



Cyberscope

# Audit Report

## **Santa Doge**

December 2022

Type           BEP20

Network       BSC

Address       0x38fD790c5F0dE8a83F8bABB78F3B7b034250e2c4

Audited by   © cyberscope

# Table of Contents

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Table of Contents</b>                                | <b>1</b>  |
| <b>Contract Review</b>                                  | <b>3</b>  |
| <b>Source Files</b>                                     | <b>3</b>  |
| <b>Audit Updates</b>                                    | <b>3</b>  |
| <b>Contract Analysis</b>                                | <b>4</b>  |
| <b>L04 - Conformance to Solidity Naming Conventions</b> | <b>6</b>  |
| Description                                             | 6         |
| Recommendation                                          | 6         |
| <b>L09 - Dead Code Elimination</b>                      | <b>7</b>  |
| Description                                             | 7         |
| Recommendation                                          | 7         |
| <b>L11 - Unnecessary Boolean equality</b>               | <b>8</b>  |
| Description                                             | 8         |
| Recommendation                                          | 8         |
| <b>L15 - Local Scope Variable Shadowing</b>             | <b>9</b>  |
| Description                                             | 9         |
| Recommendation                                          | 9         |
| <b>Contract Diagnostics</b>                             | <b>10</b> |
| <b>Contract Functions</b>                               | <b>11</b> |
| <b>Contract Flow</b>                                    | <b>15</b> |
| <b>Domain Info</b>                                      | <b>16</b> |
| <b>Summary</b>                                          | <b>17</b> |
| <b>Disclaimer</b>                                       | <b>18</b> |
| <b>About Cyberscope</b>                                 | <b>19</b> |



## Contract Review

|                         |                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Contract Name</b>    | SantaDoge                                                                                                                                               |
| <b>Compiler Version</b> | v0.8.7+commit.e28d00a7                                                                                                                                  |
| <b>Optimization</b>     | 200 runs                                                                                                                                                |
| <b>Licence</b>          | None                                                                                                                                                    |
| <b>Explorer</b>         | <a href="https://bscscan.com/token/0x38fD790c5F0dE8a83F8bABB78F3B7b034250e2c4">https://bscscan.com/token/0x38fD790c5F0dE8a83F8bABB78F3B7b034250e2c4</a> |
| <b>Symbol</b>           | STDOGE                                                                                                                                                  |
| <b>Decimals</b>         | 18                                                                                                                                                      |
| <b>Total Supply</b>     | 100,000,000                                                                                                                                             |
| <b>Domain</b>           | santadoge.cash                                                                                                                                          |

## Source Files

|                     |                                                                  |
|---------------------|------------------------------------------------------------------|
| <b>Filename</b>     | <b>SHA256</b>                                                    |
| <b>contract.sol</b> | b763d50c9650a58fd1babeb30e2b391fc2777b634c38e2f273651ecef4660814 |

## Audit Updates

|                      |                   |
|----------------------|-------------------|
| <b>Initial Audit</b> | 7th December 2022 |
| <b>Corrected</b>     |                   |

# Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

| Severity | Code | Description                        | Status |
|----------|------|------------------------------------|--------|
| ●        | ST   | Stops Transactions                 | Passed |
| ●        | OCTD | Transfers Contract's Tokens        | Passed |
| ●        | OTUT | Transfers User's Tokens            | Passed |
| ●        | ELFM | Exceeds Fees Limit                 | Passed |
| ●        | ULTW | Transfers Liquidity to Team Wallet | Passed |
| ●        | MT   | Mints Tokens                       | Passed |
| ●        | BT   | Burns Tokens                       | Passed |
| ●        | BC   | Blacklists Addresses               | Passed |

| Severity | Code | Description                                | Status     |
|----------|------|--------------------------------------------|------------|
| ●        | L04  | Conformance to Solidity Naming Conventions | Unresolved |
| ●        | L09  | Dead Code Elimination                      | Unresolved |
| ●        | L11  | Unnecessary Boolean equality               | Unresolved |
| ●        | L15  | Local Scope Variable Shadowing             | Unresolved |

## L04 - Conformance to Solidity Naming Conventions

|                    |                                      |
|--------------------|--------------------------------------|
| <b>Criticality</b> | minor / informative                  |
| <b>Location</b>    | contract.sol#L1143,1142,31,1141,1138 |
| <b>Status</b>      | Unresolved                           |

### Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow \_ at the beginning of the mixed\_case match for private variables and unused parameters.

```
marketingAddress  
marketingBuyFee  
WETH  
marketingSellFee  
maxSupply
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions>.

## L09 - Dead Code Elimination

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Criticality</b> | minor / informative                                                 |
| <b>Location</b>    | contract.sol#L470,329,1124,383,453,443,1085,397,416,305,364,426,354 |
| <b>Status</b>      | Unresolved                                                          |

### Description

Functions that are not used in the contract, and make the code's size bigger.

```
verifyCallResult  
sendValue  
_burnFrom  
functionCallWithValue  
functionDelegateCall  
_burn  
functionStaticCall  
isContract  
functionCall  
...
```

### Recommendation

Remove unused functions.

## L11 - Unnecessary Boolean equality

|                    |                     |
|--------------------|---------------------|
| <b>Criticality</b> | minor / informative |
| <b>Location</b>    | contract.sol#L1161  |
| <b>Status</b>      | Unresolved          |

### Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
taxStatus == true
```

### Recommendation

Remove the equality to the boolean constant.

## L15 - Local Scope Variable Shadowing

|                    |                        |
|--------------------|------------------------|
| <b>Criticality</b> | minor / informative    |
| <b>Location</b>    | contract.sol#L1147,882 |
| <b>Status</b>      | Unresolved             |

### Description

There are variables that are defined in the local scope containing the same name from an upper scope.

```
_symbol  
name  
symbol  
_name
```

### Recommendation

The local variables should have different names from the upper scoped variables.

# Contract Diagnostics

● Critical   ● Medium   ● Minor / Informative

# Contract Functions

| Contract                  | Type                         | Bases      |            |           |
|---------------------------|------------------------------|------------|------------|-----------|
|                           | Function Name                | Visibility | Mutability | Modifiers |
|                           |                              |            |            |           |
| <b>IUniswapV2Factory</b>  | Interface                    |            |            |           |
|                           | feeTo                        | External   |            | -         |
|                           | feeToSetter                  | External   |            | -         |
|                           | getPair                      | External   |            | -         |
|                           | allPairs                     | External   |            | -         |
|                           | allPairsLength               | External   |            | -         |
|                           | createPair                   | External   | ✓          | -         |
|                           | setFeeTo                     | External   | ✓          | -         |
|                           | setFeeToSetter               | External   | ✓          | -         |
|                           |                              |            |            |           |
| <b>IUniswapV2Router01</b> | Interface                    |            |            |           |
|                           | factory                      | External   |            | -         |
|                           | WETH                         | External   |            | -         |
|                           | addLiquidity                 | External   | ✓          | -         |
|                           | addLiquidityETH              | External   | Payable    | -         |
|                           | removeLiquidity              | External   | ✓          | -         |
|                           | removeLiquidityETH           | External   | ✓          | -         |
|                           | removeLiquidityWithPermit    | External   | ✓          | -         |
|                           | removeLiquidityETHWithPermit | External   | ✓          | -         |
|                           | swapExactTokensForTokens     | External   | ✓          | -         |
|                           | swapTokensForExactTokens     | External   | ✓          | -         |
|                           | swapExactETHForTokens        | External   | Payable    | -         |
|                           | swapTokensForExactETH        | External   | ✓          | -         |
|                           | swapExactTokensForETH        | External   | ✓          | -         |
|                           | swapETHForExactTokens        | External   | Payable    | -         |
|                           | quote                        | External   |            | -         |
|                           | getAmountOut                 | External   |            | -         |

|                           |                                                           |                    |         |   |
|---------------------------|-----------------------------------------------------------|--------------------|---------|---|
|                           | getAmountIn                                               | External           |         | - |
|                           | getAmountsOut                                             | External           |         | - |
|                           | getAmountsIn                                              | External           |         | - |
|                           |                                                           |                    |         |   |
| <b>IUniswapV2Router02</b> | Interface                                                 | IUniswapV2Router01 |         |   |
|                           | removeLiquidityETHSupportingFeeOnTransferTokens           | External           | ✓       | - |
|                           | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External           | ✓       | - |
|                           | swapExactTokensForTokensSupportingFeeOnTransferTokens     | External           | ✓       | - |
|                           | swapExactETHForTokensSupportingFeeOnTransferTokens        | External           | Payable | - |
|                           | swapExactTokensForETHSupportingFeeOnTransferTokens        | External           | ✓       | - |
|                           |                                                           |                    |         |   |
| <b>IERC20</b>             | Interface                                                 |                    |         |   |
|                           | totalSupply                                               | External           |         | - |
|                           | decimals                                                  | External           |         | - |
|                           | symbol                                                    | External           |         | - |
|                           | name                                                      | External           |         | - |
|                           | getOwner                                                  | External           |         | - |
|                           | balanceOf                                                 | External           |         | - |
|                           | transfer                                                  | External           | ✓       | - |
|                           | allowance                                                 | External           |         | - |
|                           | approve                                                   | External           | ✓       | - |
|                           | transferFrom                                              | External           | ✓       | - |
|                           |                                                           |                    |         |   |
| <b>Address</b>            | Library                                                   |                    |         |   |
|                           | isContract                                                | Internal           |         |   |
|                           | sendValue                                                 | Internal           | ✓       |   |
|                           | functionCall                                              | Internal           | ✓       |   |
|                           | functionCall                                              | Internal           | ✓       |   |
|                           | functionCallWithValue                                     | Internal           | ✓       |   |
|                           | functionCallWithValue                                     | Internal           | ✓       |   |
|                           | functionStaticCall                                        | Internal           |         |   |

|                 |                      |                                |   |           |
|-----------------|----------------------|--------------------------------|---|-----------|
|                 | functionStaticCall   | Internal                       |   |           |
|                 | functionDelegateCall | Internal                       | ✓ |           |
|                 | functionDelegateCall | Internal                       | ✓ |           |
|                 | verifyCallResult     | Internal                       |   |           |
|                 |                      |                                |   |           |
| <b>SafeMath</b> | Library              |                                |   |           |
|                 | tryAdd               | Internal                       |   |           |
|                 | trySub               | Internal                       |   |           |
|                 | tryMul               | Internal                       |   |           |
|                 | tryDiv               | Internal                       |   |           |
|                 | tryMod               | Internal                       |   |           |
|                 | add                  | Internal                       |   |           |
|                 | sub                  | Internal                       |   |           |
|                 | mul                  | Internal                       |   |           |
|                 | div                  | Internal                       |   |           |
|                 | mod                  | Internal                       |   |           |
|                 | sub                  | Internal                       |   |           |
|                 | div                  | Internal                       |   |           |
|                 | mod                  | Internal                       |   |           |
|                 |                      |                                |   |           |
| <b>Context</b>  | Implementation       |                                |   |           |
|                 | _msgSender           | Internal                       |   |           |
|                 | _msgData             | Internal                       |   |           |
|                 |                      |                                |   |           |
| <b>Ownable</b>  | Implementation       | Context                        |   |           |
|                 | <Constructor>        | Public                         | ✓ | -         |
|                 | owner                | Public                         |   | -         |
|                 | renounceOwnership    | Public                         | ✓ | onlyOwner |
|                 | transferOwnership    | Public                         | ✓ | onlyOwner |
|                 | _transferOwnership   | Internal                       | ✓ |           |
|                 |                      |                                |   |           |
| <b>ERC20</b>    | Implementation       | Context,<br>IERC20,<br>Ownable |   |           |
|                 | <Constructor>        | Public                         | ✓ | -         |
|                 | getOwner             | External                       |   | -         |

|                  |                   |          |   |           |
|------------------|-------------------|----------|---|-----------|
|                  | name              | External |   | -         |
|                  | decimals          | External |   | -         |
|                  | symbol            | External |   | -         |
|                  | totalSupply       | External |   | -         |
|                  | balanceOf         | External |   | -         |
|                  | transfer          | External | ✓ | -         |
|                  | allowance         | External |   | -         |
|                  | approve           | External | ✓ | -         |
|                  | transferFrom      | External | ✓ | -         |
|                  | increaseAllowance | External | ✓ | -         |
|                  | decreaseAllowance | External | ✓ | -         |
|                  | _transfer         | Internal | ✓ |           |
|                  | _mint             | Internal | ✓ |           |
|                  | _burn             | Internal | ✓ |           |
|                  | _approve          | Internal | ✓ |           |
|                  | _burnFrom         | Internal | ✓ |           |
|                  |                   |          |   |           |
| <b>SantaDoge</b> | Implementation    | ERC20    |   |           |
|                  | <Constructor>     | Public   | ✓ | ERC20     |
|                  | setTax            | External | ✓ | onlyOwner |
|                  | addExcludeFee     | External | ✓ | onlyOwner |
|                  | _transfer         | Internal | ✓ |           |

# Contract Flow



## Domain Info

|                               |                                                                     |
|-------------------------------|---------------------------------------------------------------------|
| <b>Domain Name</b>            | santadoge.cash                                                      |
| <b>Registry Domain ID</b>     | 313b4ed0f02a482cbc7aaafe1359b208-DONUTS                             |
| <b>Creation Date</b>          | 2022-12-03T16:32:03Z                                                |
| <b>Updated Date</b>           | 2022-12-04T14:02:44Z                                                |
| <b>Registry Expiry Date</b>   | 2023-12-03T16:32:03Z                                                |
| <b>Registrar WHOIS Server</b> | whois.namecheap.com                                                 |
| <b>Registrar URL</b>          | <a href="https://www.namecheap.com/">https://www.namecheap.com/</a> |
| <b>Registrar</b>              | NameCheap, Inc.                                                     |
| <b>Registrar IANA ID</b>      | 1068                                                                |

The domain was created 4 days before the creation of the audit. It will expire in 12 months.

There is no public billing information, the creator is protected by the privacy settings.

## Summary

Santa Doge is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 4% buy/sell fees.

## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/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 and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

## About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



The Cyberscope team

<https://www.cyberscope.io>