verichains

*SECURITY AUDIT OF*

# XPLA LAYERZERO V2 OFT

**Public Report**

*Mar 7, 2025*


## Verichains Lab

info@verichains.io

https://www.verichains.io

*Driving Technology > Forward*

# ABBREVIATIONS

| Name | Description |
|---|---|
| **Ethereum** | An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications. |
| **Ether (ETH)** | A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network. |
| **Smart contract** | A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract. |
| **Solidity** | A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform. |
| **ERC20** | ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain. |


# EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Mar 7, 2025. We would like to thank the XPLA for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the XPLA LayerZero V2 OFT. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit and penetration testing process, the audit team had identified no issue in the source code.

# TABLE OF CONTENTS

# 1. MANAGEMENT SUMMARY

## 1.1. About XPLA LayerZero V2 OFT

XPLA LayerZero V2 OFT enables seamless cross-chain asset transfers using LayerZero's omnichain messaging protocol.

## 1.2. Audit Scope

This audit focused on identifying security flaws in code and the log of the XPLA LayerZero V2 OFT.

It was conducted on commits `6fcbf76dc5c0b5ba5da8cdec3375e2be19901280` of repository https://github.com/xpladev/layerzero-oft.

| SHA256 Sum | File |
|---|---|
| cf68d7d9f664c7e08b39179f895a5d7a63204ad63cfb706de12a102ee435834e | contracts/XplaNativeOFTAdapter.sol |
| 84ccb460f0c3a6f7322f73d33becc3ac0ddb64974498c93c0747640953623b5c | contracts/XplaOFT.sol |

## 1.3. Audit Methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference

- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

| SEVERITY LEVEL | DESCRIPTION |
|---|---|
| **CRITICAL** | A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately. |
| **HIGH** | A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority. |
| **MEDIUM** | A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed. |
| **LOW** | An issue that does not have a significant impact, can be considered as less important. |

*Table 1. Severity levels*

## 1.4. Disclaimer

XPLA acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. XPLA understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, XPLA agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

## 1.5. Acceptance Minute

This final report served by Verichains to the XPLA will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the XPLA, the final report will be considered fully accepted by the XPLA without the signature.

# 2. AUDIT RESULT

## 2.1. Overview

The code was written in `Solidity` language, with the version `^0.8.22`.

`XplaOFT` is the native token of the Xpla blockchain, fully inherited from the `OFT` contract of `@layerzerolabs/oft-evm`. It is an ERC-20 compatible token with zero fees and requires no approval from the underlying token, as it already serves as the underlying asset.

`XplaNativeOFTAdapter` is a dedicated adapter for the native token (`XplaOFT`), implemented in the `NativeOFTAdapter` contract of `@layerzerolabs/oft-evm`. It enables zero-cost transfers, allowing users to exchange the native token without incurring any fees. Unlike other `OFTAdapter`, it does not have an internal token, eliminating the need for approval.

## 2.2. Findings

**During the audit process, the audit team had identified no issue in the source code.**

# 3. VERSION HISTORY

| Version | Date | Status/Change | Created by |
|---|---|---|---|
| **1.0** | *Mar 7, 2024* | Public Report | Verichains Lab |

*Table 2. Report versions history*