OFFSIDE LABS

Dynamic Bonding Curve

0.1.7

Smart Contract Security Assessment

October 2025

Prepared for:

Meteora

Prepared by:

Offside Labs

Ronny Xing

Contents

1 About Offside Labs

Offside Labs is a leading security research team, composed of top talented hackers from both academia and industry.

We possess a wide range of expertise in modern software systems, including, but not limited to, *browsers*, *operating systems*, *IoT devices*, and *hypervisors*. We are also at the forefront of innovative areas like *cryptocurrencies* and *blockchain technologies*. Among our notable accomplishments are remote jailbreaks of devices such as the **iPhone** and **PlayStation 4**, and addressing critical vulnerabilities in the **Tron Network**.

Our team actively engages with and contributes to the security community. Having won and also co-organized *DEFCON CTF*, the most famous CTF competition in the Web2 era, we also triumphed in the **Paradigm CTF 2023** within the Web3 space. In addition, our efforts in responsibly disclosing numerous vulnerabilities to leading tech companies, such as *Apple*, *Google*, and *Microsoft*, have protected digital assets valued at over **$300 million**.

In the transition towards Web3, Offside Labs has achieved remarkable success. We have earned over **$9 million** in bug bounties, and **three** of our innovative techniques were recognized among the **top 10 blockchain hacking techniques of 2022** by the Web3 security community.

 **https://offside.io/**

 **https://github.com/offsidelabs**

 **https://twitter.com/offside_labs**

2 Executive Summary

Introduction

Offside Labs completed a security audit of *Dynamic Bonding Curve* smart contracts, starting on October 20th, 2025, and concluding on October 23th, 2025.

Project Overview

The Dynamic Bonding Curve (DBC) is a permissionless launch pool protocol that enables users to create and launch tokens with customizable bonding curves directly. The program allows partners to configure key parameters such as quote tokens, token graduation curves, and fees.

In the current release, a new creation fee has been added, the protocol now supports the two new swap modes ExactOut and PartialFill, and an innovative base fee mode Rate Limiter has been implemented with related trading restrictions. Creators and partners have greater flexibility to mint the base token, the configuration supports more parameters with adjustments to certain fee constraints, withdrawal of the migration fee is supported, and rent collection for migration and for creating lock escrows has been made more flexible.

Audit Scope

The assessment scope contains mainly the smart contracts of the dynamic-bonding-curve program for the *Dynamic Bonding Curve* project.

The audit is based on the following specific branches and commit hashes of the codebase repositories:

- Dynamic Bonding Curve
  - Codebase: `https://github.com/MeteoraAg/dynamic-bonding-curve`
  - PR-129
    - Commit Hash: 7b44a8d0b39d00640167f72748c1ba992e9dd7ca
    - Codebase Link: `PR-129`

We listed the files we have audited below:

- Dynamic Bonding Curve
  - programs/dynamic-bonding-curve/src/base_fee/*.rs
  - programs/dynamic-bonding-curve/src/constants.rs
  - programs/dynamic-bonding-curve/src/error.rs
  - programs/dynamic-bonding-curve/src/event.rs
  - programs/dynamic-bonding-curve/src/instructions/admin/ix_claim_pool_creation_fee.rs
  - programs/dynamic-bonding-curve/src/instructions/admin/ix_withdraw_lamports_from_authority.rs
  - programs/dynamic-bonding-curve/src/instructions/admin/mod.rs

- programs/dynamic-bonding-curve/src/instructions/initialize_pool/ix_initialize_virtual_pool_with_spl_token.rs
- programs/dynamic-bonding-curve/src/instructions/initialize_pool/ix_initialize_virtual_pool_with_token2022.rs
- programs/dynamic-bonding-curve/src/instructions/migration/create_locker.rs
- programs/dynamic-bonding-curve/src/instructions/migration/dynamic_amm_-v2/damm_v2_metadata_state.rs
- programs/dynamic-bonding-curve/src/instructions/migration/dynamic_amm_-v2/migrate_damm_v2_initialize_pool.rs
- programs/dynamic-bonding-curve/src/instructions/migration/dynamic_amm_-v2/migration_damm_v2_create_metadata.rs
- programs/dynamic-bonding-curve/src/instructions/migration/flash_rent.rs
- programs/dynamic-bonding-curve/src/instructions/migration/meteora_damm/meteora_damm_lock_lp_token.rs
- programs/dynamic-bonding-curve/src/instructions/migration/meteora_damm/migrate_meteora_damm_initialize_pool.rs
- programs/dynamic-bonding-curve/src/instructions/migration/mod.rs
- programs/dynamic-bonding-curve/src/instructions/partner/ix_create_config.rs
- programs/dynamic-bonding-curve/src/instructions/swap/ix_swap.rs
- programs/dynamic-bonding-curve/src/instructions/swap/swap_exact_in.rs
- programs/dynamic-bonding-curve/src/lib.rs
- programs/dynamic-bonding-curve/src/state/config.rs
- programs/dynamic-bonding-curve/src/state/fee.rs
- programs/dynamic-bonding-curve/src/state/virtual_pool.rs
- programs/dynamic-bonding-curve/src/utils/cpi_checker.rs
- programs/dynamic-bonding-curve/src/utils/mod.rs
- programs/dynamic-bonding-curve/src/utils/token.rs

Findings

The security audit revealed:

- 0 critical issue
- 0 high issue
- 0 medium issue
- 0 low issue
- 2 informational issues

Further details, including the nature of these issues and recommendations for their remediation, are detailed in the subsequent sections of this report.

3 Summary of Findings

ID	Title	Severity	Status
01	Suggest to Add Data Check in CPI Wrapper	Informational	Fixed
02	Excessively Strict Lamports Check	Informational	Fixed

4 Key Findings and Recommendations

4.1 Informational and Undetermined Issues

Suggest to Add Data Check in CPI Wrapper

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Logic Error

The CPI Wrapper ensures that critical PDAs cannot be maliciously altered during CPI operations. It is recommended to implement data length verification(before data length == after data length), in addition to owner checks.

For instance, the System Program can initialize the signer account as a Nonce Account. Although the Nonce Account's owner remains the system program, the signer cannot invoke other instructions of the system program. This could potentially compromise the functionality of critical PDAs.

Fixed in PR-145

Excessively Strict Lamports Check

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Logic Error

The lamports check `before_lamports == after_lamports` in the CPI Wrapper may be excessively strict. Ensuring `after_lamports >= before_lamports` after CPI execution would not have adverse effects.

Fixed in PR-145

5 Disclaimer

This audit report is provided for informational purposes only and is not intended to be used as investment advice. While we strive to thoroughly review and analyze the smart contracts in question, we must clarify that our services do not encompass an exhaustive security examination. Our audit aims to identify potential security vulnerabilities to the best of our ability, but it does not serve as a guarantee that the smart contracts are completely free from security risks.

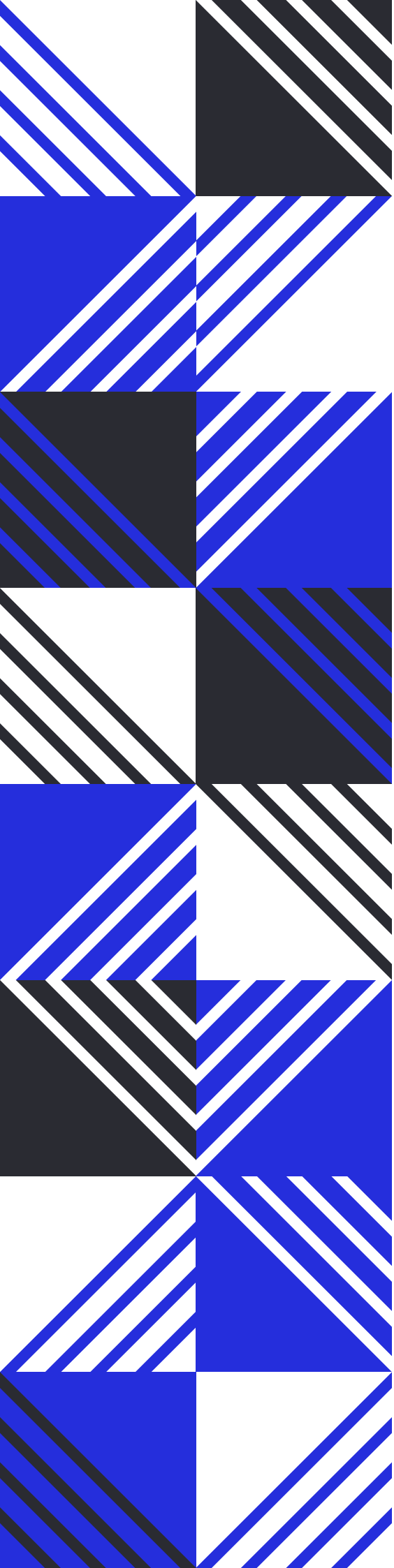
We expressly disclaim any liability for any losses or damages arising from the use of this report or from any security breaches that may occur in the future. We also recommend that our clients engage in multiple independent audits and establish a public bug bounty program as additional measures to bolster the security of their smart contracts.

It is important to note that the scope of our audit is limited to the areas outlined within our engagement and does not include every possible risk or vulnerability. Continuous security practices, including regular audits and monitoring, are essential for maintaining the security of smart contracts over time.

Please note: we are not liable for any security issues stemming from developer errors or misconfigurations at the time of contract deployment; we do not assume responsibility for any centralized governance risks within the project; we are not accountable for any impact on the project's security or availability due to significant damage to the underlying blockchain infrastructure.

By using this report, the client acknowledges the inherent limitations of the audit process and agrees that our firm shall not be held liable for any incidents that may occur subsequent to our engagement.

This report is considered null and void if the report (or any portion thereof) is altered in any manner.



OFFSIDE LABS

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs