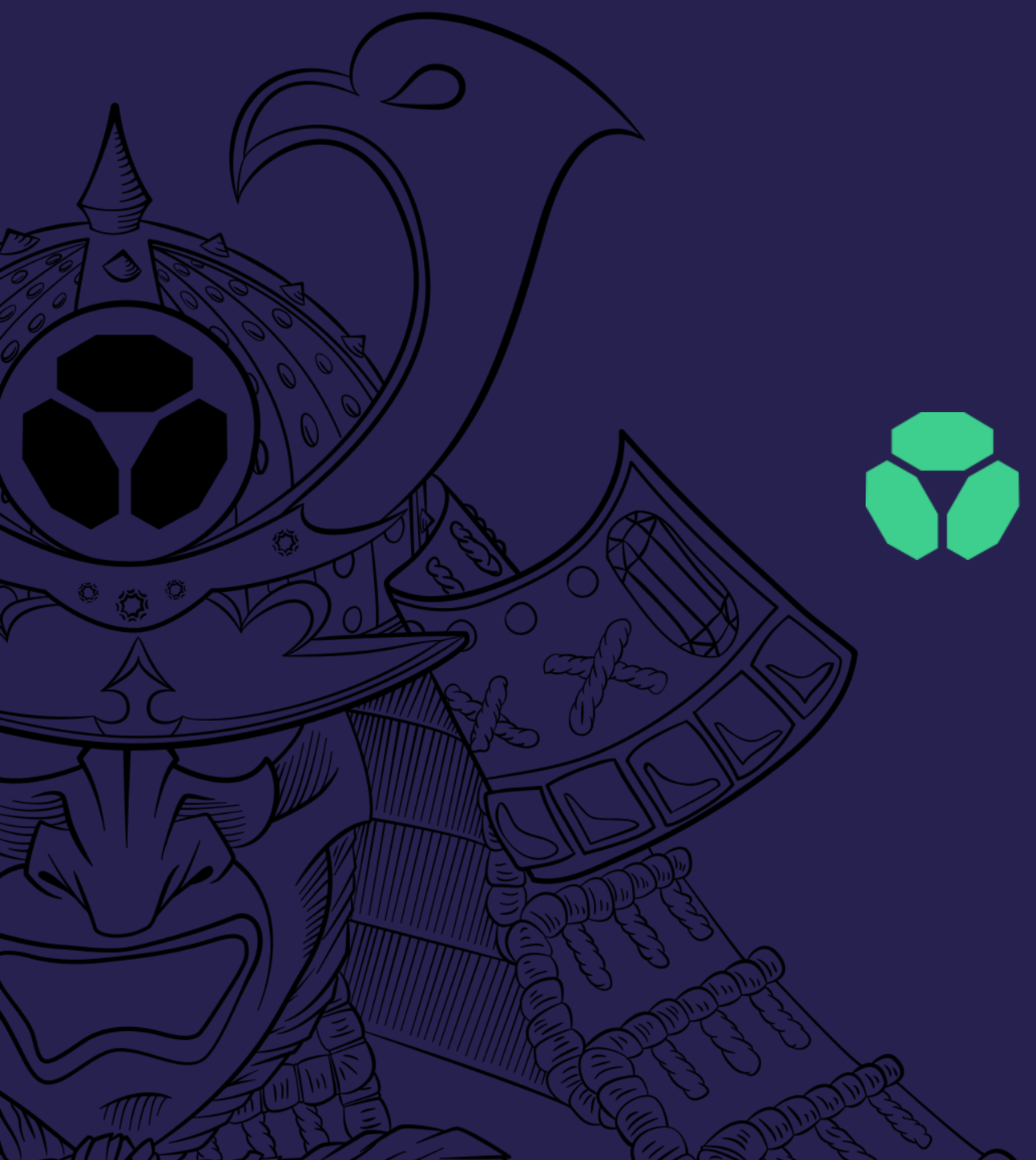


smart state

> Smart
Contract
Audit #

Jun 01
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

VESTING.SOL

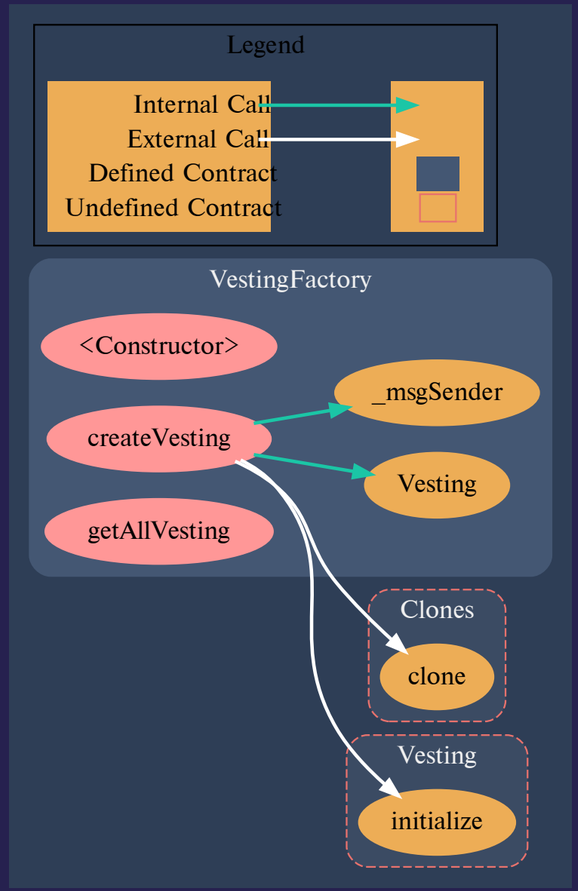
CONTRACT METHODS ANALYSIS:

- initialize(
  address _owner,
  address _tokenAddress
)

  Vulnerabilities not detected

- createStep(
  Type _stepType,
  uint256 _percent,
  uint256 _frequency,
  uint256 _time
)

  Vulnerabilities not detected



Pic. 1.1
Vesting.sol

TOKEN FLOW

- addDepositor(address _depositor, uint256 _amount, uint256 _startTime)
  Vulnerabilities not detected

Tokens in, public

TOKEN FLOW

- unlock(uint256 _vestingId)
  Vulnerabilities not detected

Tokens out, public

- calculateReward(
  address _user,
  uint256 _vestingId,
  uint256 _frequency,
  uint256 _paymentCount,
  uint256 _stepCount
)
  Vulnerabilities not detected

- calculateAmount(uint256 _depositorAmount, uint256 _percent)
  Vulnerabilities not detected

TOKEN FLOW

- claim(uint256 _vestingId)
  Function ignores transfer return value. Recommended to use safeTransfer instead

Tokens out, public

- getStep(uint256 _vestingId)
  Vulnerabilities not detected

- calculatePercent()
  Vulnerabilities not detected

- getStrategy()
  Vulnerabilities not detected

- getAllDepositor()
  Vulnerabilities not detected

- getDepositor(uint256 _vestingId)
  Vulnerabilities not detected

- getUsersVesting()
  Vulnerabilities not detected

- getTime()
  Vulnerabilities not detected

- isOwner(uint256 _vestingId)
  Vulnerabilities not detected

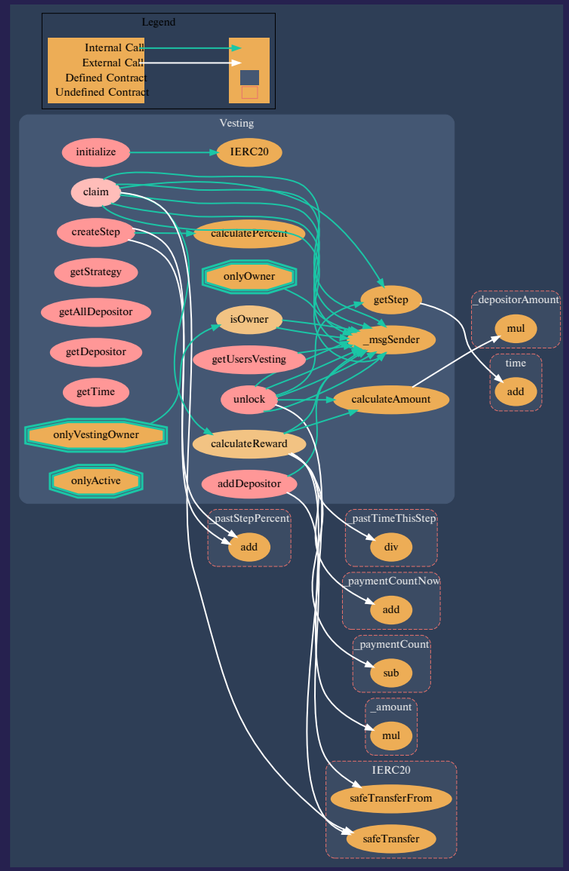
STRUCTURE OF CONTRACT

VESTINGFACTORY.SOL

CONTRACT METHODS ANALYSIS:

- createVesting(address _tokenAddress)
  Vulnerabilities not detected

- getAllVesting()
  Vulnerabilities not detected



Pic. 1.2
VestingFactory.sol

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
Vesting.sol	c0b999b6d6da134a5af120f7b5fc21d8f9e41eaf3d0ad54fbf35b1dae87d8d20
VestingFactory.sol	07b1c9a3ff0436e8ea402183008f435652b0dd3b9dd708592cd16c44bb5d8f2b

Get In Touch

info@smartstate.tech

smartstate.tech