ASSURE DEFI®
THE VERIFICATION GOLD STANDARD

Security Assessment:

Regayov STAKING

November 27, 2024

- Audit Status: **Pass**
- Audit Edition: **Advance**

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
Critical	Danger or Potential Problems.
High	Be Careful or Fail test.
Medium	Pass, Not-Detected or Safe Item.
Low	Function Detected

Manual Code Review Risk Results

Contract Privilege	Description
Buy Tax	0%
Sale Tax	5%
Cannot Buy	Pass
Cannot Sale	Pass
Max Tax	5%
Modify Tax	No
Fee Check	Pass
Is Honeypot?	Not Detected
Trading Cooldown	Not Detected
Can Pause Trade?	Pass
Pause Transfer?	Not-Detected
Max Tx?	Pass
Is Anti Whale?	Not-Detected
Is Anti Bot?	Not-Detected

Contract Privilege	Description
Is Blacklist?	Not-Detected
Blacklist Check	Pass
is Whitelist?	Not-Detected
Can Mint?	Pass
Is Proxy?	Not Detected
Can Take Ownership?	Not Detected
Hidden Owner?	Not-Detected
Owner	0x57272861395F1858eA5400fbB7A24b7Cebc211A0
Self Destruct?	Not Detected
External Call?	Not-Detected
Other?	Not Detected
Holders	4
Auditor Confidence	Medium
KYC Present	No
KYC URL	

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Project Overview

Token Summary

Parameter	Result
Address	0x80ca5D601390Ca7Cc87F775abF0E3b112AC91895
Name	Regayov
Token Tracker	Regayov (HSACV)
Decimals	18
Supply	10,000,000,000
Platform	ETHEREUM
compiler	v0.8.6+commit.11564f7e
Contract Name	Staking
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://sepolia.etherscan.io/address/0x80ca5D601390Ca7Cc87F775abF0E3b112AC91895#code
Payment Tx	Corporate

Main Contract Assessed
Contract Name

Name	Contract	Live
Regayov	0x80ca5D601390Ca7Cc87F775abF0E3b112AC91895	Yes

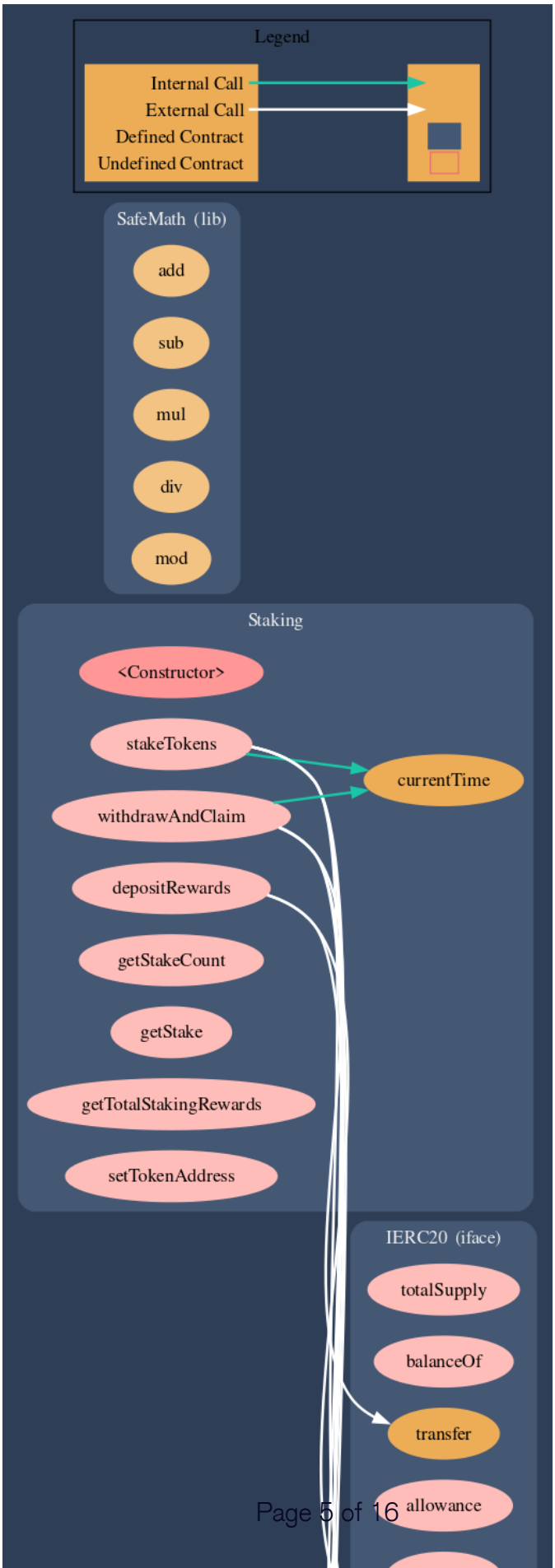
TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
Staking	75b6ee250b22d5aed6517a2d8139773b6d5702d9	Staking.sol
Staking		.sol
Staking		.sol
Staking		.sol
Staking		.sol
Staking		.sol

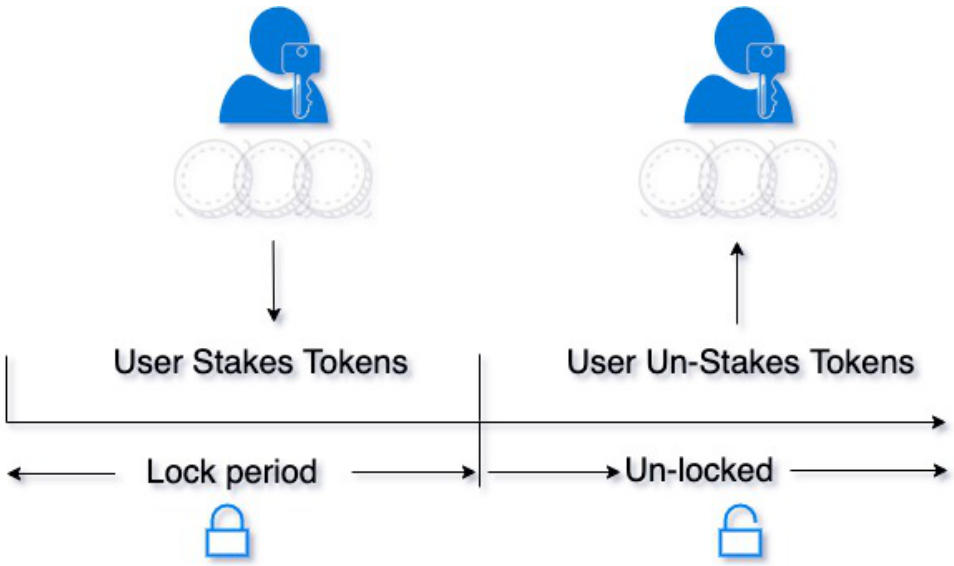
Call Graph

The contract for Regayov has the following call graph structure.



What is a Staking Contract

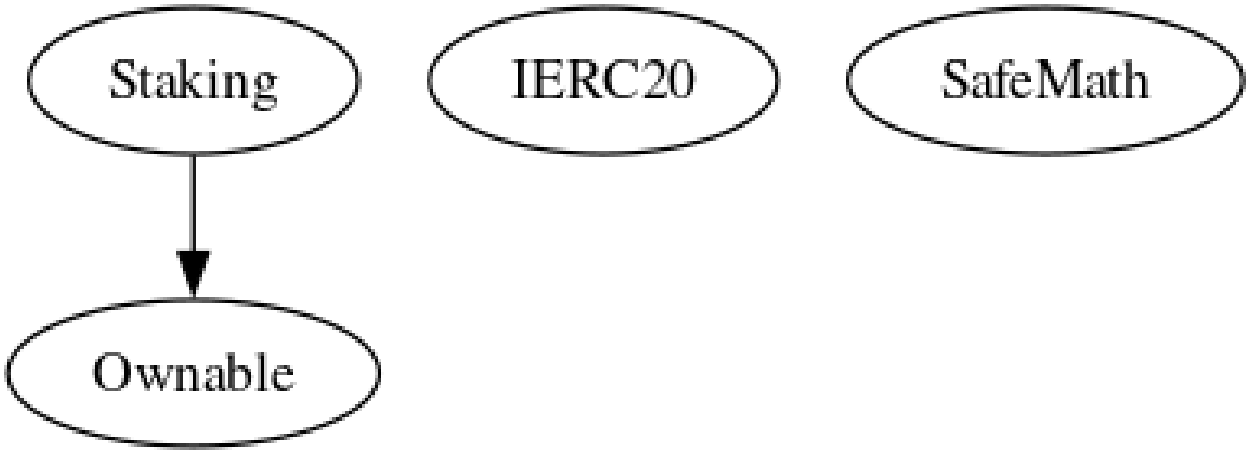
A smart contract which allows users to stake and un-stake a specified ERC20 token. Staked tokens are locked for a specific length of time (set by the contrat owner at the outset). Once the time period has elapsed, the user can remove their tokens again.



Inheritance

The contract for Regayov has the following inheritance structure.

The Project has a Total Supply of 10,000,000,000



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership		Public
depositRewards		External
setTokenAddress		External

HSACV-20 | Lack of Emergency Withdraw Functionality .

Category	Severity	Location	Status
	Medium	Staking.sol:	Detected

Description

No function to allow users to withdraw staked tokens in case of an emergency.

Remediation

Implement an emergency withdraw function..

Project Action

Technical Findings Summary

Classification of Risk

Severity	Description
Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
Critical	0	0	0
High	0	0	1
Medium	1	1	3
Low	0	0	2
Informational	0	0	0
Total	1	1	6

Social Media Checks

Social Media	URL	Result
Twitter		Pass
Other		N/A
Website		Pass
Telegram		Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Assessment Results

Score Results

Review	Score
Overall Score	91/100
Auditor Score	90/100
Review by Section	**Score**
Manual Scan Score	18
Auto Scan Score	37
Advance Check Score	36

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Assessment Results

Important Notes:

- User Safety: There is no emergency withdrawal function, which could leave users unable to access their funds in unforeseen circumstances.ı
- Flexibility: Hardcoded stake durations and rewards limit adaptability to changing conditions or strategies.ı
- Monitoring: Some critical actions lack event emissions, reducing transparency and traceability.ı
- Usability: Users cannot extend their stake durations, which may limit their engagement with the platform.ı
- Debugging: Error messages are generic, which could hinder troubleshooting and user experience.ı
- Overall Classificationı
- Risk Level: Mediumı
- Areas of Concern: User Safetyı
- Scoreı
- Score: 91/100ı
- Pass/Fail: Passı
- Summary: The contract Pass the audit with a score of 91 due to medium risk issues in user safety. Addressing these issues is crucial for improving security and functionality.

Auditor Score =90
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.