the user unstakes is forfeited. Cool down period is 7 days. An instant emergency exit option is available with a 20% penalty for stakers.

4.4 Reward Pool Funding

Every vault is bootstrapped with reward tokens at launch, drawn from the token's own allocation. Stakers begin earning rewards from day one without requiring any external contribution.

Beyond the initial bootstrap, anyone can contribute additional reward tokens to the pool at any time, the project team, third-party sponsors, partners, or individual community members. The vault distributes everything pro-rata to active stakers over the configured distribution period.

4.5 Fee Schedule

Fee Event	Rate	Where Applied
Reward deposit/claim	5%	Vault contract
Buy / Sell swap	1% in USDC	Universal Router

SECTION 05

Trading Architecture

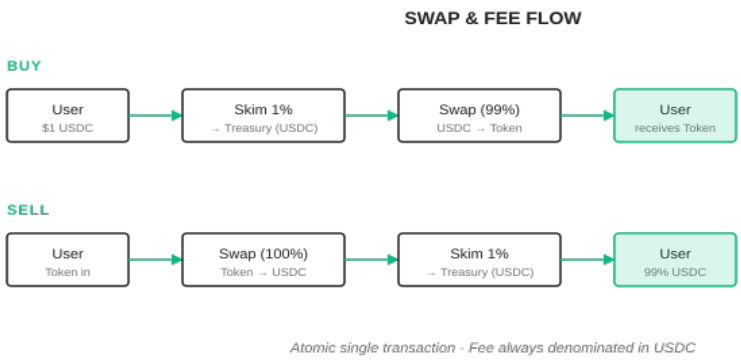
Atomic swaps with USDC-denominated platform fees.

5.1 Swap Execution

All trading executes through the Uniswap Universal Router using bundled command sequences. The protocol supports two distinct swap paths:

- **Single-hop swaps** for tokens launched via the Pantheon Launchpad (paired against USDC in their V4 pool)
- **Two-hop swaps** for external tokens not paired with USDC - routed through an intermediate liquid token (e.g., USDC → ZORA → JESSE)

Both paths execute atomically. The full sequence - token transfer, swap, fee skim, and final delivery - completes in a single transaction. If any step fails, the entire transaction reverts. No partial states are possible.



Swap and Fee Flow · BUY skims input, SELL skims output, treasury always in USDC

5.2 Platform Fee Mechanism

A 1% platform fee is collected on every swap, always denominated in USDC for treasury currency consistency. The mechanism varies by direction:

- **Buy:** the platform fee is skimmed from the user's USDC input before the swap executes. The user's remaining 99% routes through the swap path to produce the target token.
- **Sell:** the swap executes first, producing USDC output. The 1% fee is then skimmed before the user receives their proceeds.

This pattern ensures the treasury accumulates only USDC regardless of which token the user is buying or selling. No token-price exposure on accumulated fees, no manual conversion required.

5.3 Slippage Protection

Every swap includes slippage protection at the protocol level. Users select their tolerance (typically 0.5%, 1%, or 3%) and the contract enforces a minimum output. If the actual output would fall below the minimum, the transaction reverts entirely protecting users from price manipulation and adverse market movements.

SECTION 06

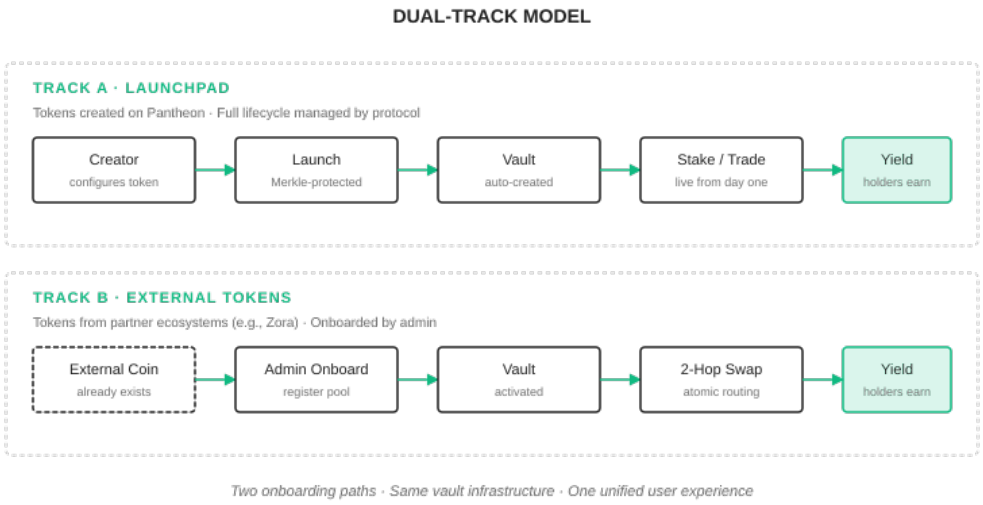
External Creator Coins

Open architecture for tokens beyond the Pantheon Launchpad.

6.1 Architectural Position

In our goal to improve the larger crypto ecosystem, the platform supports external coins ie tokens minted on partner ecosystems with compatible Uniswap V4 pool architectures. The first supported integrations are Bankr and Zora's CoinV4 creator coin system along with any evm compatible asset. Solana will be available mid June 2026.

Creators who issue coins on Zora can have a Pantheon vault created for their token. Their community can stake, earn rewards, and trade through the Pantheon app without Pantheon needing to have launched the token itself.



Dual-Track Model · Two onboarding paths, one unified user experience

6.2 Two-Hop Swap Routing

External tokens are typically not paired directly against USDC. Zora creator coins, for example, pair against the ZORA token in their V4 pools. The platform handles this via two-hop swap routing through Uniswap V4 and V3:

- **Buy direction:** USDC → ZORA (Uniswap V3) → target token (Uniswap V4)
- **Sell direction:** target token → ZORA (Uniswap V4) → USDC (Uniswap V3)

Both paths execute atomically in a single Universal Router transaction. From the user's perspective, the experience is identical to a direct swap USDC in, target token out (or vice versa), with a single confirmation.

6.3 Onboarding External Pools

External pools registration captures the pool key (currency0, currency1, fee tier, tick spacing, hook address) and the intermediate routing token. Once registered, the vault becomes immediately available for staking, trading, and reward distribution.

6.4 Hook-Aware Reward Distribution

Some external pool architectures implement custom hooks that perform reward distribution inside every swap sending portions of the swap output to creators, platform recipients, and other slots. The Pantheon swap path is designed to coexist with these hooks, layering its 1% USDC fee on top without interfering with the host ecosystem's reward mechanics.

Creators retain their full host-ecosystem rewards while their community gains access to Panth3on's staking infrastructure and yield generation.

SECTION 07

Smart Contract Architecture

Audited vault contracts and protocol dependencies.

7.1 Vault Smart Contracts (Audited)

The vault staking system is implemented in Solidity and has been audited by Salus Security (February 2026). The audit covered five contract files across three review rounds.

Contract	Purpose
StakingVault.sol	Core staking logic: stake / unstake / claim / reward-per-share
TokenLock.sol	Token vesting and locking with cliff enforcement and linear release
ProjectTokenConfig.sol	Fee configuration (fee % / fee recipient) per project token
ProjectTokenFactory.sol	Factory for deploying new project token instances
ProjectToken.sol	ERC-20 token implementation for project tokens

7.2 Audit Summary

Salus Security identified 12 issues. 10 resolved, 2 acknowledged as intentional design decisions.

Issue	Severity	Status
Logical errors in accruedReward()	High	Resolved
Extra reward at boundary month	High	Resolved
Cliff duration month-boundary compression	Medium	Acknowledged
Rescue permanently disabled after lock	Medium	Resolved
Rewards lost after unstaking	Medium	Resolved
Monthly step accrual (integer division)	Medium	Resolved
Centralization risk (single owner)	Medium	Acknowledged
Pre-cliff reward claiming	Low	Resolved
AutoRestake flag not enforced	Low	Resolved

Centralization risk (single owner with withdrawRewardPool access) is acknowledged. Migration to multi-sig with timelock governance has been resolved prior to production deployment.

8 Smart Contract Layer

All financial logic is implemented in Solidity and deployed on Base. The contracts have been audited by Salus Security (Feb 2026). Base provides Ethereum-level security with consumer-friendly transaction fees — a typical swap costs cents in gas rather than dollars.

9 Authentication

Wallet-based authentication is handled via Privy, the standard authentication layer for crypto-native applications. This supports both connected wallet flows (MetaMask, Coinbase Wallet, Rainbow, Rabby) and email/social login with embedded wallets for users new to crypto.

10. Future Development

Planned next 30 day protocol extensions and governance upgrades.

- Additional external coin source integrations from Solana and other chains.
- Cross-chain reward contributions.
- Dynamic raise structures
- Trade-referrer revenue capture on external pools where supported
- Cross platform integration for socials (Tiktok, Instagram, Youtube)

End of Document