



Smart Contract Security Audit Report

STAY

December 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

STAY



Deployer address

0x9e1b604766b7b55dc48196fa150f66ecc7598f87



Client contacts

STAY Team



Blockchain

Binance smart chain



Website

<https://www.staytoken.org/>

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by STAY to perform an audit of smart contracts:

- <https://bscscan.com/address/0x127415D59E508c70A3990175C8267eb9C49b84fC#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understood to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

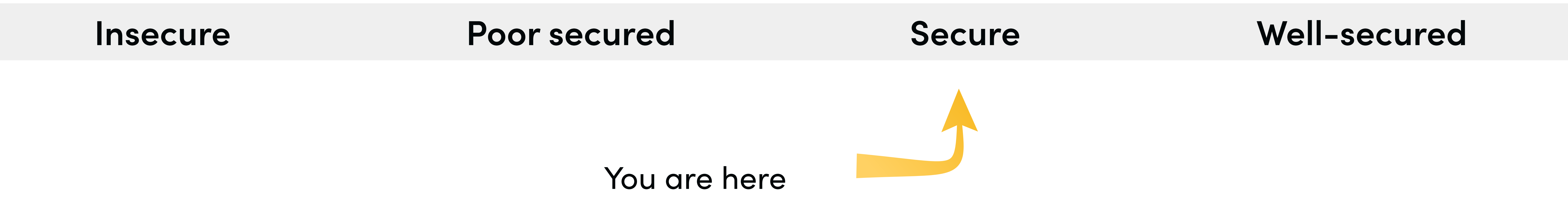
Contract Details

Token contract details for 19.12.2022

Token Type	: UTILITY
Contract name	: STAY
Contract address	: 0x127415D59E508c70A3990175C8267eb9C49b84fC
Total supply	: 100,000,000
Token ticker	: STAY
Decimals	: 18
Token Holders	: 329
Transactions count	: 5,865
Compiler version	: v0.8.6+commit.11564f7e
Contract deployer address	: 0x9e1b604766b7b55dc48196fa150f66ecc7598f87
Owner address	: 0x9e1b604766b7b55dc48196fa150f66ecc7598f87

Audit Summary


According to the standard audit assessment, Customer`s solidity smart contracts are “**Secure**”. This token contract does contain owner control, which do not make it fully decentralized.




We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 1 low.

STAY Token Distribution

 The top 100 holders collectively own 99.82% (99,820,844.15 Tokens) of STAY

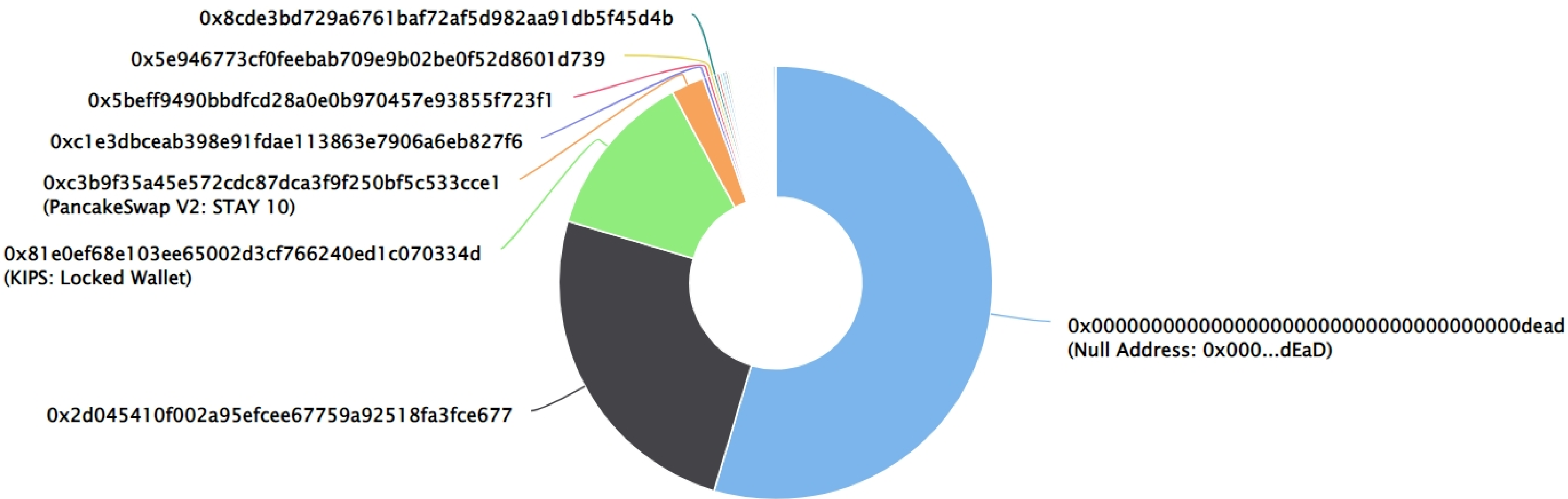
 Token Total Supply: 100,000,000.00 Token

|

Total Token Holders: 329




STAY Top 100 Token Holders

Source: BscScan.com



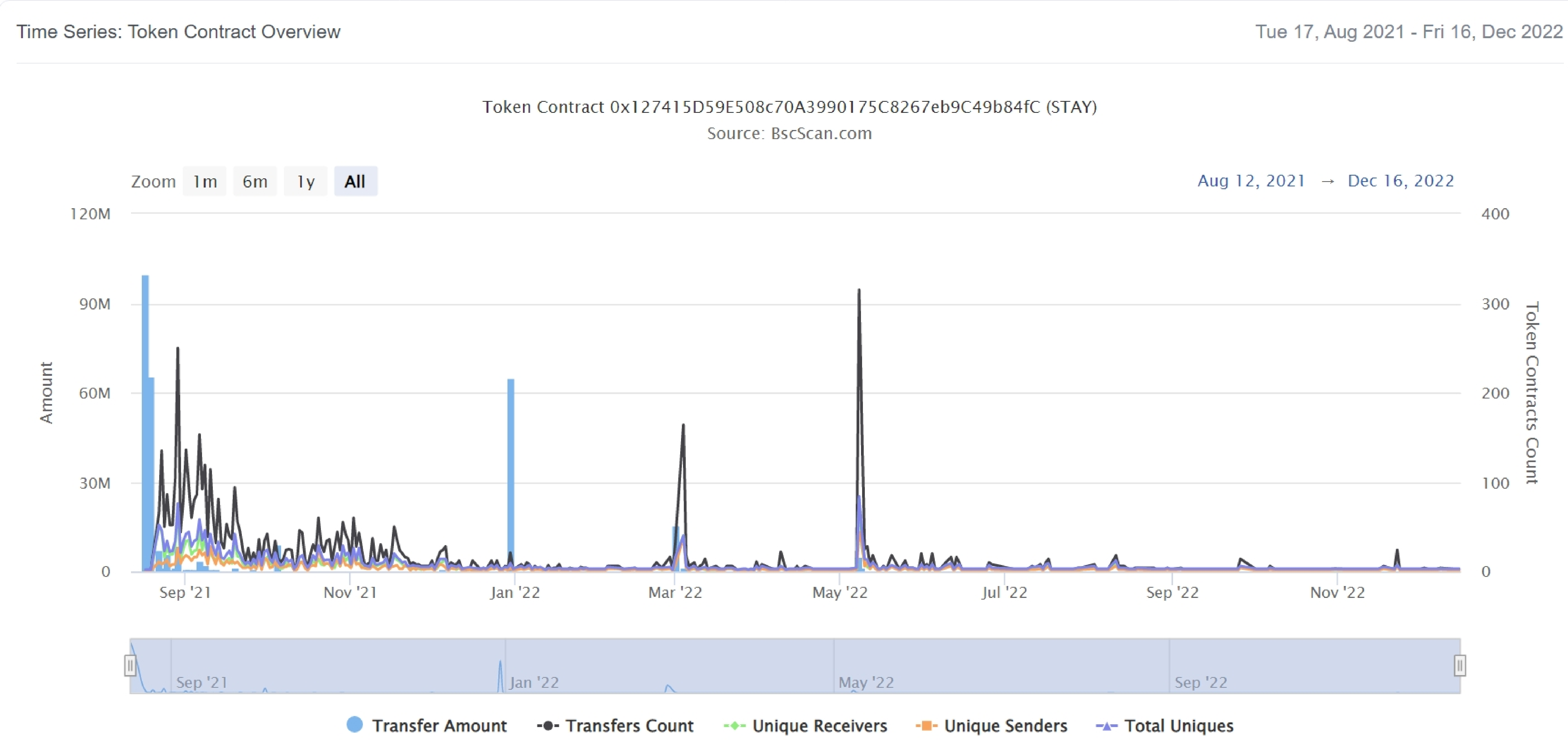
STAY Top 20 Token Holders

(A total of 99,820,844.15 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	54,600,000.018931855479408236	54.6000%
2	 0x2d045410f002a95efcee67759a92518fa3fce677	24,999,999.999999997	25.0000%
3	 KIPS: Locked Wallet	12,497,826.66756672515483976	12.4978%
4	 PancakeSwap V2: STAY 10	2,447,844.346404933220408696	2.4478%
5	0xc1e3dbceab398e91fdae113863e7906a6eb827f6	299,507.8	0.2995%
6	0x5beff9490bbdfcd28a0e0b970457e93855f723f1	274,450.853092392341867732	0.2745%
7	0x5e946773cf0feebab709e9b02be0f52d8601d739	245,682.127449235026	0.2457%
8	0x8cde3bd729a6761baf72af5d982aa91db5f45d4b	230,012.956736789451851722	0.2300%
9	0x8e2373f0f07fa80e69a335960ee186218ff31e66	229,908	0.2299%
10	0xda05e72f786684e5de155d9ee2340790be215316	209,237.924652853384274343	0.2092%
11	0xf2a7335e254b8d6fed9a59d9872d9ec281e2552f	195,942.36129893858318854	0.1959%
12	0x991bbb0099997f105138ca11a36bdc8a532d1852	176,450.641251009007078645	0.1765%
13	0x44f548a69d635bf7825542af8b4821a3f5c98a47	158,879.601404437510555205	0.1589%
14	0x06749e3f7a636e097ccc5d213485ec4757bb9012	150,000	0.1500%
15	0xb7efa70c64869d77a1d0da73f464df6815bb9ced	149,136.531431339616939061	0.1491%
16	0xc3b107bcf143105d50d7fdc3088a1136cc5829f3	144,384.73682763042505658	0.1444%
17	0xfa2a8267e7b53bdd60eae502bccad689638443a1	135,100.134332146890339838	0.1351%
18	0x228cb0a899aed59e5a56ef5eea20d961576190b2	130,340	0.1303%
19	0xfa139403a0d3284f161ff6c30fea1af0004eda57	126,721.494991112581615157	0.1267%
20	0x1f9b018bf18481b18ebd8431f29c41c89578b26b	124,424.032540111246390035	0.1244%

STAY Token Distribution

STAY Contract Overview



Contract functions details

+STAY

- <constructor>
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] transferFrom #
- [Pub] approve #
- [Pub] allowance
- [Pub] setTaxAddress #
 - modifiers: isOwner
- [Pub] setTaxPercent #
 - modifiers: isOwner
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
 - modifiers: isOwner
- [Pub] includeInFee #
 - modifiers: isOwner

(\$) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

✔ Critical Severity Issues

No critical severity issue found.

✔ High Severity Issues

No high severity issue found.

✔ Medium Severity Issues

No medium severity issue found.

✔ Low Severity Issues

One low severity issue found.

1. Unlocked Compiler Version.

• Description

The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

• Recommendation

It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.8.6 the contract should contain the following line:

```
pragma solidity 0.8.6;
```

Centralization

Owner privileges :

- STAY Contract:
 - Owner can change tax addresses.
 - Owner can change tax percent.
 - Owner can exclude/include in fee.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would not create trouble, as smart contract ownership has been renounced. Following are admin functions:

- `setTaxAddress`
- `setTaxPercent`
- `excludeFromFee`
- `includeInFee`

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.