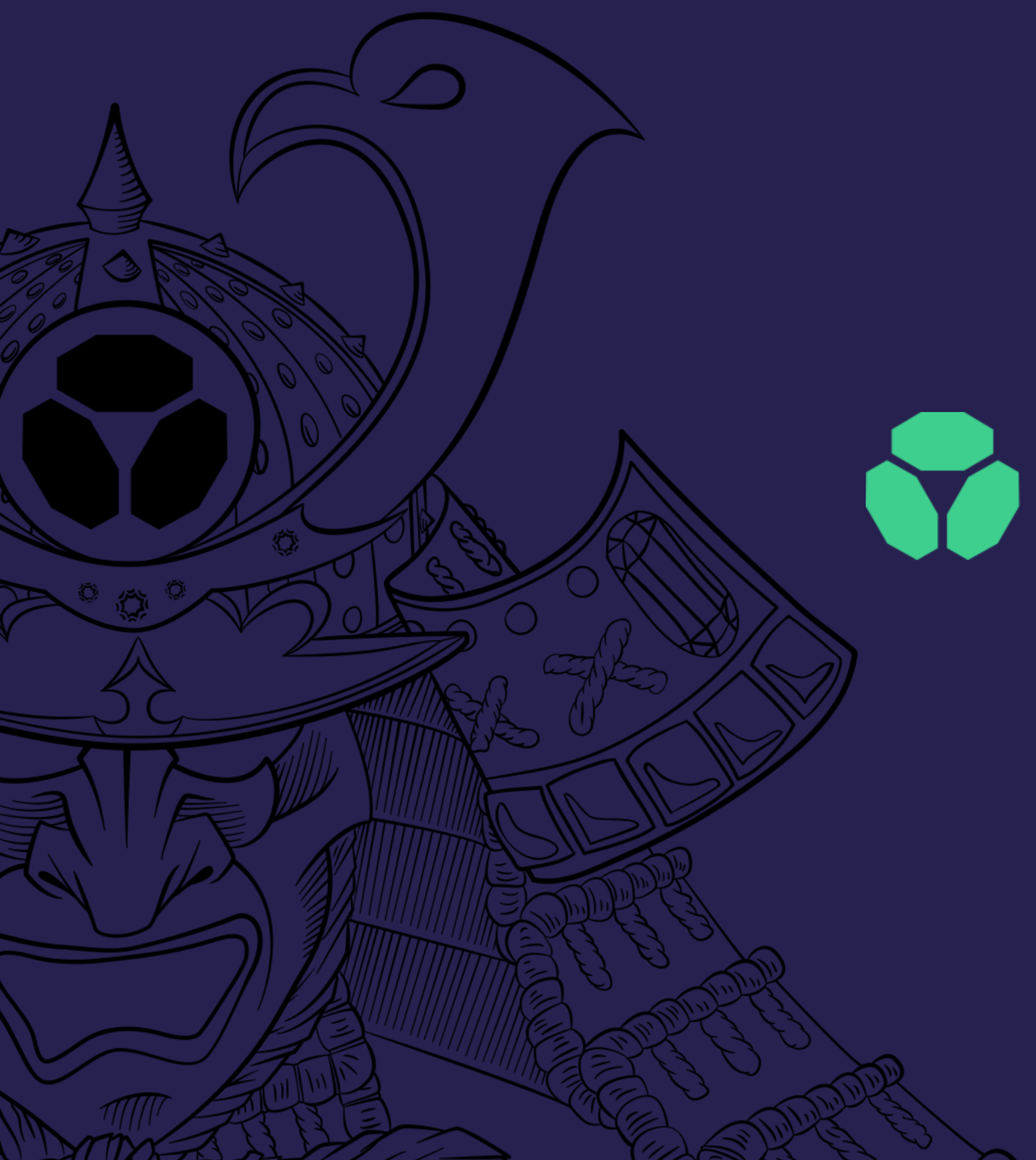


smart state

> Smart
Contract
Audit #

DAO Maker

Dec 13
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

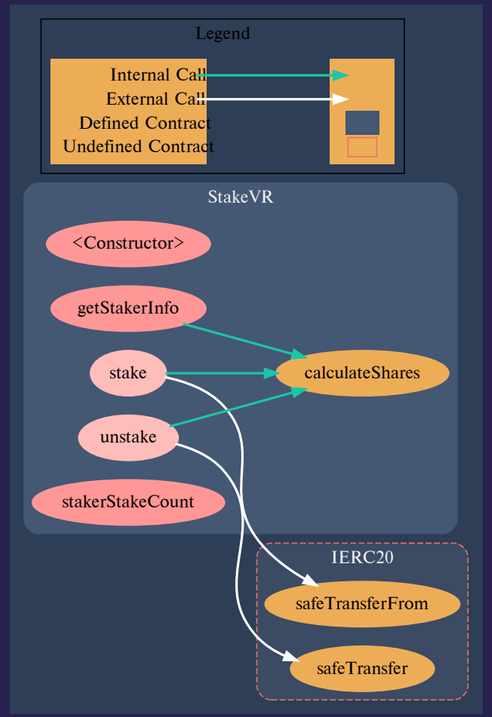
STAKEVR.SOL

CONTRACT METHODS ANALYSIS:

- stake(uint128 amount, uint16 lockDays)
  Vulnerabilities not detected

WARNING

- unstake(uint stakeIndex)
  Unstake method doesn't pay any rewards, it returns the same amount as deposited to the user. We suggest that the point of staking is earning profit, however current contract looks more like vesting.



Pic. 1.1.
StakeVR.sol

- calculateShares(
  uint amount,
  uint lockDays
)

  Vulnerabilities not detected

- getStakerInfo(
  address stakerAddress
)

  Function can be declared external

- stakerStakeCount(address stakerAddress)

  Function can be declared external

Get In Touch

info@smartstate.tech

smartstate.tech