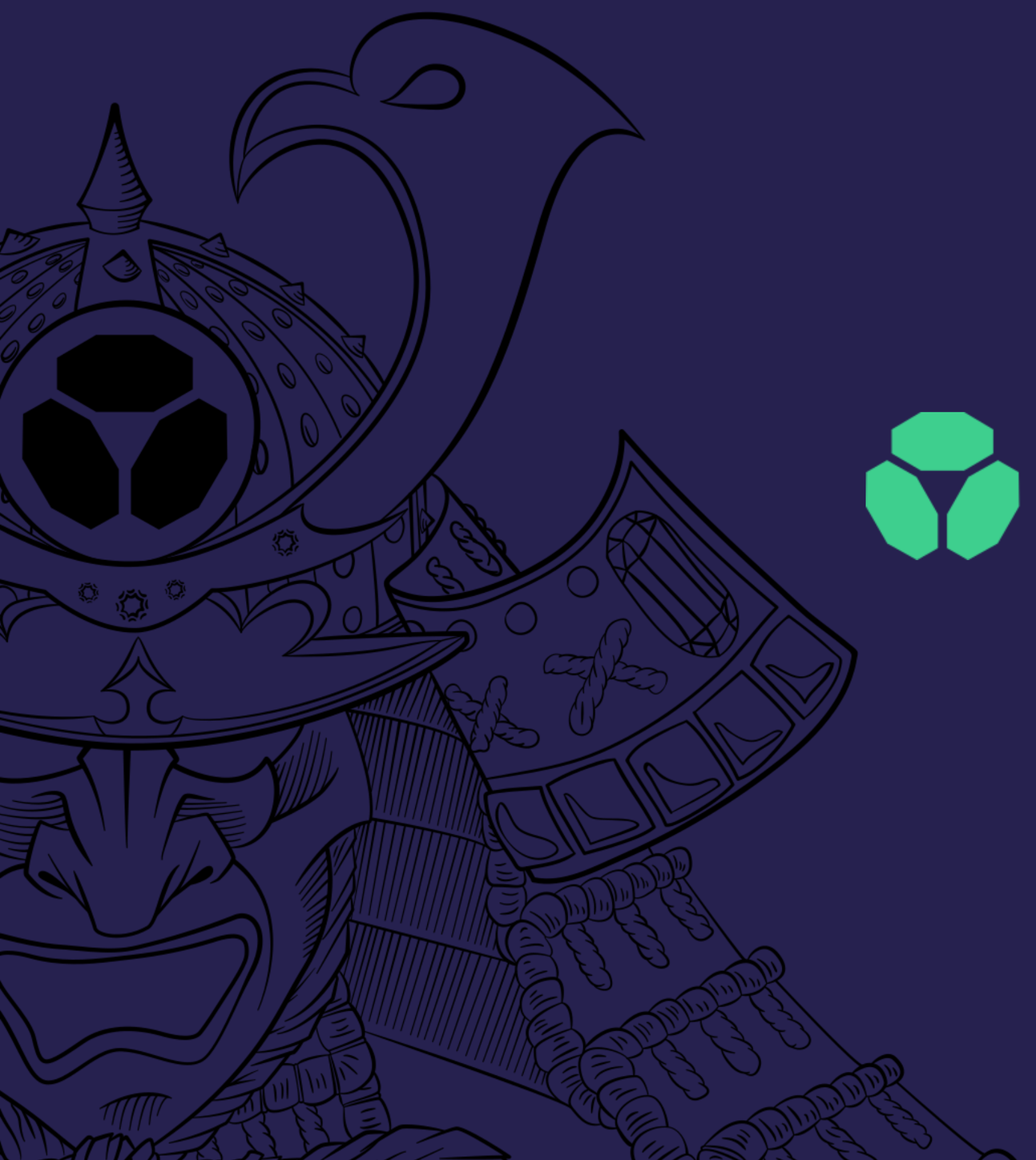


smart state

> Smart
Contract
Audit #

# Finnovant

Mar 08
2021

# TABLE OF CONTENTS

# METHODOLOGY

## MAIN TESTS LIST:

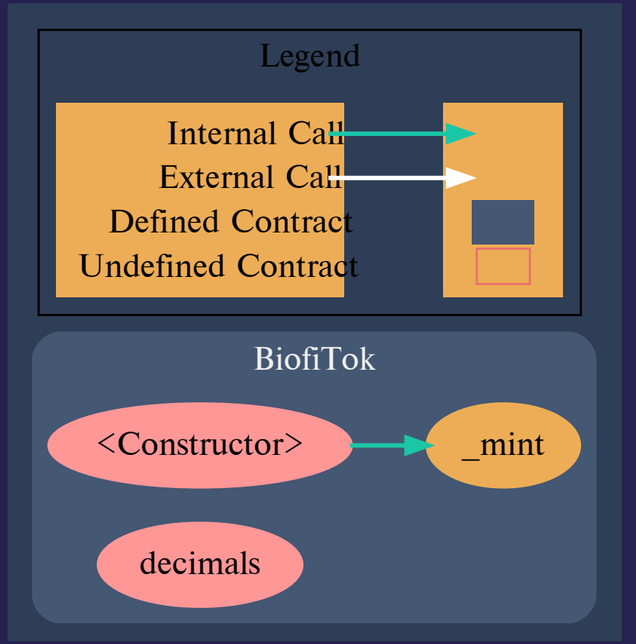
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unsed vars
- Uncheked call return method
- Code with no effects
- Pool Asset Security (backdoors in the 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

## BIOFI_TOK.SOL

### CONTRACT METHODS ANALYSIS:

- decimals()
  Vulnerabilities not detected




Pic. 1.1
biofi_tok.sol

# STRUCTURE OF CONTRACT

## BIOFINFTTEST.SOL

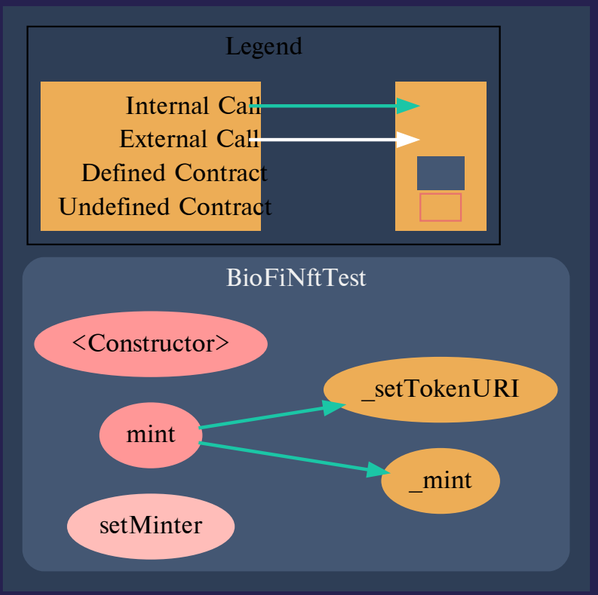
### CHECK SUMMARY:

Vulnerabilities not detected

### CONTRACT METHODS ANALYSIS:

- mint(address _to, string calldata _uri)
  Vulnerabilities not detected

- setMinter(address newMinter)
  Function should emit an event.
  Recommended to use onlyOwner modifier




Pic. 1.2
BiofiNftTest.sol

# STRUCTURE OF CONTRACT

## BIOFI_STAKE.SOL

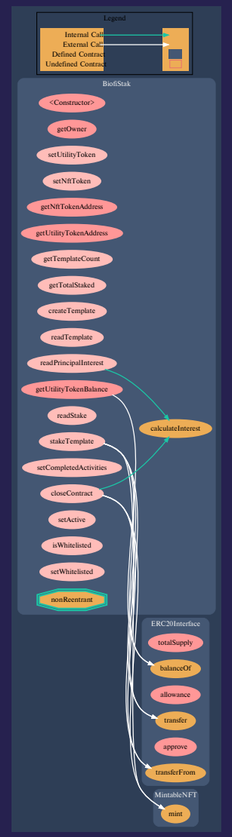
### CONTRACT METHODS ANALYSIS:

- getOwner()
  Vulnerabilities not detected

- setUtilityToken(address token)
  Function should emit an event.
  Recommended to use onlyOwner modifier

- setNftToken(address token)
  Function should emit an event.
  Recommended to use onlyOwner modifier

- getNftTokenAddress()
  Vulnerabilities not detected




Pic. 1.3
biofi_stake.sol

- getUtilityTokenAddress()
  Vulnerabilities not detected

- getTemplateCount()
  Vulnerabilities not detected

- getTotalStaked(uint256 stakeIndex)
  Vulnerabilities not detected

- createTemplate(
  string calldata name, Timebox calldata timebox,
  Fraction calldata requiredPenalty, Fraction calldata apr,
  InvestmentRange calldata utilityInvestmentRange,
  string [] calldata beginNfts, string [] calldata endNfts)
  Function should emit an event. Recommended to use onlyOwner modifier

- readTemplate(uint256 templateIndex)
  Vulnerabilities not detected

**PAYABLE**

- stakeTemplate(uint256 stakeIndex, uint256 utilityTokenAmount)
  Vulnerabilities not detected

**Tokens in, NFT out**

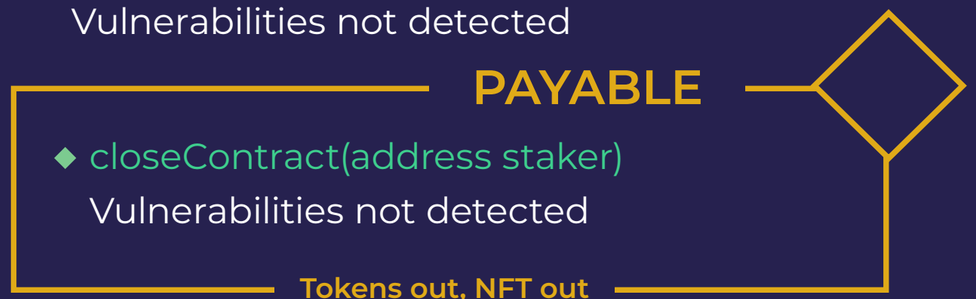
- readStake(address staker)
  Vulnerabilities not detected

- readElapsedSeconds(address staker)
  Vulnerabilities not detected

- calculateInterest(address staker)
  Vulnerabilities not detected

- readPrincipalInterest(address staker)
  Vulnerabilities not detected

- setCompletedActivities(address staker, uint256 completedActivities)
  Vulnerabilities not detected




- setActive(uint256 templateIndex, bool willBeActive)
  Vulnerabilities not detected

- isWhitelisted(address addr)
  Vulnerabilities not detected

- setWhitelisted(address addr, bool whitelistArg)
  Function should emit an event. Recommended to use onlyOwner modifier.

# VERIFICATION CHECK SUMS

| Contract Name | Bytecode hash (SHA 256) |
|---|---|
| biofi_tok | dae72255a1f39c44514e062a608ffe9cfd2b956b5615f354875717e3ea262b68 |
| BiofiNftTest | c51b4fcd09869ac080ae3d87c5c3d62f008a7ec0204c210b95ed4cb0509495e6 |
| biofi_stake | 89f89fb955460c5a9d2d76c4c993bb8144a725f0a7980960f7bf66916e6c3a3a |

# Get In Touch

info@smartstate.tech

smartstate.tech