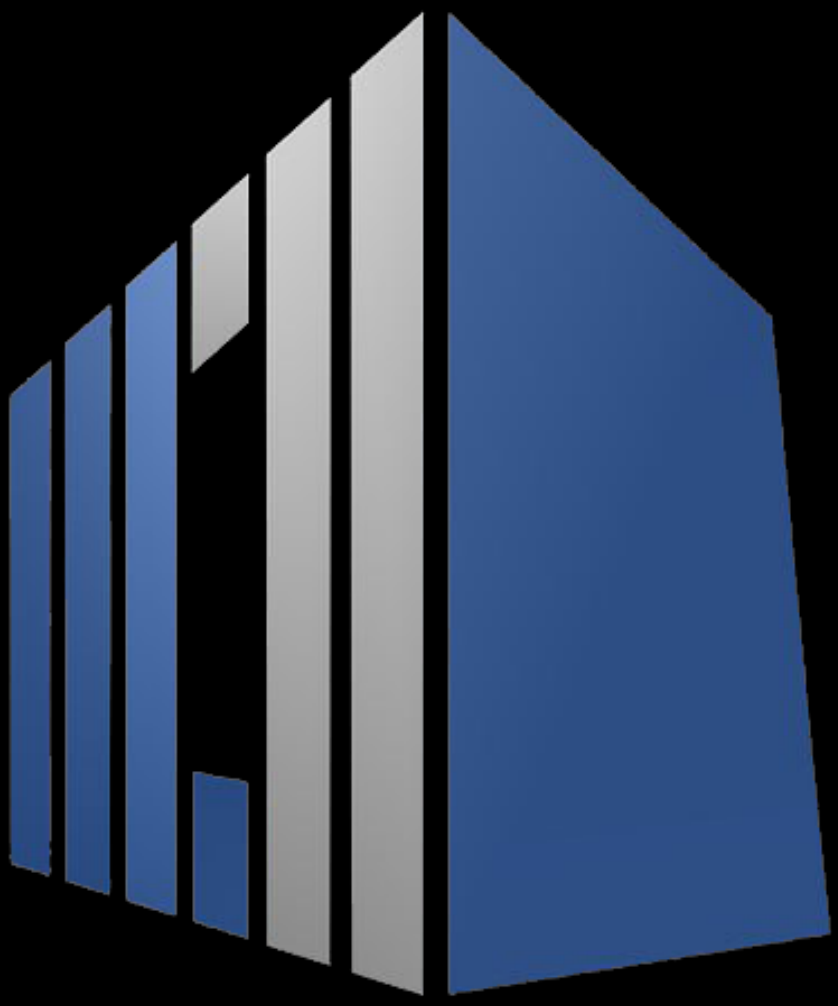


LayerOne

Audit & KYC

LayerOne
Audit & KYC

Table of Contents

SUMMARY OF AUDIT

TECHNICAL DETAILS

Audited Project:	Gambler Shiba – (AGS)
Source Code:	https://arbiscan.io/address/0x1c7f32699ff9163f928089c0a4d6ee5ad5885c6f#code
Solidity File:	GamblerShiba.sol
Security Audit Date:	2023-01-04
Revisions:	Initial audit 2023-01-04
Auditing Methods:	Automatic review + manual review

AUDITING METHODS AND VALIDATIONS

Evaluation objective for the security audit:

- Smart contract code quality assurance check
- Security issues and vulnerabilities deep code evaluation
- Use-case specifications validation
- Best practice smart contract code compliance
- Documentation, project specifications and comments

The contract is checked for possible vulnerabilities and issues. Recommendations may be made for code improvements where severe or medium issues are found:

- Dependence transaction order
- Reentrancy issues
- Time dependency
- Integer overflow
- Integer underflow
- Mishandled exceptions
- Call stack limits
- Unsafe external calls
- Number rounding errors
- Gas efficiency check
- Logical oversights
- Access control
- Centralization issues
- Logic-specification
- Contradiction
- Functionality duplication
- Malicious contract behavior
- Abusable functions
- Potential DoS vulnerabilities

The code review conducted for this audit follows the following structure:

1. Review of the specifications, documentation and commenting provided by the project owners regarding the functionality of the smart contract.
2. Automated analysis of the smart contract followed by manual, line-by-line analysis of the smart contract.
3. Assessment of smart contracts alignment with the documentation and comments when compared to its functionality.
4. Assessment of the code against best practices.
5. Recommendations for code improvements where severe or medium vulnerabilities are found.

LayerOne
Audit & KYC

SMART CONTRACT DETAILS

Contract ID:	0x1c7f32699ff9163f928089c0a4d6ee5ad5885c6
Blockchain:	Arbitrum
Language Used:	Solidity
Compiler Version:	v0.6.12+commit.27d51765
Blockchain Scan Verification:	2022-11-04
Type of Smart Contract:	ERC20 Token
Optimization Enabled:	Yes – 200 runs
Number of Interfaces:	3
Number of Contracts:	4
Number of Libraries:	3

SUMMARY OF AUDIT RESULTS - **PASSED**

LayerOne Cloud (Pty) Ltd smart contract audit for Gambler Shiba (AGS) is marked as PASSED without severe issues on the logic and functions of the contract.

Review of the documentation, description of the projects use-case and the contract, reveals that it follows the line of good practice. It is a clean and default commented contract. There are no severe vulnerability findings in the contract and no concerns about malicious use of the contract functions.

NOTE:
*Contract owner can change maximum transaction amount.
*Contract owner is able to whitelist wallets and change limits.
*Contract is not renounced.

AUDIT DETAILS

SEVERITY OF RISKS AND VULNERABILITIES

LOW-SEVERITY	MEDIUM-SEVERITY	HIGH-SEVERITY
0	0	0

REPORTED VULNERABILITIES AND ISSUES

No issues or vulnerabilities.

FINDINGS

No medium or severe findings on the contract or noticeable logical issues.

SPECIFICATIONS, DOCUMENTATION AND COMMENTS

The code has a decent number of comments and documentation.

Improving comments in smart contracts using simple, commonly understood terms, helps the userbase understand its functionalities and use-case. Functions in this contract are written to be human readable and easy to understand given a previous knowledge of basic functions and the project goals.

CORRECTNESS OF SPECIFICATIONS

Smart contract follows the functionality that is stated in the documentation and description of the contract. The use-case is also in line what is described about the project.

MANUAL AND AUTOMATED CODE REVIEW RESULTS

Code Audit

Critical: no findings, nothing to worry about.
Major: no findings, nothing to worry about.
Medium: no findings, nothing to worry about.
Minor: no findings, nothing to worry about.
Informational: none

Checks Completed

Gas efficiency check: passed
Contract vulnerabilities check: passed
Reentrancy issues check: passed
Integer over/under flows check: passed
Front running opportunities check: passed
Interface / naming issues check: passed
Order of execution check: passed
Time component check: passed
Blockhash function check: passed
Exception handling check: passed
Third-party integration check: passed
Replay attack check: passed
Short address attack check: passed

ALIGNMENT WITH DOCUMENTATION, COMMENTS AND FUNCTIONALITY

Review of the documentation, description of the projects use-case and the contract, reveals that it follows the line of good practice. It is a clean and default commented contract. There are no severe vulnerability findings in the contract and no concerns about malicious use of the contract functions.

ASSESSMENT OF BEST PRACTICES COMPLIANCE

The contract follows the best practices in majority and there are no concerns from the auditor of any malicious use of the contracts functions. Team is fully verified and interviewed.

RECOMMENDATIONS

None

DETAILED DESIGN DIAGRAMS

DIAGRAM A – view online

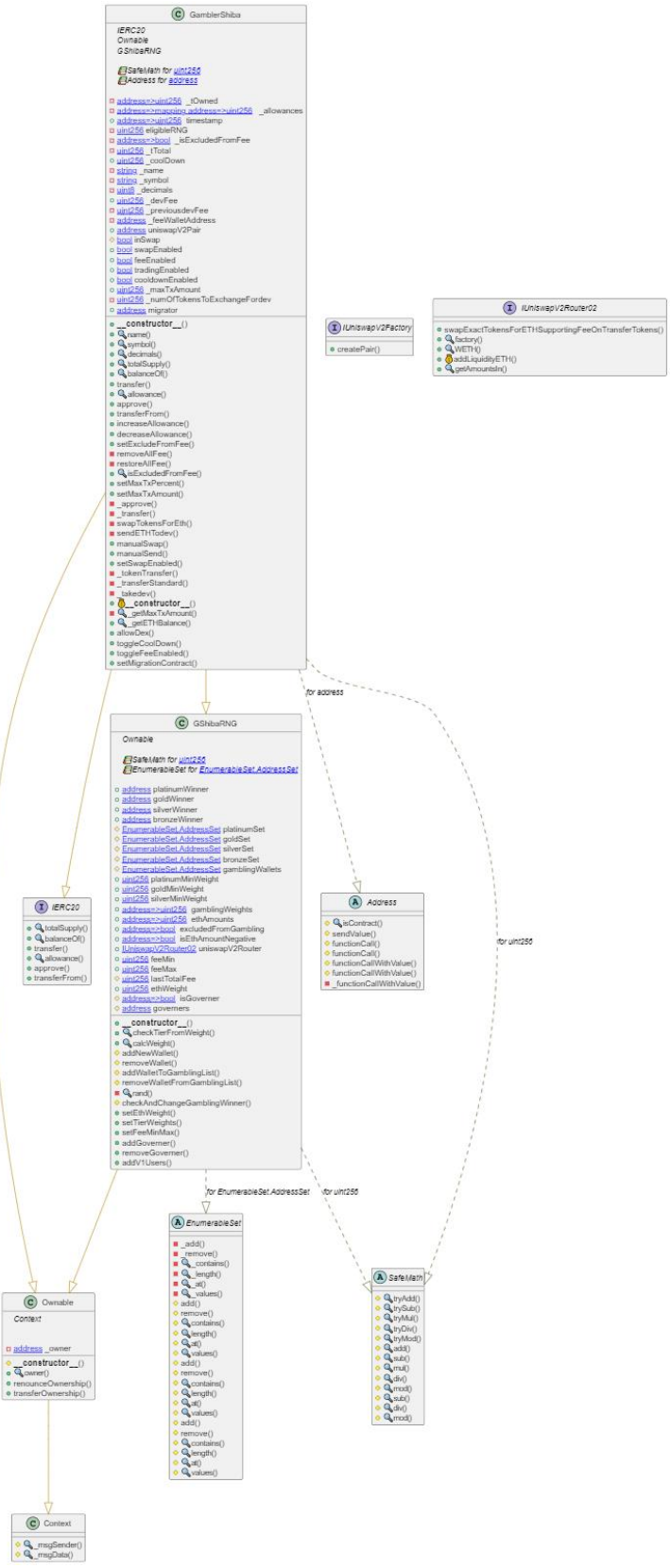
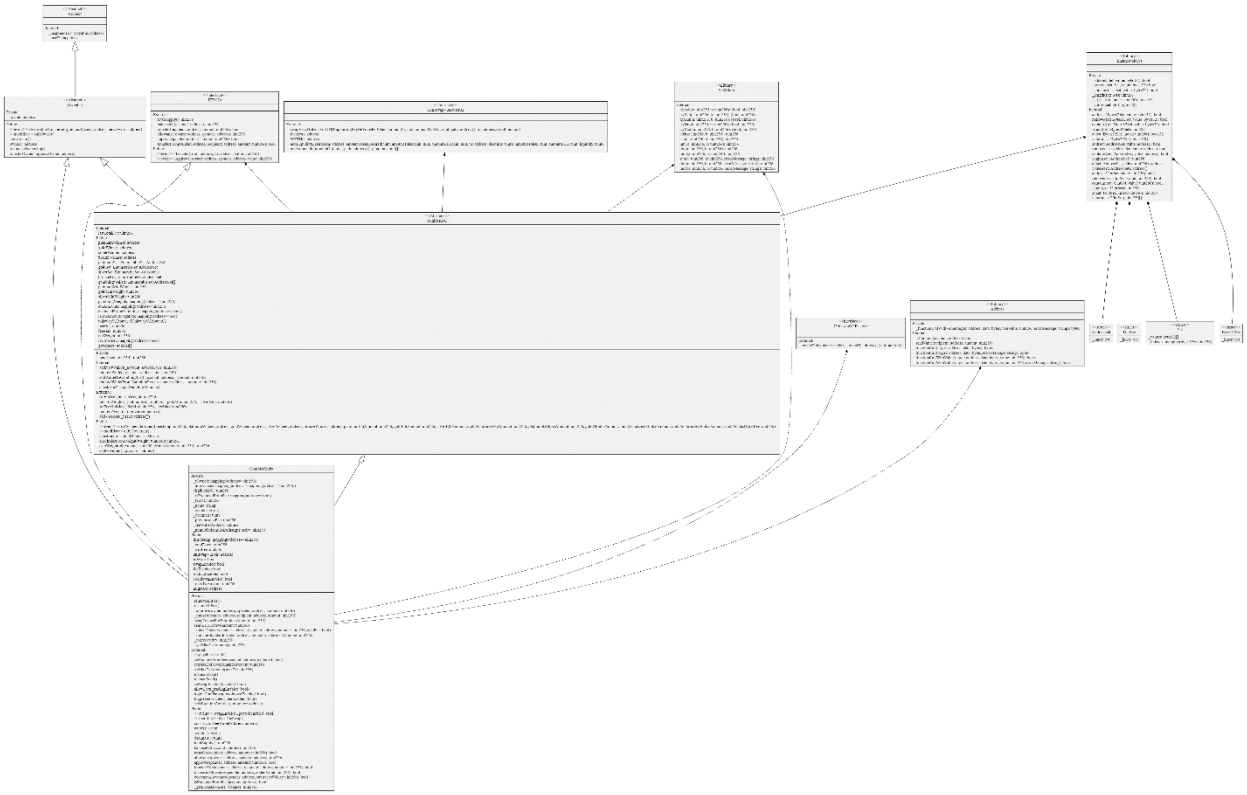


DIAGRAM B – view online



HISTORY OF REVISIONS

Initial audit was performed 2023-01-04 and there is no need for further revisions of the smart contract. The project team has been informed of a clean audit result.