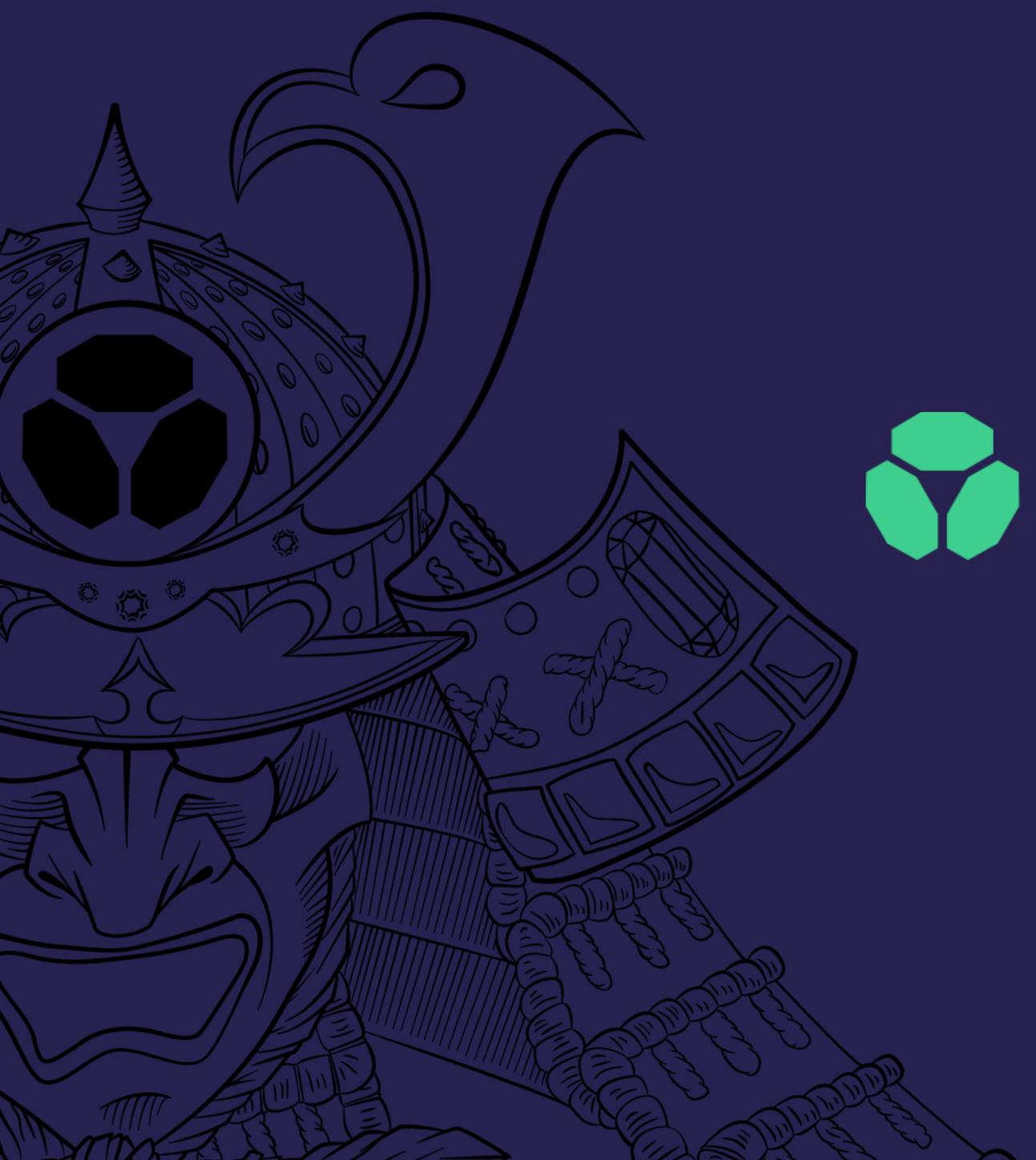


smart state

> Smart
Contract
Audit #

OpenDAO

May 15
2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

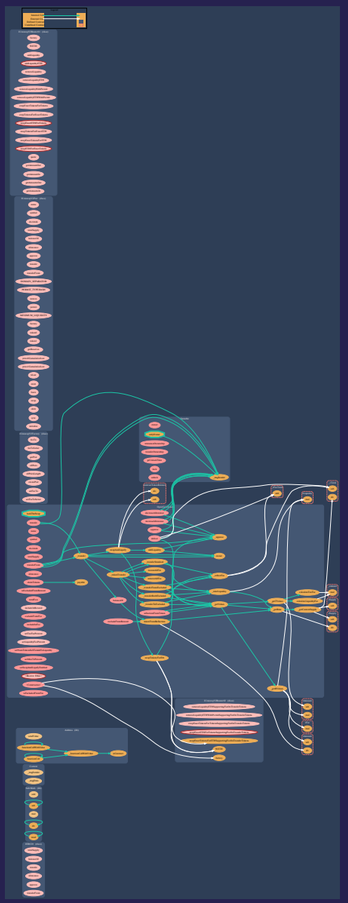
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked call return method
- Code with no effects
- Pool Asset Security (backdoors in the underlying ERC-20)
- Function visibility
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Over/Under Flows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/ Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

STRUCTURE OF CONTRACT

1.2._OPENCOIN.SOL

CONTRACT METHODS ANALYSIS:

- name()
  Vulnerabilities not detected
- symbol()
  Vulnerabilities not detected
- decimals()
  Vulnerabilities not detected



Pic. 1.1
1.2._OpenCoin.sol

- totalSupply()
  Vulnerabilities not detected
- balanceOf(address account)
  Vulnerabilities not detected
- transfer(address recipient, uint256 amount)
  Vulnerabilities not detected
- allowance(address owner, address spender)
  Vulnerabilities not detected
- approve(address spender, uint256 amount)
  Vulnerabilities not detected
- transferFrom(address sender, address recipient, uint256 amount)
  Vulnerabilities not detected
- increaseAllowance(address spender, uint256 addedValue)
  Vulnerabilities not detected
- decreaseAllowance(address spender, uint256 subtractedValue)
  Vulnerabilities not detected
- isExcludedFromReward(address account)
  Vulnerabilities not detected
- totalFees()
  Vulnerabilities not detected
- deliver(uint256 tAmount)
  Vulnerabilities not detected

- reflectionFromToken(uint256 tAmount, bool deductTransferFee)
  Vulnerabilities not detected
- tokenFromReflection(uint256 rAmount)
  Vulnerabilities not detected
- excludeFromReward(address account)
  Vulnerabilities not detected
- includeInReward(address account)
  Vulnerabilities not detected
- _transferBothExcluded(address sender, address recipient, uint256 tAmount)
  Vulnerabilities not detected
- excludeFromFee(address account)
  Vulnerabilities not detected
- includeInFee(address account)
  Vulnerabilities not detected
- setTaxFeePercent(uint256 taxFee)
  Vulnerabilities not detected

- setLiquidityFeePercent(uint256 liquidityFee)
  Vulnerabilities not detected

- setNumTokensSellToAddToLiquidity (uint256 swapNumber)
  Vulnerabilities not detected

- setMaxTxPercent(uint256 maxTxPercent)
  Vulnerabilities not detected

- setSwapAndLiquifyEnabled(bool _enabled)
  Vulnerabilities not detected

- _reflectFee(uint256 rFee, uint256 tFee)
  Vulnerabilities not detected

- _getValues(uint256 tAmount)
  Vulnerabilities not detected

- _getTValues(uint256 tAmount)
  Vulnerabilities not detected

- _getRValues(uint256 tAmount, uint256 tFee, uint256 tLiquidity, uint256 currentRate)
  Vulnerabilities not detected

- _getRate()
  Vulnerabilities not detected
- _getCurrentSupply()
  Vulnerabilities not detected
- _takeLiquidity(uint256 tLiquidity)
  Vulnerabilities not detected
- claimTokens()
  Vulnerabilities not detected
- _takeLiquidity(uint256 tLiquidity)
  Vulnerabilities not detected
- calculateTaxFee(uint256 _amount)
  Vulnerabilities not detected
- calculateLiquidityFee(uint256 _amount)
  Vulnerabilities not detected
- removeAllFee()
  Vulnerabilities not detected
- restoreAllFee()
  Vulnerabilities not detected
- isExcludedFromFee(address account)
  Vulnerabilities not detected

- _approve(address owner, address spender, uint256 amount)
  Vulnerabilities not detected
- _transfer(address from,address to,uint256 amount)
  Vulnerabilities not detected
- swapAndLiquify(uint256 contractTokenBalance)
  Vulnerabilities not detected
- swapTokensForEth(uint256 tokenAmount)
  Vulnerabilities not detected
- addLiquidity(uint256 tokenAmount, uint256 ethAmount)
  Vulnerabilities not detected
- _tokenTransfer(address sender, address recipient, uint256 amount,bool takeFee)
  Vulnerabilities not detected
- _transferStandard(address sender, address recipient, uint256 tAmount)
  Vulnerabilities not detected
- _transferToExcluded(address sender, address recipient, uint256 tAmount)
  Vulnerabilities not detected
- _transferFromExcluded(address sender, address recipient, uint256 tAmount)
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
1.2._OpenCoin.sol	0.6.12	200	bd5de4c1bc6d7b0ba511ee5b4f7ebb57f7d2c1b54178e86275bbfa77b28485bd

Get In Touch

info@smartstate.tech

smartstate.tech