Defense By Thesis

Security Audit Report

Mezo

MezoBridge Smart Contract

Initial Report // August 28, 2025
Final Report // September 10, 2025

Team Members

Ahmad Jawid Jamiulahmadi // Senior Security Auditor
Mukesh Jaiswal // Senior Security Auditor

Table of Contents

About Thesis Defense

Defense is the security auditing arm of Thesis, Inc., the venture studio behind tBTC, Fold, Mezo, Acre, Taho, Etcher, and Embody. At Defense, we fight for the integrity and empowerment of the individual by strengthening the security of emerging technologies to promote a decentralized future and user freedom. Defense is the leading Bitcoin applied cryptography and security auditing firm. Our team of security auditors have carried out hundreds of security audits for decentralized systems across a number of ecosystems including Bitcoin, Ethereum + EVMs, Stacks, Cosmos SDK, NEAR and more. We offer our services within a variety of technologies including smart contracts, bridges, cryptography, node implementations, wallets and browser extensions, and dApps.

Defense will employ the Defense Audit Approach and Audit Process to the in scope service. In the event that certain processes and methodologies are not applicable to the in scope services, we will indicate as such in individual audit or design review SOWs. In addition, Thesis Defense provides clear guidance on successful Security Audit Preparation.

Section 1.0
Scope

Technical Scope

- **Repository:** https://github.com/thesis/mezo-portal
- **Audit Commit:** `efe1b481741066c23dfb8fb4738c3faf50b18329`
- **Verification Commit:** `e9d5b6d3d1a8dd83a2ab986cc04bcd120d593838`
- **File in Scope:** MezoBridge.sol

Section 2.0
Executive Summary

Schedule

This security audit was conducted from August 25, 2025 to August 28, 2025 by 2 senior security auditors for a total of 8 person days.

Overview

The `MezoBridge` smart contract serves as the central component responsible for securely holding all funds bridged into the Mezo blockchain and ensuring their correct release during bridge-out operations. The smart contract implements bridge-out functionality to enable users to move funds from Mezo to Ethereum and Bitcoin, supporting both individual and batch attestation processes that allow validators to confirm and authorize withdrawals. It also facilitates native BTC withdrawals as part of its core bridging capability, while managing the lifecycle of bridge validators to ensure proper registration and governance over validator participation. Additionally, the contract provides mechanisms for setting and adjusting withdrawal fees, as well as overseeing reimbursement processes tied to attestations.

Tests

A comprehensive test suite is implemented.

Project Documentation

We found comprehensive external and inline documentation.

Section 3.0
Key Findings Table

Issues	Severity	Status
ISSUE #1 Premature Attestations Possible with Incomplete Validator Set	Low	Acknowledged
ISSUE #2 Improper Validator ID Management Enables Double Attestation	Low	Partially Fixed
ISSUE #3 Gas Optimization via Unchecked Increment in `_countSetBits`	None	Acknowledged

Severity definitions can be found in Appendix A

Section 4.0
Findings

We describe the security issues identified during the security audit, along with their potential impact. We also note areas for improvement and optimizations in accordance with best practices. This includes recommendations to mitigate or remediate the issues we identify, in addition to their status before and after the fix verification.

ISSUE#1

Premature Attestations Possible with Incomplete Validator Set

Low

Acknowledged

Location

contracts/MezoBridge.sol#L290-L340

Description

The `attestBridgeOut` function allows attestations to proceed with the currently registered set of `bridgeValidators`. However, there is no mechanism ensuring that a minimum validator threshold has been established before attestations begin. As a result, if governance has only added one validator so far, this single validator can complete the attestation process alone—despite governance intending to later require, for example, 5 out of 6 validators. This creates a mismatch between governance's intended quorum policy and the protocol's actual enforcement at the time of attestation.

Impact

- A single validator could complete attestations during the setup phase, effectively bypassing multi-sig security guarantees.
- This creates a window of vulnerability where attestations may succeed with insufficient validator participation.
- It undermines governance's intended validator threshold until the full set of validators is added, potentially exposing the bridge to premature attestations.

Recommendation

We recommend introducing a governance-controlled state variable (e.g., `minValidatorsRequired`) that specifies the minimum number of validators expected for valid attestations. The contract should block attestation attempts until this threshold is met, ensuring that attestations cannot proceed prematurely with only a partial validator set.

Verification Status

The Mezo team stated that multiple validators will be added at once, in a single SAFE transaction immediately after the smart contract upgrade. The governance is also in-charge of maintaining a proper number of validators depending on the network conditions, for example, if hypothetically, the total number of validators would drop to 3, there must still be a possibility to bridge out, and the smart contracts cannot enforce any minimum threshold on their own.

ISSUE#2

Improper Validator ID Management Enables Double Attestation

Low

Partially Fixed

Location

contracts/MezoBridge.sol#L290-L340

contracts/MezoBridge.sol#L650-L671

Description

The `attestBridgeOut` function allows a validator to attest a bridge out action, with each validator identified by a unique ID (e.g., v1 to v10 with IDs 1 to 10). However, the implementation does not prevent reuse of validator IDs without invalidating previous attestations linked to those IDs. If a validator (e.g., v3) is removed during an ongoing attestation process and their ID (e.g., 3) is reassigned to another validator (e.g., v10, the last validator), that validator can call `attestBridgeOut` function again using the reassigned ID, effectively enabling them to attest twice.

Impact

The finalization of `attestBridgeOut` operation may occur with fewer unique validator approvals than required.

Recommendation

We recommend maintaining a mapping of used validator addresses per attestation, rather than relying solely on validator IDs.

Verification Status

The Mezo team has modified the smart contract to make the bridge validator removal process a two-step process. They stated that the decision to implement the two-step process instead of the recommended mapping was dictated by significant gas savings on bridging operations if a separate mapping was to be maintained. This two-step process does not aim to address the issue fully, but rather enforce a proper process on the governance side that reduces risk of this issue.

ISSUE#3

Gas Optimization via Unchecked Increment in `_countSetBits`

None Acknowledged

Location

contracts/MezoBridge.sol#L345-L350

Description

In the `_countSetBits` function, the `count` is a `uint8`, and the loop increments it once per set bit. Given the protocol invariant that the number of validators (i.e., the number of set bits) never exceeds 255, the increment cannot overflow. Wrapping the `count++` in an `unchecked` block avoids the unnecessary overflow check and saves gas per iteration.

Impact

None.

Recommendation

We recommend enclosing the increment in an `unchecked` block to save gas.

Verification Status

The Mezo team stated that the gas saving is negligible (92363 vs 92193 on average for `attestBridgeOut`).

Section 5.0
Appendix A

Severity Rating Definitions

At Thesis Defense, we utilize the Immunefi Vulnerability Severity Classification System - v2.3.

Severity	Definition
Critical	• Manipulation of governance voting result deviating from voted outcome and resulting in a direct change from intended effect of original results • Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield • Direct theft of any user NFTs, whether at-rest or in-motion, other than unclaimed royalties • Permanent freezing of funds • Permanent freezing of NFTs • Unauthorized minting of NFTs • Predictable or manipulable RNG that results in abuse of the principal or NFT • Unintended alteration of what the NFT represents (e.g. token URI, payload, artistic content) • Protocol insolvency
High	• Theft of unclaimed yield • Theft of unclaimed royalties • Permanent freezing of unclaimed yield • Permanent freezing of unclaimed royalties • Temporary freezing of funds • Temporary freezing NFTs
Medium	• Smart contract unable to operate due to lack of token funds • Enabling/disabling notifications • Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol) • Theft of gas • Unbounded gas consumption
Low	• Contract fails to deliver promised returns, but doesn't lose value
None	• We make note of issues of no severity that reflect best practice recommendations or opportunities for optimization, including, but not limited to, gas optimization, the divergence from standard coding practices, code readability issues, the incorrect use of dependencies, insufficient test coverage, or the absence of documentation or code comments.

Section 6.0
Appendix B

Thesis Defense Disclaimer

Thesis Defense conducts its security audits and other services provided based on agreed-upon and specific scopes of work (SOWs) with our Customers. The analysis provided in our reports is based solely on the information available and the state of the systems at the time of review. While Thesis Defense strives to provide thorough and accurate analysis, our reports do not constitute a guarantee of the project's security and should not be interpreted as assurances of error-free or risk-free project operations. It is imperative to acknowledge that all technological evaluations are inherently subject to risks and uncertainties due to the emergent nature of cryptographic technologies.

Our reports are not intended to be utilized as financial, investment, legal, tax, or regulatory advice, nor should they be perceived as an endorsement of any particular technology or project. No third party should rely on these reports for the purpose of making investment decisions or consider them as a guarantee of project security.

Links to external websites and references to third-party information within our reports are provided solely for the user's convenience. Thesis Defense does not control, endorse, or assume responsibility for the content or privacy practices of any linked external sites. Users should exercise caution and independently verify any information obtained from third-party sources.

The contents of our reports, including methodologies, data analysis, and conclusions, are the proprietary intellectual property of Thesis Defense and are provided exclusively for the specified use of our Customers. Unauthorized disclosure, reproduction, or distribution of this material is strictly prohibited unless explicitly authorized by Thesis Defense. Thesis Defense does not assume any obligation to update the information contained within our reports post-publication, nor do we owe a duty to any third party by virtue of making these analyses available.