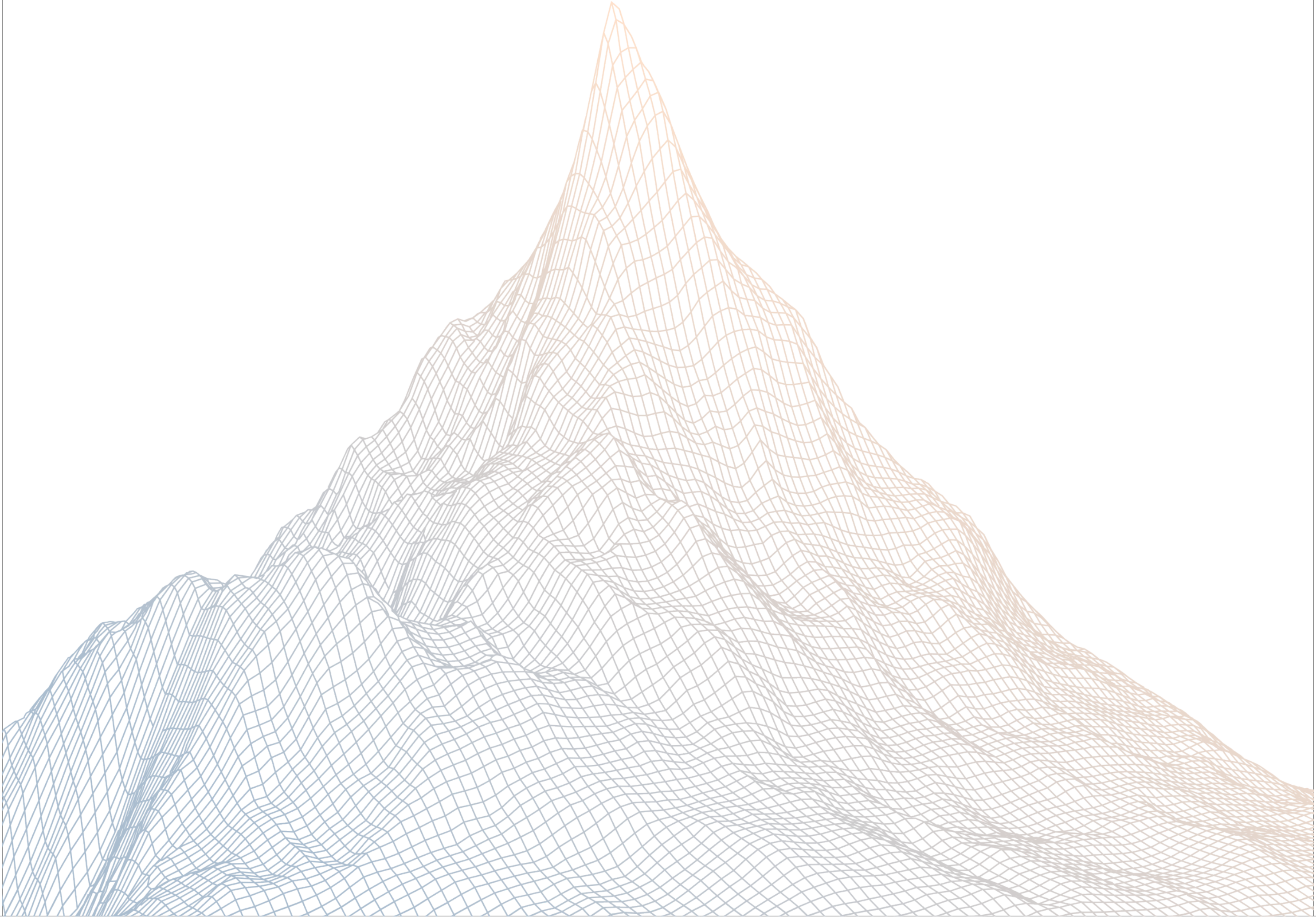
Zenith

Berachain

Smart Contract Security Assessment

VERSION 1.1



AUDIT DATES: October 3rd to October 4th, 2025

AUDITED BY: Matte
ether_sky

Contents

1 Introduction

1.1 About Zenith

Zenith assembles auditors with proven track records: finding critical vulnerabilities in public audit competitions.

Our audits are carried out by a curated team of the industry's top-performing security researchers, selected for your specific codebase, security needs, and budget.

Learn more about us at https://zenith.security.

1.2 Disclaimer

This report reflects an analysis conducted within a defined scope and time frame, based on provided materials and documentation. It does not encompass all possible vulnerabilities and should not be considered exhaustive.

The review and accompanying report are presented on an "as-is" and "as-available" basis, without any express or implied warranties.

Furthermore, this report neither endorses any specific project or team nor assures the complete security of the project.

1.3 Risk Classification

SEVERITY LEVEL	IMPACT: HIGH	IMPACT: MEDIUM	IMPACT: LOW
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

2

Executive Summary

2.1 About Berachain

Berachain is a high-performance EVM-Identical Layer 1 blockchain utilizing Proof-of-Liquidity (PoL) and built on top of the modular EVM-focused consensus client framework BeaconKit.

2.2 Scope

The engagement involved a review of the following targets:

Target	contracts-meta-aggregator
Repository	https://github.com/berachain/contracts-meta-aggregator
Commit Hash	`0e46a1f3f14a7637cfb37622c85e671fa76e7513`
Files	`Changes in PR-10`

2.3 Audit Timeline

October 3, 2025	Audit start
October 4, 2025	Audit end
October 6, 2025	Report published

2.4 Issues Found

SEVERITY	COUNT
Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Informational	1
Total Issues	**1**

3

Findings Summary

ID	Description	Status
I-1	A type mismatch exists in IRewardVault	Resolved

4

Findings

4.1 Informational

A total of 1 informational findings were identified.

[I-1] A type mismatch exists in IRewardVault

SEVERITY: Informational	IMPACT: Informational
STATUS: Resolved	LIKELIHOOD: Low

Target

- IRewardVault.sol

Description:

In BeraChain, the `stakingToken` in the reward vault is of type `IERC20`, so the public getter returns `IERC20`.

```
IERC20 public stakeToken;
```

However, in `IRewardVault`, the getter is defined to return `address`.

- IRewardVault.sol#L6

```
function stakeToken() external view returns (address);
```

While this does not cause an error, it's recommended to match the return types for consistency.

Recommendations:

```
function stakeToken() external view returns (address);
function stakeToken() external view returns (IERC20);


function _stake
    (uint256 amount, address rewardVault,
    SwapOutputData calldata outputData) internal {
    // Check is token out is stake token for the reward vault.
    if (IRewardVault(rewardVault).stakeToken() ≠
        outputData.tokenOut) revert TokenOutIsNotStakeToken();
    if (address(IRewardVault(rewardVault).stakeToken()) ≠
        outputData.tokenOut) revert TokenOutIsNotStakeToken();
}
```

BeraChain: Resolved with @2196d927228...

Zenith: Verified.