



Building the Futuristic **Blockchain Ecosystem**

SECURITY AUDIT REPORT

Joule-Aptos

TABLE OF CONTENTS

02	Table of Contents	
03	Overview	
04	Audit Summary	
05	Contract Details	
06	Audit Methodology	
07	Vulnerabilities Checklist	
08	Risk Classification	
09	Ownership Privileges	
14	Functions	
16	Centralization Privileges	
17	Manual Review	
18	Findings	
22	About Expelee	
23	Disclaimer	

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Overall Security	Contract is Safe to Deploy
Audit Date	16 March 2024

Note for Investors: We only audited contracts mentioned in the File Overview. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way

AUDIT SUMMARY

Version : v1.0

- Manual Functionality Review
- Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract's logic. We cannot guarantee 100% logical correctness of the contract as it was not functionally tested by us.

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with a SHA-1 Hash.

1. Move.toml
2. bridge.move
3. limiter.move
4. lz_impl.move

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

1. Aptos-framework
2. layerzero
3. layerzero_common
4. ZRO

CONTRACT DETAILS

Token Name: --

Symbol: --

Network: Aptos

Language: Move

Contract Address: --

Owner's Wallet: --

Deployer's Wallet: --

AUDIT METHODOLOGY

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - Reviewing the specifications, sources, and instructions provided to Expelee to ensure we understand the size, scope, and functionality of the smart contract.
 - Manual review of the code, i.e. reading the source code line by line to identify potential vulnerabilities.
 - Comparison to the specification, i.e. verifying that the code does what is described in the specifications, sources, and instructions provided to Expelee
2. Testing and automated analysis that includes the following:
 - Test coverage analysis, which determines whether test cases actually cover code and how much code is executed when those test cases are executed.
 - Symbolic execution, which is analyzing a program to determine what inputs causes each part of a program to execute.
3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.
4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zepplin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warnings that can remain unfixed.

Informational

Issues on this level are minor details and warnings that can remain unfixed.


OWNERSHIP PRIVILEGES

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refers to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or a designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner cannot mint new tokens

 **The owner cannot mint new tokens**

Description :

The owner is not able to mint new tokens once the contract is deployed

Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens

 **The owner cannot burn tokens**

Description

The owner is not able burn tokens without any allowances.

OWNERSHIP PRIVILEGES

Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

**Contract owner cannot
blacklist addresses**



The owner cannot blacklist addresses

Description :


The owner is not able blacklist addresses to lock funds.

OWNERSHIP PRIVILEGES

Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fee

 **The owner cannot set fees**

Description :

The owner is not able to set the fees above 25%

Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Contract owner can lock the contract

The owner is able to lock the contract

Description

Locking the contract means that the owner is able to lock any funds of addresses that they are not able to transfer bought tokens anymore.

Example

An example of locking is by pausing the contract or blacklisting any addresses. That causes that the blacklisted address is not able to transfer (buy/sell) anymore.

OWNERSHIP PRIVILEGES

Ownership

The ownership is not renounced

X The owner is not renounce

Description :

The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including:

- Centralizations
- The owner has significant control over contract's operations

Comment :

In case of this contract, as it is a token bridge, the ownership is needed to administrate the bridge during its on-chain operations.

Note - If the contract is not deployed then we would consider the ownership to be not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced

OWNERSHIP PRIVILEGES

Upgradeability

Contract is an upgradeable

✗ Deployer can update the contract with new functionalities

Description :

The deployer can replace the old contract with a new one with new features. Be aware of this, because the owner can add new features that may have a negative impact on your investments.

Example :

We assume that you have funds in the contract and it has been audited by any security audit firm. Now the audit has passed. After that, the deployer can upgrade the contract to allow him to transfer the funds you purchased without any approval from you. This has the consequence that your funds can be taken by the creator.

Comment :

Important to Know! The Aptos blockchain natively supports different upgrade policies, which allow move developers to explicitly define the constraints around how their move code can be upgraded. The default policy, which is also use in the audited contract, is backwards compatible. This means that code upgrades are accepted only if they guarantee that no existing resource storage or public APIs are broken by the upgrade (including public functions).

FUNCTIONS





External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables



State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable

Components

 Contracts	 Libraries	 Interfaces	 Abstract
3	3	0	0


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

 Public	 Payable
15	0




External	Internal	Private	Pure	View
3	31	0	0	4

State Variable

Total	 Public
11	11

FUNCTIONS

Capabilities

Move Versions observed	 Experimental Features	Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
3.0.1	_____	_____	_____	_____

CENTRALIZATION PRIVILEGES

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.

In the project there are authorities that has the authority over the following functions:

File	Privileges
bridge.move	<ul style="list-style-type: none">❖ onlyAdmin<ul style="list-style-type: none">• Owner can register coins• Owner can set limiter cap• Owner can set remote coins• Owner can pause contract global• Owner can pause single token• Owner can enable custom adapter parameters• Owner get coin capabilities

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart contract-based accounts, such as multi-signature wallets.

Here are some suggestions what the client can do.

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness on privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are dividend into three primary risk categorieis:

High

Medium

Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious input handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

RISK FINDINGS

Findings	Severity	Found
High Risk	● High	0
Medium Risk	● Medium	0
Low Risk	● Low	0
Suggestion & discussion	● Informational	3

INFORMATIONAL RISK FINDING

Unused Alias

File: Main

Severity: Informational

Location: L19

Status: Open

Description

- Make sure to alias only if you need.
- There are also multiple unused aliases in used packages, further details are appended in output.txt

INFORMATIONAL RISK FINDING

Unused Return Values

File: Bridge.move

Severity: Informational

Location: L276

Status: Open

Description

- Ensure that all the return values of the function calls are used.

INFORMATIONAL RISK FINDING

Unused Function Parameters

File: Layerzero packages

Severity: Informational

Status: Open

Description

- There are multiple unused function parameters in used packages. Further details are appended in output.txt

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

 www.expelee.com

 [expeleeofficial](https://twitter.com/expeleeofficial)

 [expelee](https://medium.com/expelee)

 [Expelee](https://t.me/Expelee)

 [expelee](https://in.linkedin.com/company/expelee)

 [expelee_official](https://www.instagram.com/expelee_official)

 [expelee-co](https://github.com/expelee-co)

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.

The logo for Expelee, featuring the word "expelee" in a stylized font. The "ex" is in white, and "pelee" is in orange. The letters are bold and modern.

Building the Futuristic **Blockchain Ecosystem**