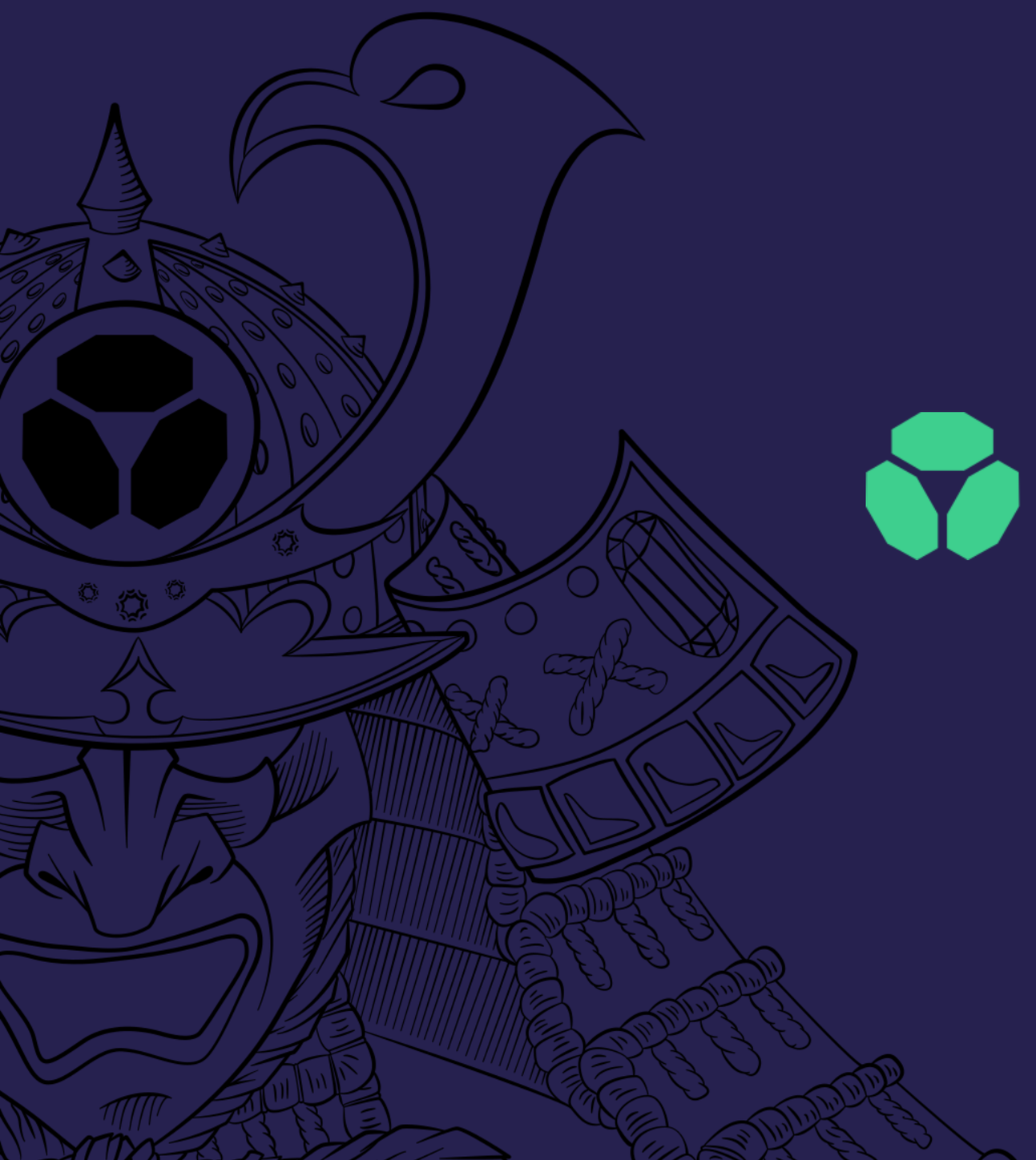


smart state

> Smart
Contract
Audit #

safle

Jan 06
2022

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

FXBASECHILDTUNNEL.SOL

CONTRACT METHODS ANALYSIS:

- setFxRootTunnel(address _fxRootTunnel)
  Method should be OnlyOwner or called in the same tx with contract deployment. Otherwise it can be called by third parties

PAYABLE

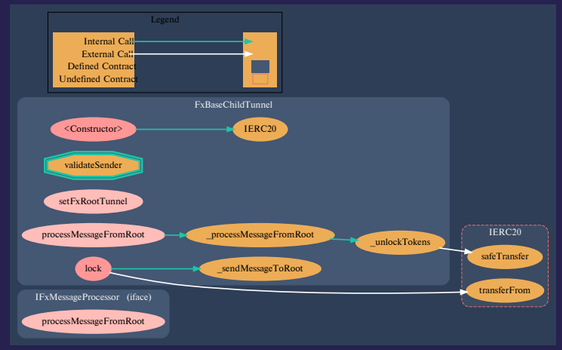
- withdraw(uint256 amount) public returns (bool)
  Vulnerabilities not detected

Tokens in

PAYABLE

- processMessageFromRoot(
  uint256 stateId,
  address rootMessageSender,
  bytes calldata data)
  Vulnerabilities not detected

Tokens out



Pic. 1.1
FxBaseChildTunnel.sol

- _sendMessageToRoot(bytes memory message)
  Vulnerabilities not detected

- _processMessageFromRoot(uint256 stateId, address sender, bytes memory message)
  Vulnerabilities not detected

- _unlockTokens(address receiver, uint256 amount)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

FXBASEROOTTUNNEL.SOL

CONTRACT METHODS ANALYSIS:

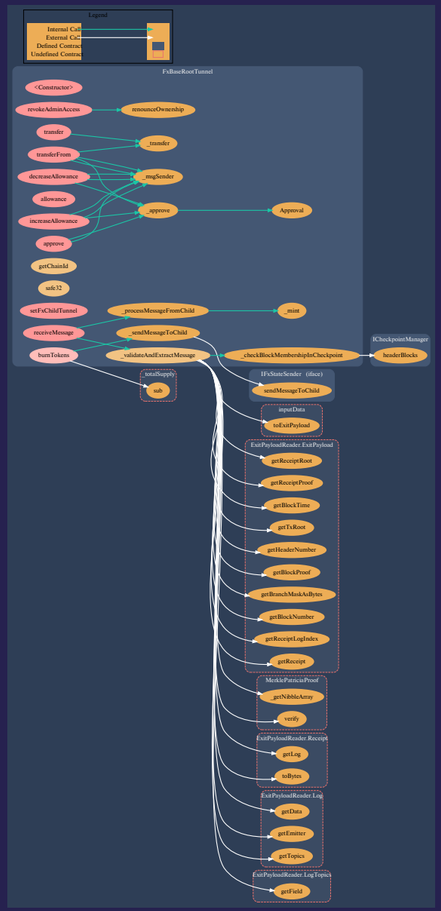
- setFxChildTunnel(address _fxChildTunnel)
  Method should be OnlyOwner or called in the same tx with contract deployment. Otherwise it can be called by third parties

PAYABLE

- deposit(uint256 amount) external returns (bool)
  Vulnerabilities not detected

Tokens in

- _sendMessageToChild(bytes memory message)
  Vulnerabilities not detected



Pic. 1.2
FxBaseRootTunnel.sol

- _checkBlockMembershipInCheckpoint(
  uint256 blockNumber,
  uint256 blockTime,
  bytes32 txRoot,
  bytes32 receiptRoot,
  uint256 headerNumber,
  bytes memory blockProof
)

  Vulnerabilities not detected

PAYABLE

- receiveMessage(bytes memory inputData)

  Vulnerabilities not detected

Tokens out

- _processMessageFromChild(bytes memory message)

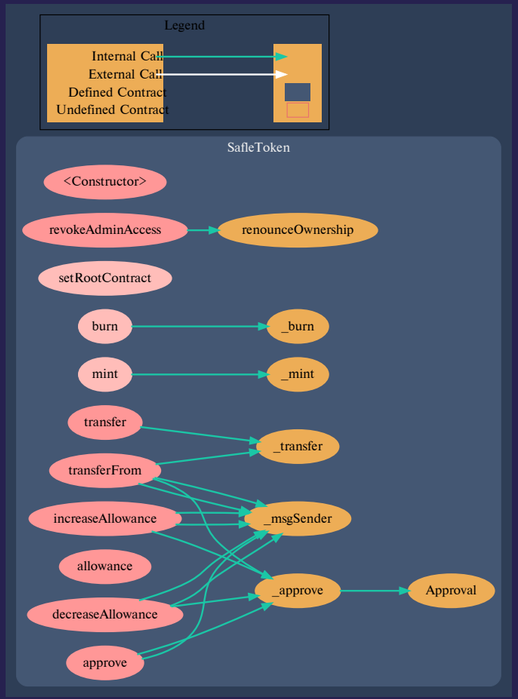
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

ETH TOKEN/SAFLE.SOL

CONTRACT METHODS ANALYSIS:

- setRootContract(address contractAddress)
  Vulnerabilities not detected
- burn(address account, uint256 amount)
  Vulnerabilities not detected
- mint(address account, uint256 amount)
  Vulnerabilities not detected
- transfer(address recepient, uint256 amount)
  Vulnerabilities not detected



Pic. 1.3
eth token/Safle.sol

- transferFrom(address src, address dst, uint amount)
  Vulnerabilities not detected

- approve(address spender, uint256 amount)
  Vulnerabilities not detected

- _approve(
    address owner,
    address spender,
    uint256 amount
)
  Vulnerabilities not detected

- allowance(address owner, address spender)
  Vulnerabilities not detected

- increaseAllowance(address spender, uint256 addedValue)
  Vulnerabilities not detected

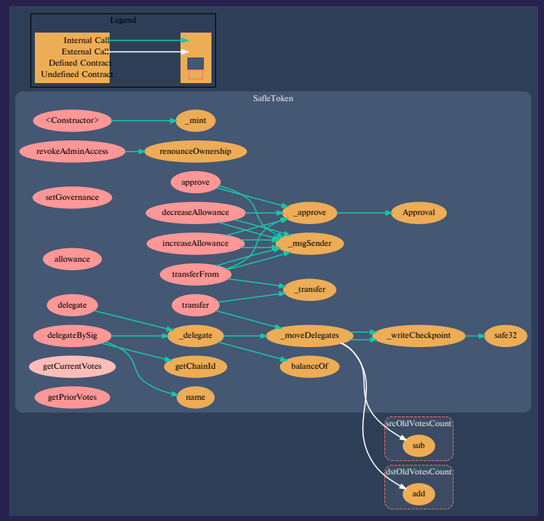
- decreaseAllowance(address spender, uint256 subtractedValue)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

POLYGON TOKEN/SAFLE.SOL

CONTRACT METHODS ANALYSIS:

- revokeAdminAccess()
  Vulnerabilities not detected
- setGovernance(address _governance)
  Vulnerabilities not detected
- transfer(address recepient, uint256 amount)
  Vulnerabilities not detected
- transferFrom(address src, address dst, uint amount)
  Function should call _moveDelegates.
- approve(address spender, uint256 amount)
  Vulnerabilities not detected



Pic. 1.4
polygon token/Safle.sol

- _approve(
  address owner,
  address spender,
  uint256 amount
)
  Vulnerabilities not detected

- allowance(address owner, address spender)
  Vulnerabilities not detected

- increaseAllowance(address spender, uint256 addedValue)
  Vulnerabilities not detected

- decreaseAllowance(address spender, uint256 subtractedValue)
  Vulnerabilities not detected

- delegate(address delegatee)
  Vulnerabilities not detected

- delegateBySig(address delegatee, uint256 nonce, uint256 expiry, uint8 v, bytes32 r, bytes32 s)
  Vulnerabilities not detected

- getCurrentVotes(address account)
  Vulnerabilities not detected

- getPriorVotes(address account, uint256 blockNumber)
  Vulnerabilities not detected

- _delegate(address delegator, address delegatee)
  Vulnerabilities not detected

- _moveDelegates(address source, address destination, uint256 amount)
  Vulnerabilities not detected

- _writeCheckpoint(address delegatee, uint256 nCheckpoints, uint256 oldVotes, uint256 newVotes)
  Vulnerabilities not detected

- getChainId()
  Vulnerabilities not detected

- safe32(uint n, string memory errorMessage)
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
FxBaseChildTunnel	0.8.11	200	a542670f030d4d4124a3e03a3b4ecde6e8dda06ae3fa5e96bf3324c0b19855ac
FxBaseRootTunnel	0.8.11	200	f8288137c9a89682c3cfb3569664914a23623beb16d770de3dd344210c3692f5
eth token/Safle	0.8.11	200	cc0574d5563b843de8254d42c4dddafe69a0d06ab210ece2b8280ece8d2f52e7
polygon token/Safle	0.8.11	200	d777557807aa4dd70575057971722e6172190ddebd26b14a9d7a17ddf6d1dc0b

Get In Touch

info@smartstate.tech

smartstate.tech