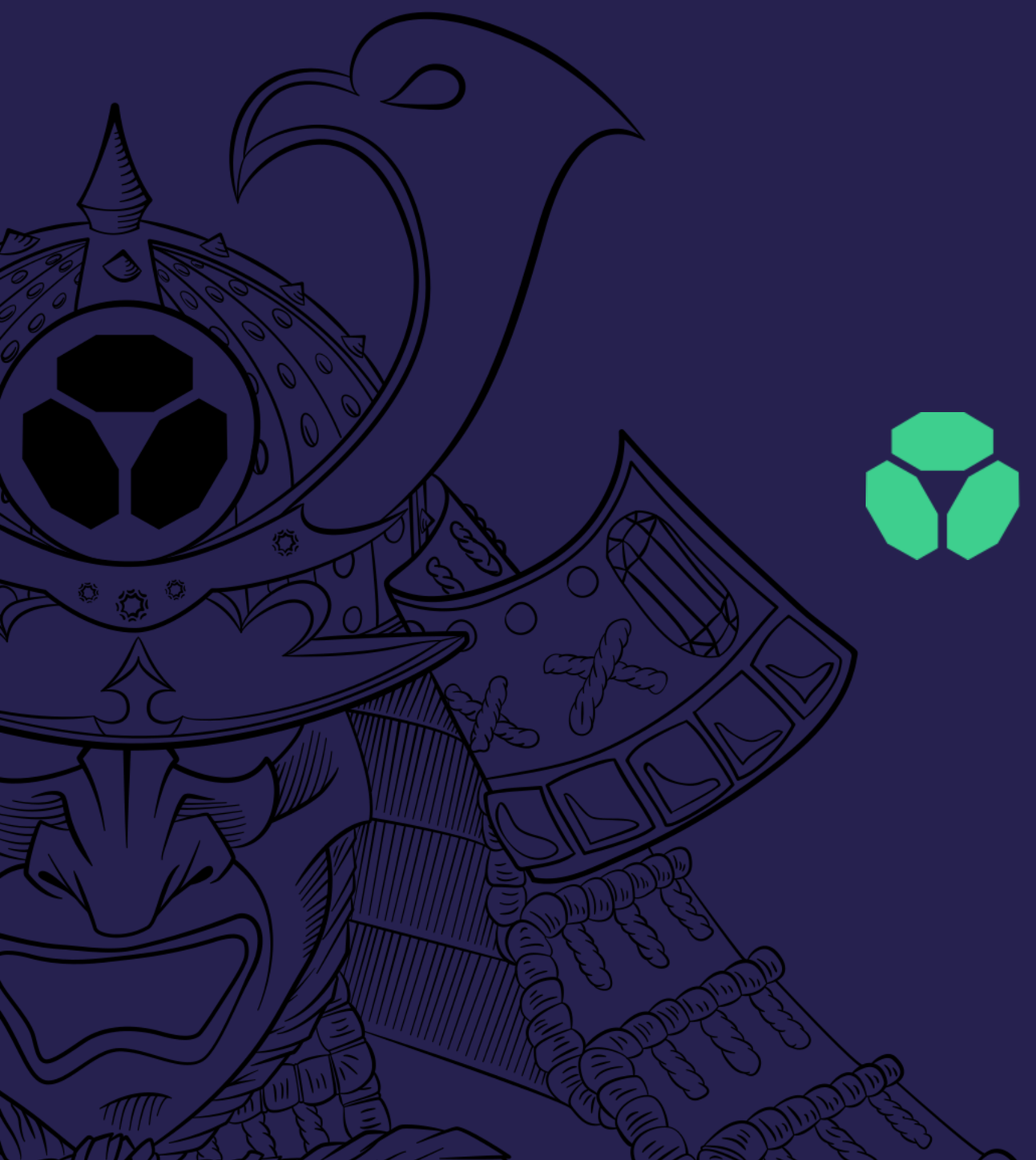


smart state

> Smart
Contract
Audit #

DAO Maker

Mar 13
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
- Unsed vars
- Uncheked 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

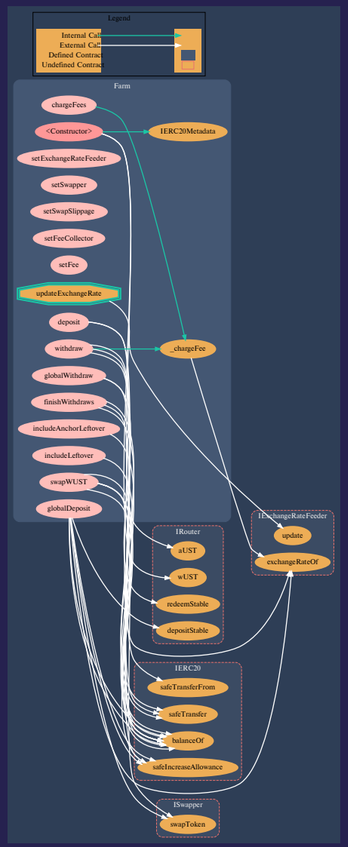
FARM.SOL

CONTRACT METHODS ANALYSIS:

- setExchangeRateFeeder(IExchangeRateFeeder newFeeder)
  Function should emit an event. Function lacks for 0 address check.

- setSwapper(ISwapper newSwapper)
  Function should emit an event. Function lacks for 0 address check.

- setSwapSlippage(uint24 newSwapSlippage)
  Function should emit an event.



Pic. 1.1
Farm.sol

- setFeeCollector(address newFeeCollector)
  Function should emit an event. Function lacks for 0 address check.

- setFee(uint24 newFeePercentage)
  Function should emit an event.

PAYABLE

- deposit(uint128 amount)
  Vulnerabilities not detected

Tokens in, public

- globalDeposit(uint128 amount)
  Vulnerabilities not detected

PAYABLE

- withdraw(uint128 requestedAmount)
  Vulnerabilities not detected

Tokens out, public

- globalWithdraw(uint128 shares)
  We recommend not to set minAmountOut to 0 when performing swap in order not to catch any extra reverts due to frontrunning attacks

PAYABLE

- finishWithdraws(address[] calldata userAddresses, bool wUSTWithdraw)
  Vulnerabilities not detected

Tokens out, public

- includeLeftover()
  Vulnerabilties not detected

- includeAnchorLeftover()
  Vulnerabilties not detected

- swapWUST()
  We recommend not to set minAmountOut to 0 when performing swap in order not to catch any extra reverts due to frontrunning attacks

- chargeFees(address[] calldata userAddresses)
  Vulnerabilties not detected

- _chargeFee(address userAddress)
  Vulnerabilties not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
Farm	0.8.4	200	7e0294d4f831c0bf431a91efb701b45ce1eaf54287d047cd5c39b3019a7c3db9

Get In Touch

info@smartstate.tech

smartstate.tech