SOLIDITY AUDIT

AUDIOTRIUM

www.auditorium.com

SOLIDITY REVIEW

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

AUDITORIUM

SMART CONTRACT REVIEW

SECURITY ANALYSIS REPORT

CLIENT :

AUDITORIUM - REG

Telegram : @AuditorBSC

AuditorBsc@gmail.com

NAME	ZETA SYSTEM
APPROVED BY	FREY | SOURCE CONTRACT AUDITOR
TYPE	BEP20 SMART CONTRACT
PLATFORM	BNB SMART CHAIN (BEP20)
Language	SOLIDITY
Methods	MANUAL REVIEW BY TEAM
WEBSITE	https://zeta-system.org/
TIMELINE	10.11.2022 - 10.11.2022
LOG	10.11.2022 - MANUAL REVIEW

Auditorium is a solidity auditor born in 2022 with a vision of transforming Web3 into a safer place.

Auditorium protects technological businesses and crypto communities worldwide with the most competitive suite of professional cybersecurity services.

AUDITORIUM - REG
Telegram : @AuditorBSC
AuditorBsc@gmail.com

Introduction

Auditorium (Consultant) was contracted by Zeta System (Customer) to conduct a Smart Contract Code Review and Security Analysis.

This report presents the findings of the security assessment of the Customer's smart contracts.

Smart Contract	0x4d9705f0cbf61f760a4b913a3808cfab557b61ff	🟩
Owner / Deployer	https://bscscan.com/address/0xf030aa56bdf2f1c3bc8922f43b59d9739e7ecd9f	🟩
Smart Contract Reposity	https://github.com/AuditoriumSolidity/ZetaFinance_Audit/blob/main/Smartcontract.sol	🟩
Documentation Client	-	▨
TAX	**BUY : 8 / SELL : 9**	🟩
MARKET	**PANCAKESWAP**	🟩
CAN SELL	**YES**	🟩
GASS	**BUY : 184,758 | SELL : 338,437**	🟩

NOTE

🟥	WARNING	🟩	PASSED
▨	NEED ACTION		

AUDITORIUM - REG
Telegram : @AuditorBSC
AuditorBsc@gmail.com

CHECKED ITEM

We have audited provided smart contracts for commonly known and more,specific vulnerabilities. Here are some of the items that are considered:

ITEM	TYPE	DESCRIPTION	STATUS
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	PASSED
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	PASSED
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASSED
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	PASSED
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASSED
Access Control & Authorization	SWC-105	Ownership takeover should not be possible. All crucial functions should be protected. Users could not affect data that belongs to other users.	PASSED
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASSED

AUDITORIUM - REG
Telegram : @AuditorBSC
AuditorBsc@gmail.com

ITEM	TYPE	DESCRIPTION	STATUS
Liquidity Lock	SWC-107	Liquidity must be locked for 1 year, making sure everything is safe to avoid scams	PASSED
Check-Effect Interaction	SWC-107	Check-Effect-Interaction pattern should be followed if the code performs ANY external call.	PASSED
Assert Violation	SWC-110	Properly functioning code should never reach a failing assert statement.	PASSED
Deprecated to Untrusted Callee	SWC-111	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	PASSED
Unchecked Call Return Value	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASSED
DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless it is required.	PASSED
Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	PASSED
Authorization	SWC-115	Authorization SWC-115 tx.origin should not be used for	PASSED
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	PASSED
Signature Unique Id	SWC-117 SWC-121 SWC-122 EIP-155	Signed be used as a unique id. Chain identifier should always have a unique id. A transaction hash should not should always be used.	PASSED
Shadowing State Variable	SWC-119	State variables should not be shadowed.	PASSED

AUDITORIUM - REG
Telegram : @AuditorBSC
AuditorBsc@gmail.com

PROJECT OVERVIEW

ZETA SYSTEM

Zeta is a start-up company that focuses on the security of decentralized cryptocurrency systems

Zeta Network's is open, permissionless, a standard allowing anyone to build on top and fully empowering the user with the ability to create regulatory compliant digital assets. Will bring about significant efficiency gains, cost savings, transparency, faster payouts, and fraud mitigation while allowing for data to be shared in real-time between various parties in a trusted and traceable manner.ZETA SYSTEM Token staking, governance, paying transaction fees and gaining eligibility in ZETA SYSTEM.

- **ZETA SYSTEM — a simple ERC-20 token that not mints all initial supply ,to a deployer. Additional minting is not allowed. It has the following attributes:**

- NAME TOKEN : ZETA SYSTEM
- TICKER : ZETA
- DECIMALS : 9
- TOTAL SUPPLY : 10,000,000,000 **ZETA**

Privileged roles

- set_Max_Transaction_Percent can modify max tx amount
- set_New_Pair_Address has onlyOwner modifier
- set_New_Router_Address has onlyOwner modifier
- set_New_Router_and_Make_Pair has onlyOwner modifier
- blacklist_Remove_Wallets has onlyOwner modifier
- Owner can blacklist addresses, honeypot risk
- _set_Fees has onlyOwner modifier
- _set_Fees can probably change the fees

MEDIUM RISK

AUDITORIUM - REG
Telegram : @AuditorBSC
AuditorBsc@gmail.com

RECOMENDATION

🟥 CRITICAL : No critical severity issues were found.

🟨 HIGH : No high severity issues were found.

🟩 MEDIUM :

- set_Max_Transaction_Percent can modify max tx amount - Rec : **Turn Off**
- Owner can blacklist addresses, honeypot risk - Rec : **Turn Off**
- _set_Fees has onlyOwner modifier - Rec : **Turn Off**
- blacklist_Add_Wallets has onlyOwner modifier - Rec : **Turn Off**

🟦 LOW : No low severity issues were found.

Additional Report

LIQUIDITY LOCK	https://mudra.website/?certificate=yes&type=0&lp=0x19937c64c5e9dc4587d61ec78aa54418c117e75d
LIQUIDITY LOCK PERCENTAGE	**87,3 % - 360 DAYS**
TOTAL LOCK OWNER	**1 DEPLOYER ADDRESS**

AUDITORIUM - REG
Telegram : @AuditorBSC
AuditorBsc@gmail.com

DISCLAIMERS

Auditorium Disclaimer

The smart contracts given for audit have been analyzed by the best industry and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit cannot guarantee the explicit security of the audited smart contracts.

DONATION

0x7C2EAaf8C19C1f7f2b4D1086BfFB52E7A765aB5B

BEP20 , BNB , BUSD , USDT

Auditorium contact
https://t.me/Ferrykillua