InterFi Network

@interfinetwork

SMART CONTRACT SECURITY AUDIT

STAKED ADA

AUDITED ON SEPTEMBER 13, 2021

USING INTERFI AUDITING ARCHITECTURE

Summary

Audit:

Auditing Firm	InterFi Network
Architecture	InterFi Auditing Architecture
Smart Contract Audit Approved By	Chris | Blockchain Specialist at InterFi
Project Overview Approved BY	Albert | Project Specialist at InterFi
Platform	Solidity
Audit Check (Mandatory)	Vulnerability Check, Source Code Review, Functional Test
Project Check (Optional)	Website Review, Socials Review, Token Review (Not Applicable)
Consultation Request Date	September 09, 2021
Report Date	September 13, 2021

Risk profile:

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit, **Staked ADA's smart contract source code has No-Risk Severity.**

Staked ADA has also successfully passed the KYC verification with InterFi. Please check InterFi's GitHub to check the KYC certificate.

For a detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit.

Table Of Contents

Project Overview

InterFi was consulted by Staked ADA on September 09, 2021, to conduct a smart contract security audit of their solidity source code.

Public information

Staked ADA is a reward-generating smart contract on the Binance Smart Chain that allows the holders to passively build a long-term portfolio of the Cardano. Staked ADA distributes the users 13% transaction tax in ADA rewards.

Summary: **Holders automatically build long-term investment in ADA just by holding Staked ADA.**

Information	Staked ADA
Blockchain	Binance Smart Chain
Language	Solidity
Contract	0x5f311d27e391c6d4f09e3044c3cef3ad2fa6e5b6
Symbol	STADA
Website	https://stakedada.com/
Twitter	https://twitter.com/StakedADA
Reddit	https://www.reddit.com/r/StakedADA/

Public logo

Solidity Source Code & Extras

https://bscscan.com/address/0x5f311d27e391c6d4f09e3044c3cef3ad2fa6e5b6#code

https://github.com/interfinetwork/audited-codes/blob/main/Staked%20ADA.sol

GitHub Commits

Solidity source code committed at: 91f8181d4cf86fee77490ccbef4f4c8a85e9a1b5

Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of Staked ADA. The source code can be viewed in its entirety on

https://github.com/interfinetwork/audited-codes/blob/main/Staked%20ADA.sol

InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category	
Smart Contract Vulnerabilities	❖ Re-entrancy (RE) ❖ Unhandled Exceptions (UE) ❖ Transaction Order Dependency (TO) ❖ Integer Overflow (IO) ❖ Unrestricted Action (UA)
Source Code Review	❖ Ownership Takeover ❖ Gas Limit and Loops ❖ Deployment Consistency ❖ Repository Consistency ❖ Data Consistency ❖ Code Typo Error ❖ Token Supply Manipulation
Functional Assessment	❖ Access Control and Authorization ❖ Operations Trail and Event Generation ❖ Assets Manipulation ❖ Liquidity Access

ECHELON-1 Analysis

The aim of "InterFi's ECHELON-1 Analysis" is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

1. Code review that includes the following
   - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
   - ❖ Manual review of code, which is the process of reading source code line-by-line to identify potential vulnerabilities.
2. Testing and automated analysis that includes the following
   - ❖ Test coverage analysis, which is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
   - ❖ Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

Automated 3P frameworks used to assess the smart contract vulnerabilities

- ❖ Slither
- ❖ MythX
- ❖ Consensys Mythril
- ❖ Open Zeppelin
- ❖ Solidity Code Complier

InterFi's Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in Ether. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

Vulnerable: A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false positive.

Exploitable: A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the "vulnerability" flagged by a tool is in a function that requires owning the contract, it would be vulnerable but not exploitable.

Exploited: A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

Risk severity	Meaning
! Critical	This level of vulnerability could be exploited easily and can lead to asset loss, data loss, asset manipulation, or data manipulation. They should be fixed right away.
! High	This level of vulnerability is hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to critical risk severity
! Medium	This level of vulnerability should be fixed, as they carry an inherent risk of future exploits, and hacks that may or may not impact the smart contract execution.
! Low	This level of vulnerability can be ignored. They are code-style violations and informational statements in the code. They may not affect the smart contract execution

Smart Contract Overview

Knick-knacks in the smart contract

Query	Result
_name	Staked ADA
_symbol	STADA
_decimals	9
TotalSupply	100,000,000,000
ADA Address	0x3EE2200Efb3400fAbB9AacF31297cBdD1d435D47
WBNB Address	0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c
minimumTokenBalanceForDividends	1,000,000
_burnFee	1%
_reflectionFee	13%
_marketingFee	3%
_totalFees	17%
IDEXRouter	0x10ED43C718714eb63d5aA57B78B54704E256024E

Vulnerability	Status
Compiler errors	Passed
Re-entrancy. Race conditions and cross-function race conditions (RE)	Passed
Possible delays in data delivery	Passed
Gas optimization	Passed
Integer Underflow and overflow	Passed
Oracle Calls	Passed
Call stack depth attack	Passed
Parity Multisig Bug	Passed
Tx ordering dependency (TO)	Passed
DOS with revert and block gas limit	Passed
Private user data leaks	Passed
Malicious event log	Passed
Safe open zeppelin contract implementation and usage	Passed
The impact of exchange rate on the logic	Passed
Functions that are not used (dead-code)	Passed
Typographical Errors	Passed
Signature Malleability	Passed
Floating Pragma	Passed
Scoping and declarations	Passed

Verifying token functions

Function	Description	Tested	Verdict
Total Supply	provides information about the total token supply	**Yes**	**Passed**
Balance Of	provides account balance of the owner's account	**Yes**	**Passed**
Transfer	executes transfers of a specified number of tokens to a specified address	**Yes**	**Passed**
Transfer From	executes transfers of a specified number of tokens from a specified address	**Yes**	**Passed**
Approve	allow a spender to withdraw a set number of tokens from a specified account	**Yes**	**Passed**
Allowance	returns a set number of tokens from a spender to the owner	**Yes**	**Passed**

Verified

- The owner can mint tokens at token launch.
- The owner cannot pause the contract.
- The owner cannot burn/lock users' assets

Note

- Be aware that active smart contract owner privileges constitute an elevated impact on smart contract safety.

Points To Note

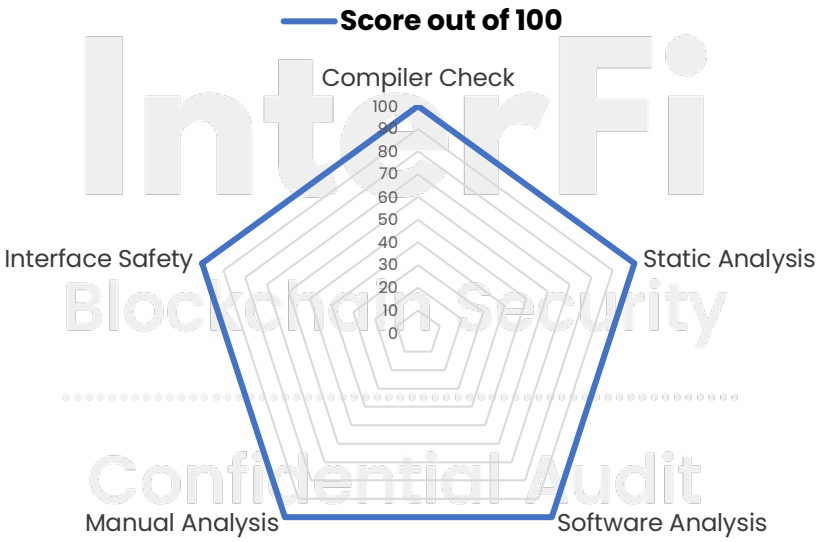
The Staked ADA smart contract utilizes the "SafeMath" to prevent Integer Overflow.

```
    ftrace | funcSig
    function mul(uint256 a1, uint256 b1) internal pure returns (uint256) {
        if (a1 == 0) {
            return 0;
        }

        uint256 c = a1 * b1;
        require(c / a1 == b1, "SafeMath: multiplication overflow");

        return c;
    }
    ftrace | funcSig
    function div(uint256 a1, uint256 b1) internal pure returns (uint256) {
        return div(a1, b1, "SafeMath: division by zero");
    }
    ftrace | funcSig
    function div(uint256 a1, uint256 b1, string memory errorMessage1) internal pure returns (uint256) {
        // Solidity only automatically asserts when dividing by 0
        require(b1 > 0, errorMessage1);
        uint256 c = a1 / b1;
        // assert(a == b * c + a % b); // There is no case in which this doesn't hold

        return c;
    }
}
```

Smart Contract Risk Assessment

SWC Errors	Issue	Severity
NULL	NULL	NULL

Risk Severity	Status
! Critical	No critical severity issues are identified
! High	No high severity issues are identified
! Medium	No medium severity issues are identified
! Low	No low severity issues are identified
Passed	**25 functions and instances are verified and passed**



Compiler Check	100
Static Analysis	100
Software Analysis	100
Manual Analysis	99.9
Interface Safety	99.9

Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

Staked ADA's smart contract source code has NO RISK SEVERITY.

Staked ADA has PASSED InterFi's ECHELON-1 standard smart contract audit.

Staked ADA has also PASSED InterFi's KYC verification. The KYC certificate can be accessed on our GitHub.

Auditor's Footnote:

- Be aware that active smart contract owner privileges constitute an elevated impact on smart contract safety and security.
- The project's liquidity pair isn't checked and verified due to being out of scope.
- The project website is not checked due to being out of scope. The website hasn't been reviewed for SSL and lighthouse reports.

Important Disclaimer

InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyze the on-chain smart contract source code and to provide a basic overview of the project. **This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purpose without InterFi's prior written consent.**

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, 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. **Be aware that smart contracts deployed on a blockchain aren't resistant to external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact on smart contract safety and security. Therefore, InterFi does not guarantee the explicit security of the audited smart contract.**

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report should not be considered as an endorsement or disapproval of any project or team. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. Do conduct your due diligence and consult your financial advisor before making any investment decisions.

About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. **InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy to use.**

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. **InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.**

For more information, visit https://interfi.network

To book an audit, message https://t.me/interfiaudits