soken

SMART CONTRACT SECURITY AUDIT

Adshares

November, 2021

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 30.11.2021

Contract Name: **WrappedADS**

Deployed address Ethereum:
0xcfcEcFe2bD2FED07A9145222E8a7ad9Cf1Ccd22A

Deployed address Binance Smart Chain:
0xcfcEcFe2bD2FED07A9145222E8a7ad9Cf1Ccd22A

Total Supply: **526,416.435479**

Token Tracker: **ADS**

Decimals: **11**

Token holders: **6,212**

Transactions count: **43,204**

Top 100 holders dominance: **67.30%**

Audit Details

Project Name: **WrappedADS**

Language: **Solidity**

Compiler Version: **v0.5.17**

Blockchain: **BSC**

Social Profiles

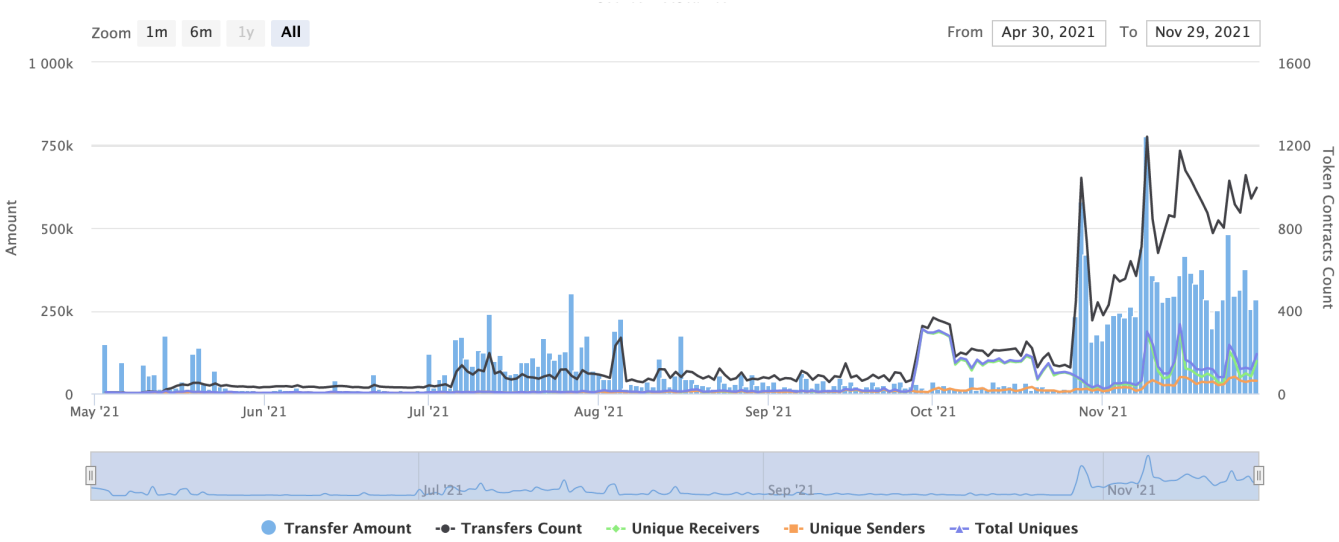
Project Website: **https://adshares.net**

Project Twitter: **https://twitter.com/adsharesNet**

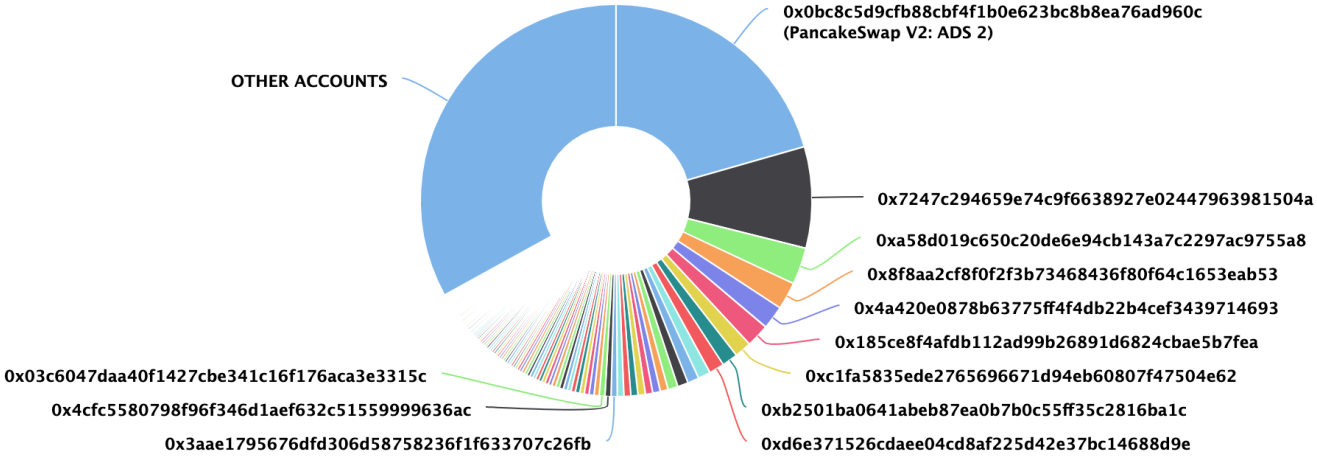
Project Telegram: **https://t.me/adshares**

Project blog: **https://blog.adshares.net**

Contract Analytics



ADS Token Distribution



ADS Top Holders

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: ADS 2	108,307.25708020342	20.5744%
2	0x7247c294659e74c9f6638927e02447963981504a	44,001.80518700637	8.3587%
3	0xa58d019c650c20de6e94cb143a7c2297ac9755a8	15,991.27223159287	3.0378%
4	0x8f8aa2cf8f0f2f3b73468436f80f64c1653eab53	11,899.35265933009	2.2604%
5	0x4a420e0878b63775ff4f4db22b4cef3439714693	10,240.9089728241	1.9454%
6	0x185ce8f4afdb112ad99b26891d6824cbae5b7fea	10,000	1.8996%
7	0xc1fa5835ede2765696671d94eb60807f47504e62	7,380.82666586559	1.4021%
8	0xb2501ba0641abeb87ea0b7b0c55ff35c2816ba1c	6,866.41810361501	1.3044%
9	0xd6e371526cdaee04cd8af225d42e37bc14688d9e	6,620.64250269265	1.2577%
10	0xce5279780024a996b8f2d5ffd27d15dac1d13317	5,443.20679684818	1.0340%

Swap Analysis

✔ Token is sellable (not a honeypot) at this time

Contract Analysis

✔ Verified contract source

✔ No prior similar token contracts

✔ Source does not contain a proxy contract

✔ Source does not contain a pausable contract

✔ Ownership renounced or source does not contain an owner contract.

Holder Analysis

✔ Owner/creator wallet contains less than 10% of token supply (< 0.01%)

✔ All other holders possess less than 10% of token supply

Contract Analysis

✔ Adequate liquidity present (730.65 BNB)

Contract Function Details

+ Context.sol
- [int] _msgSender
- [int] _msgData

+[lib] SafeMath
- [int] add
- [int] sub
- [int] sub
- [int] mul
- [int] div
- [int] div
- [int] mod
- [int] mod

+IERC20
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

+ERC20 is Context, IERC20
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer
- [Pub] allowance
- [Pub] approve
- [Pub] transferFrom
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [int] _transfer
- [int] _mint
- [int] _burn
- [int] _approve
- [int] _burnFrom

+ERC20Detailed is IERC20
- [Pub] name
- [Pub] symbol
- [Pub] decimals

+ PauserRole is Context
- [Pub] isPauser
- [Pub] addPauser
- [Pub] enouncePauser
- [int] _addPauser
- [int] _removePauser

+ ERC20Pausable is ERC20, Pausable
- [Pub] paused
- [Pub] pause
- [Pub] unpause
- [Pub] transfer
- [Pub] transferFrom
- [Pub] approve
- [Pub] increaseAllowance
- [Pub] decreaseAllowance

+[lib] Address
- [int] isContract
- [int] toPayable
- [int] sendValue

+SafeERC20
- [int] safeTransfer
- [int] safeTransferFrom
- [int] safeApprove
- [int] safeIncreaseAllowance
- [int] safeDecreaseAllowance

+[lib] Roles
- [int] add
- [int] remove
- [int] has

+ MinterRole is Context
- [Pub] isMinter
- [Pub] addMinter
- [Pub] renounceMinter
- [int] _addMinter
- [int] _removeMinter

+ OwnerRole is Context
- [Pub] isOwner
- [Pub] addOwner
- [Pub] renounceOwner

- [int] _addOwner
- [int] _removeOwner

+ WrappedADS is ERC20, ERC20Detailed, ERC20Pausable, OwnerRole, MinterRole
- [Pub] wrapTo
- [Pub] unwrap
- [Pub] unwrapMessage
- [int] _unwrap
- [Pub] unwrapFrom
- [Pub] minterAllowance
- [Pub] minterApprove
- [Pub] increaseMinterAllowance
- [Pub] decreaseMinterAllowance
- [int] _minterApprove
- [Pub] isMinter
- [Pub] removeMinter
- [Pub] isPauser
- [Pub] removePauser
- [Ext] reclaimEther
- [Ext] reclaimToken
- [int] _checksumCheck

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Conclusion

Smart contracts are free from any low, medium or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team