SMART CONTRACT AUDIT

Neko

Experimental Network of Maze Protocol

PROJECT: NEKO

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
- 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
- Pool Asset Security (backdoors in the underlying ERC-20)

STRUCTURE OF CONTRACT
DEBTTOKEN.DOL

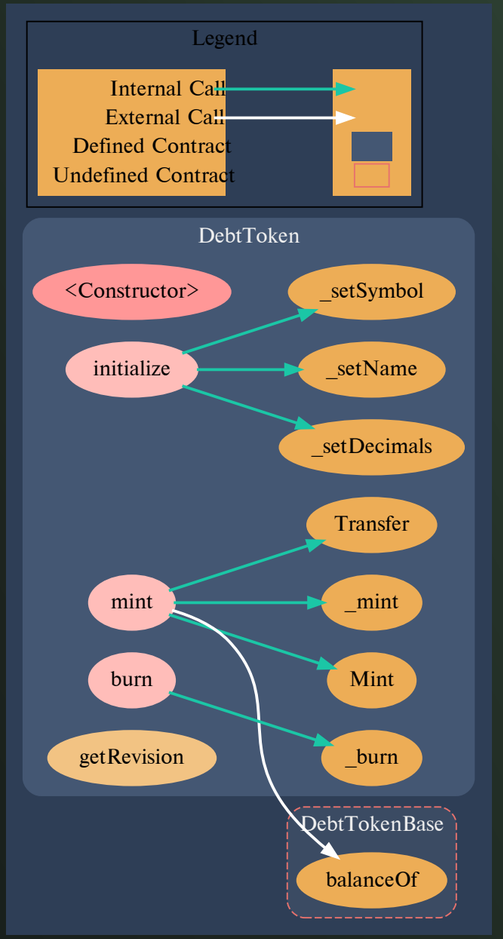
Contract methods analysis

initialize()
Vulnerabilities not detected

mint()
Vulnerabilities not detected

burn()
Vulnerabilities not detected

getRevision()
Vulnerabilities not detected



Pic. 1.1.
DebtToken.dol

STRUCTURE OF CONTRACT DEBTTOKENBASE.SOL

Contract methods analysis

approveDelegation()
Vulnerabilities not detected

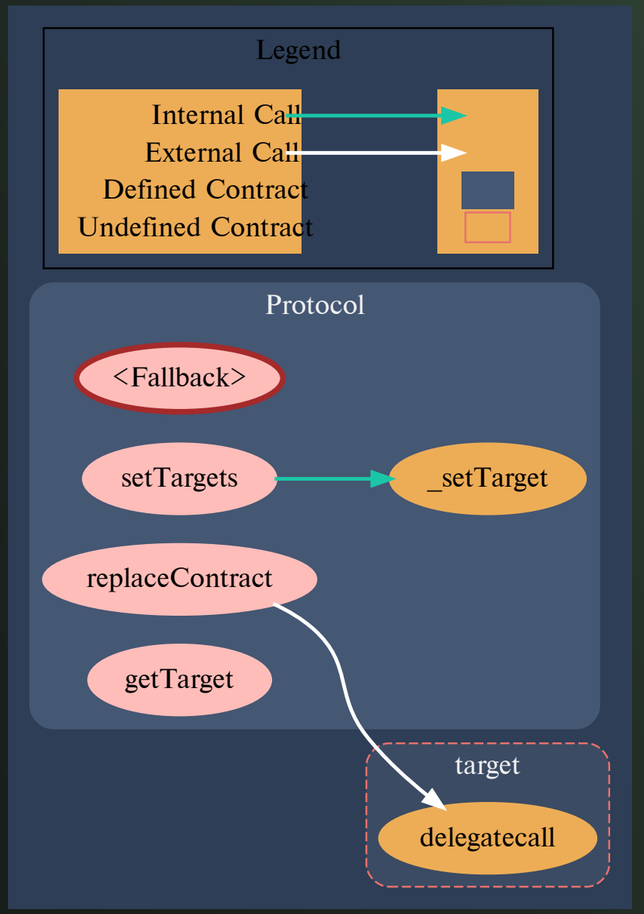
borrowAllowance()
Vulnerabilities not detected

transfer()
Vulnerabilities not detected

allowance()
Vulnerabilities not detected

approve()
Vulnerabilities not detected

transferFrom()
Vulnerabilities not detected



Pic. 1.2.
DebtTokenBase.sol

increaseAllowance()
Vulnerabilities not detected

decreaseAllowance()
Vulnerabilities not detected

_decreaseBorrowAllowance()
Vulnerabilities not detected

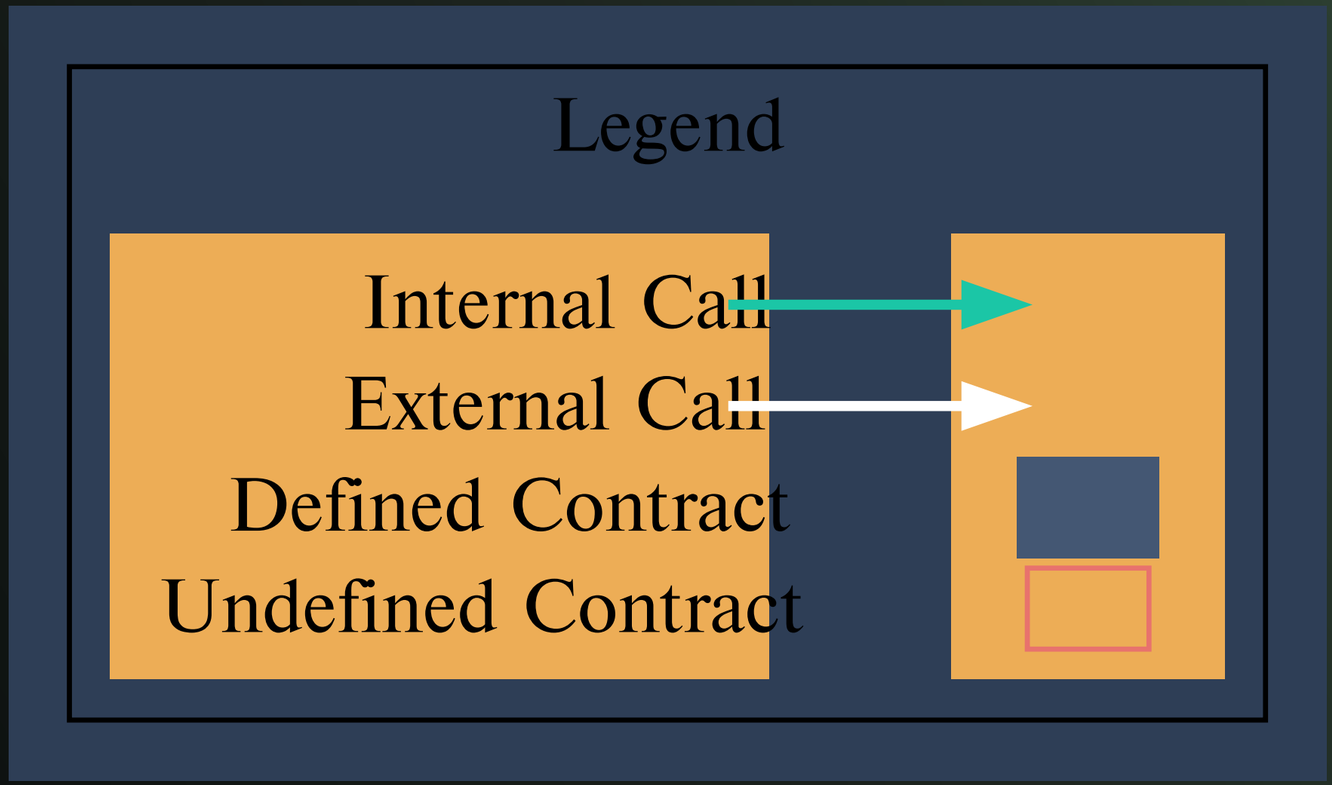
setTokenOwner()
Vulnerabilities not detected

removeTokenOwner()
Vulnerabilities not detected

STRUCTURE OF CONTRACT
ERRORS.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 1.3.
Errors.sol

STRUCTURE OF CONTRACT FUNDINGTOKEN.SOL

Contract methods analysis

burn()
Vulnerabilities not detected

mint()
Vulnerabilities not detected

transferUnderlyingTo()
Vulnerabilities not detected

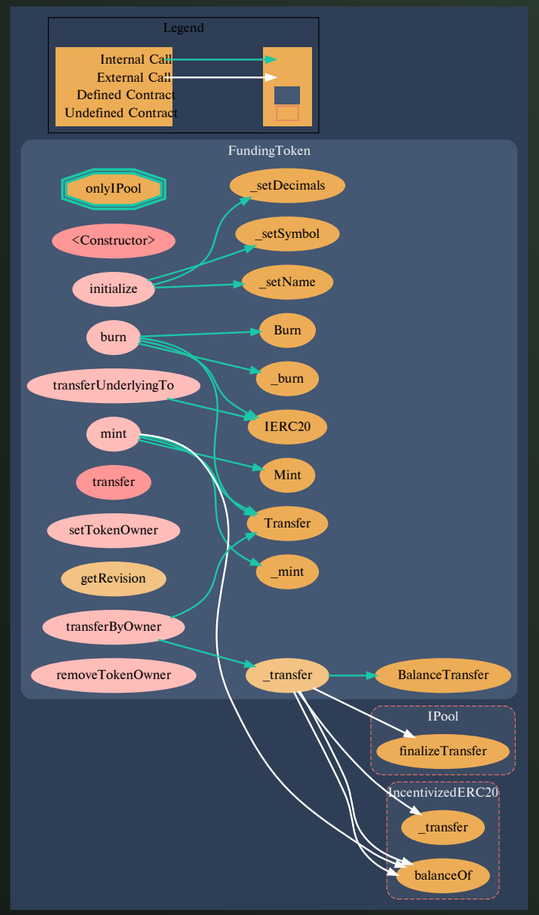
transfer()
Vulnerabilities not detected

setTokenOwner()
Vulnerabilities not detected

getRevision()
Vulnerabilities not detected

transferByOwner()
Vulnerabilities not detected

removeTokenOwner()
Vulnerabilities not detected



Pic 1.4.
FundingToken.sol

STRUCTURE OF CONTRACT GENERICLOGIC.SOL

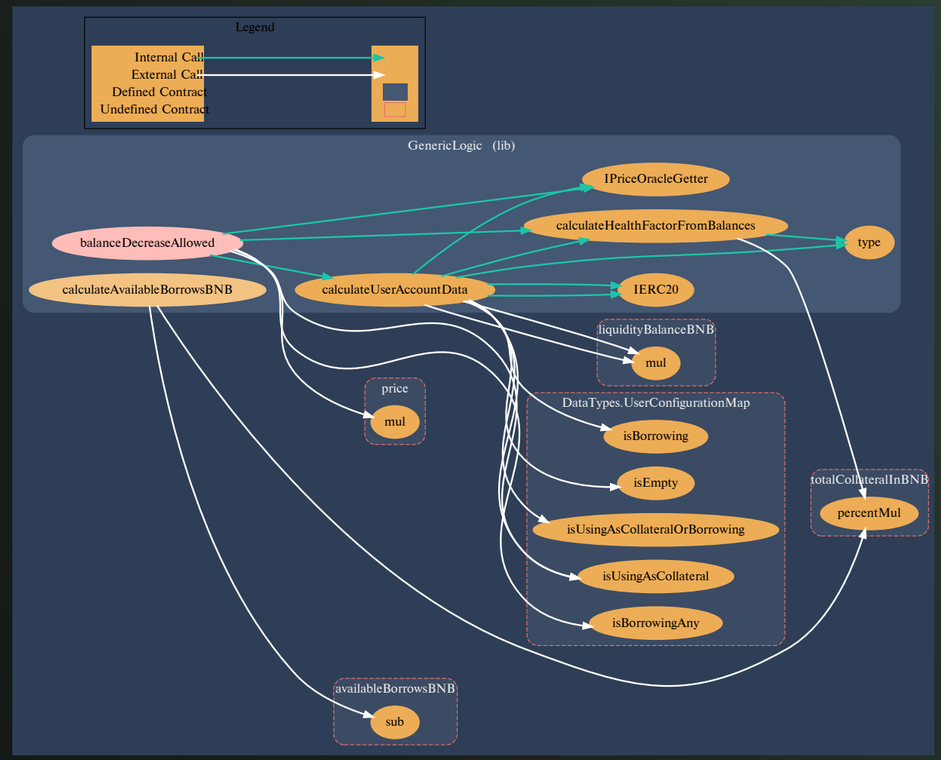
Contract methods analysis

balanceDecreaseAllowed()
Vulnerabilities not detected

calculateUserAccountData()
Vulnerabilities not detected

calculateHealthFactorFromBalances()
Vulnerabilities not detected

calculateAvailableBorrowsBNB()
Vulnerabilities not detected



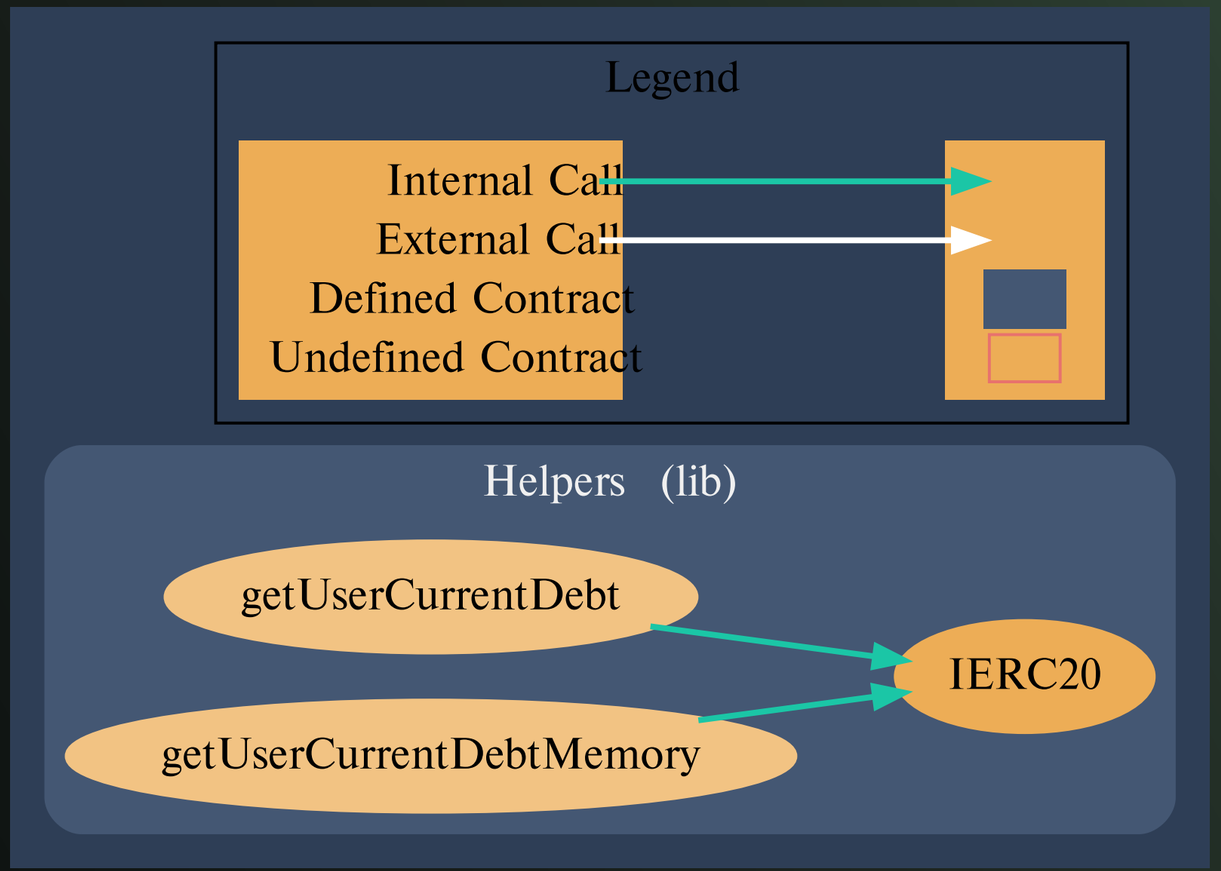
Pic. 1.5.
GenericLogic.sol

STRUCTURE OF CONTRACT
HELPERS.SOL

Contract methods analysis

getUserCurrentDebt()
Vulnerabilities not detected

getUserCurrentDebtMemory()
Vulnerabilities not detected

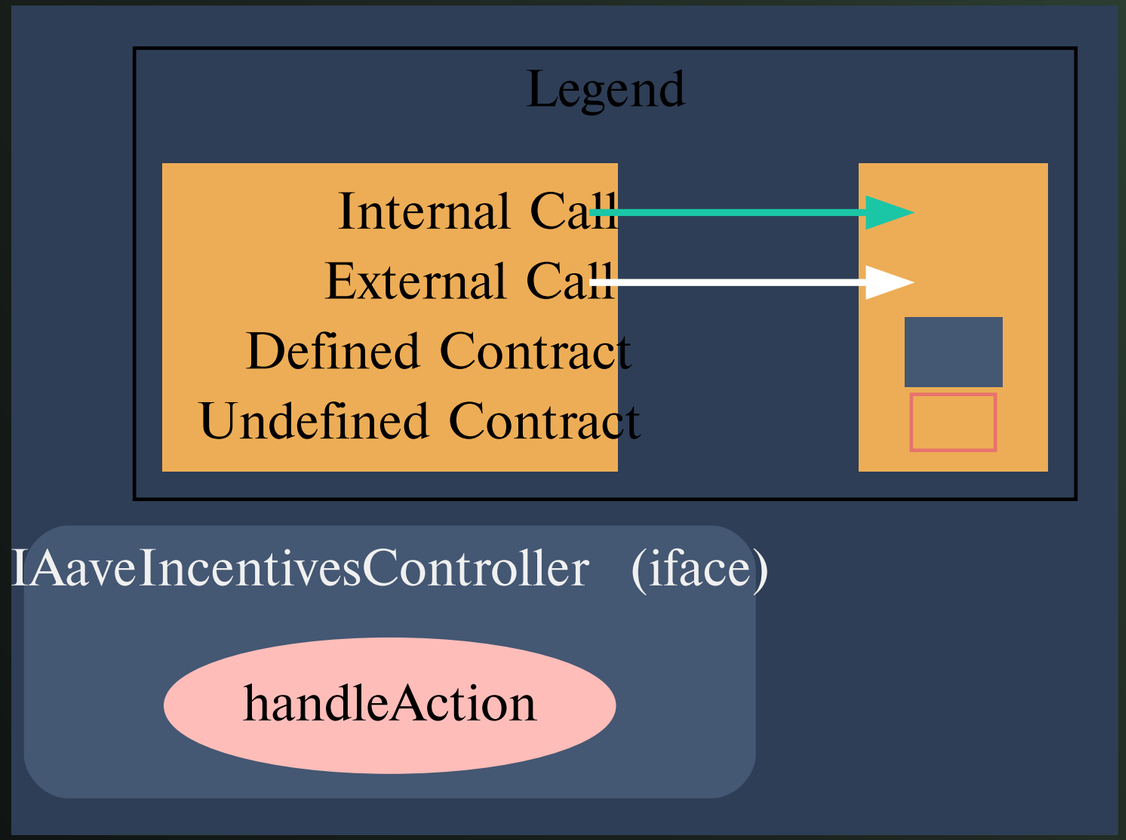


Pic. 1.6.
Helpers.sol

STRUCTURE OF CONTRACT
IAAVEINCENTIVESCONTROLLER.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 1.7.
IAaveIncentivesController.sol

STRUCTURE OF CONTRACT IDEBTTOKEN.SOL

Contract methods analysis

Vulnerabilities not detected

Pic. 1.8.
IDebtToken.sol

STRUCTURE OF CONTRACT IMTOKEN.SOL

Contract methods analysis

Vulnerabilities not detected

Pic. 1.9.
IMToken.sol

STRUCTURE OF CONTRACT
IMINE.SOL

Contract methods analysis

Vulnerabilities not detected

Pic. 2.0.
Imine.sol

STRUCTURE OF CONTRACT
IMININGTOKEN.SOL

Contract methods analysis

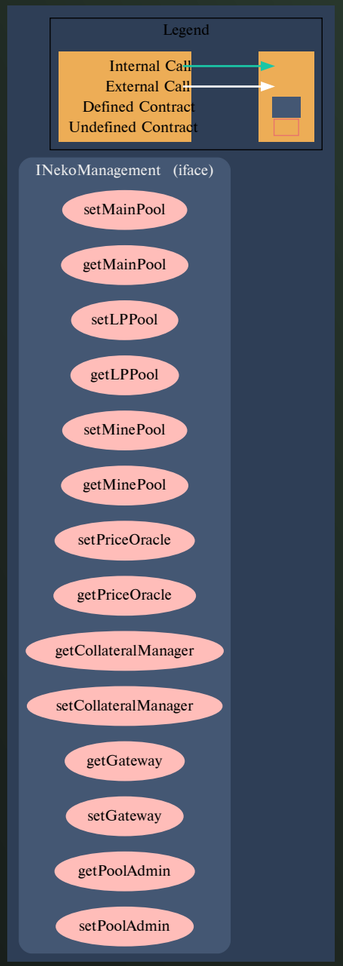
Vulnerabilities not detected

Pic. 2.0.1.
IMiningToken.sol

STRUCTURE OF CONTRACT INEKOMANAGEMENT.SOL

Contract methods analysis

Vulnerabilities not detected

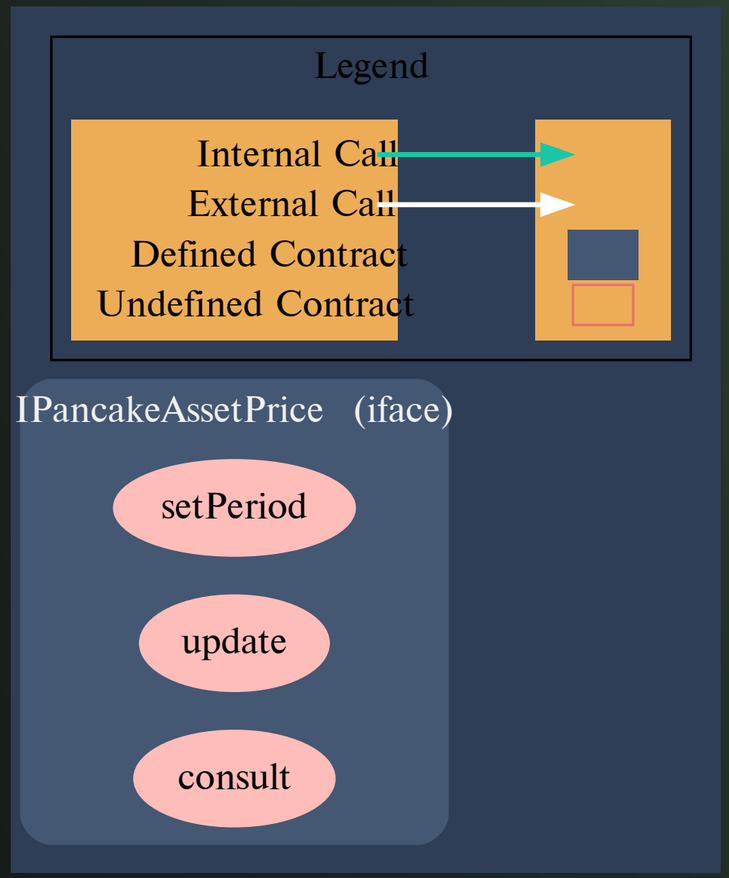


Pic. 2.1.
INekoManagement.sol

STRUCTURE OF CONTRACT
IPANCAKEASSETPRICE.SOL

Contract methods analysis

Vulnerabilities not detected

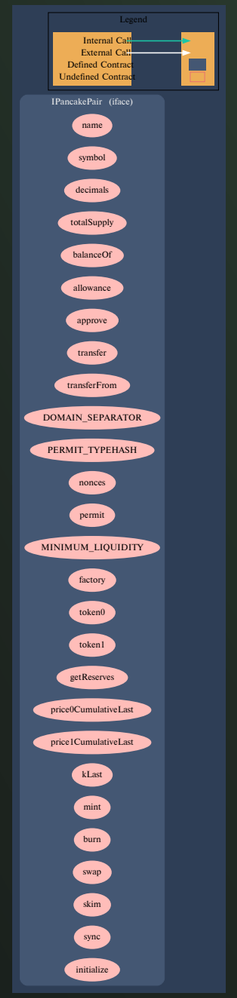


Pic. 2.2.
IPancakeAssetPrice.sol

STRUCTURE OF CONTRACT IPANCAKEPAIR.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 2.3.
IPancakePair.sol

STRUCTURE OF CONTRACT
IPOOL.SOL

Contract methods analysis

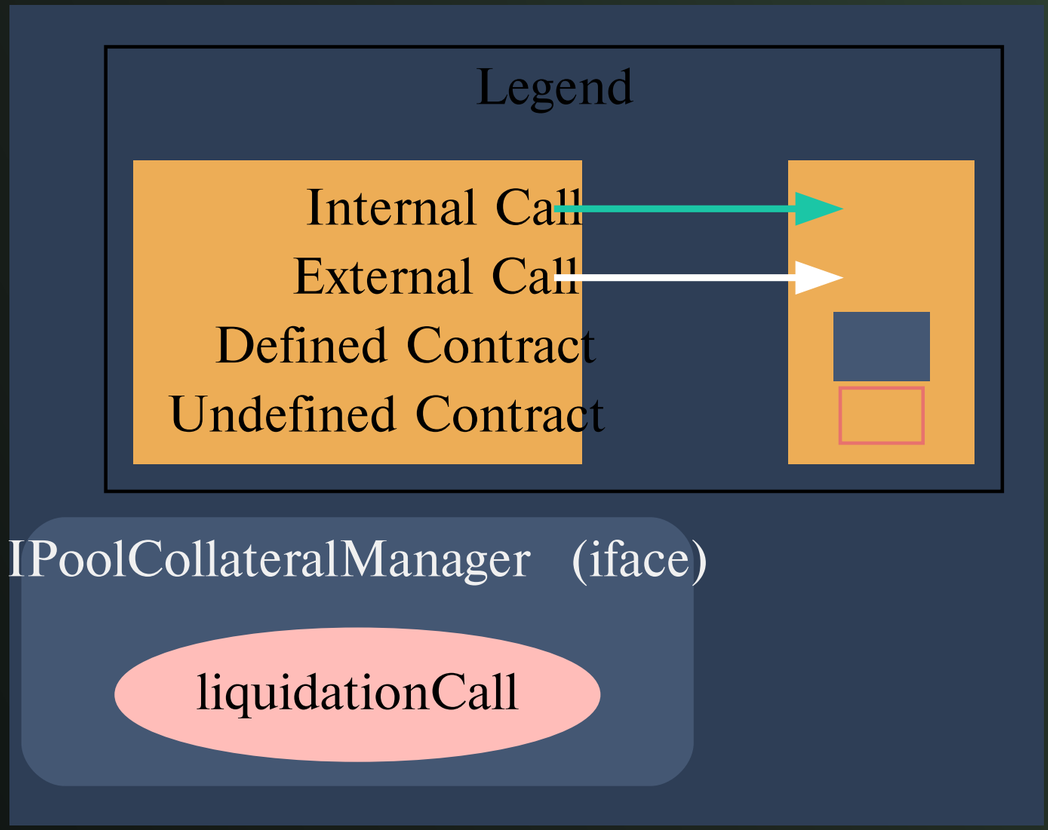
Vulnerabilities not detected

Pic 2.4.
Ipool.sol

STRUCTURE OF CONTRACT IPOOLCOLLATERALMANAGER.SOL

Contract methods analysis

Vulnerabilities not detected

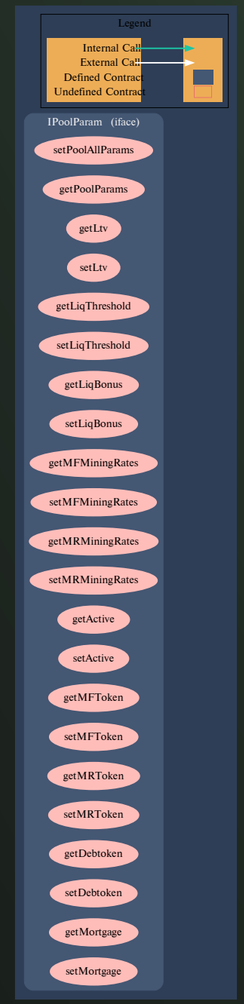


Pic. 2.5.
IPoolCollateralManager.sol

STRUCTURE OF CONTRACT
IPOOLPARAM.SOL

Contract methods analysis

Vulnerabilities not detected

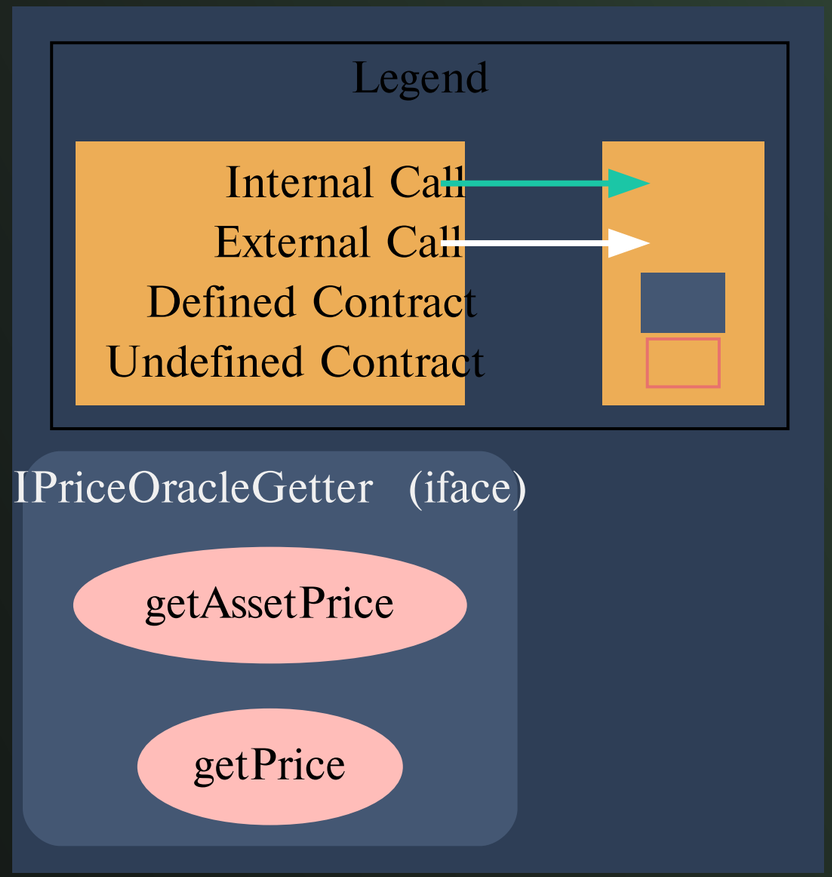


Pic. 2.6.
IPoolParam.sol

STRUCTURE OF CONTRACT
IPRICEORACLEGETTER.SOL

Contract methods analysis

Vulnerabilities not detected



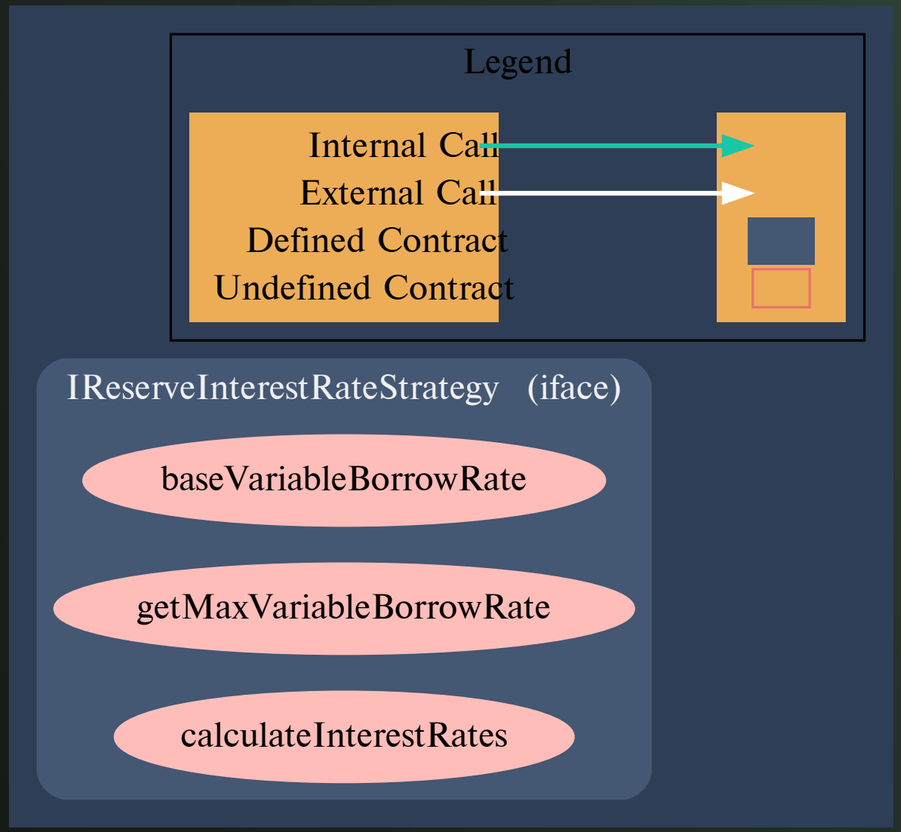
Pic. 2.7.
IPriceOracleGetter.sol

STRUCTURE OF CONTRACT

IRESERVEINTERESTRATESTRATEGY.SOL

Contract methods analysis

Vulnerabilities not detected

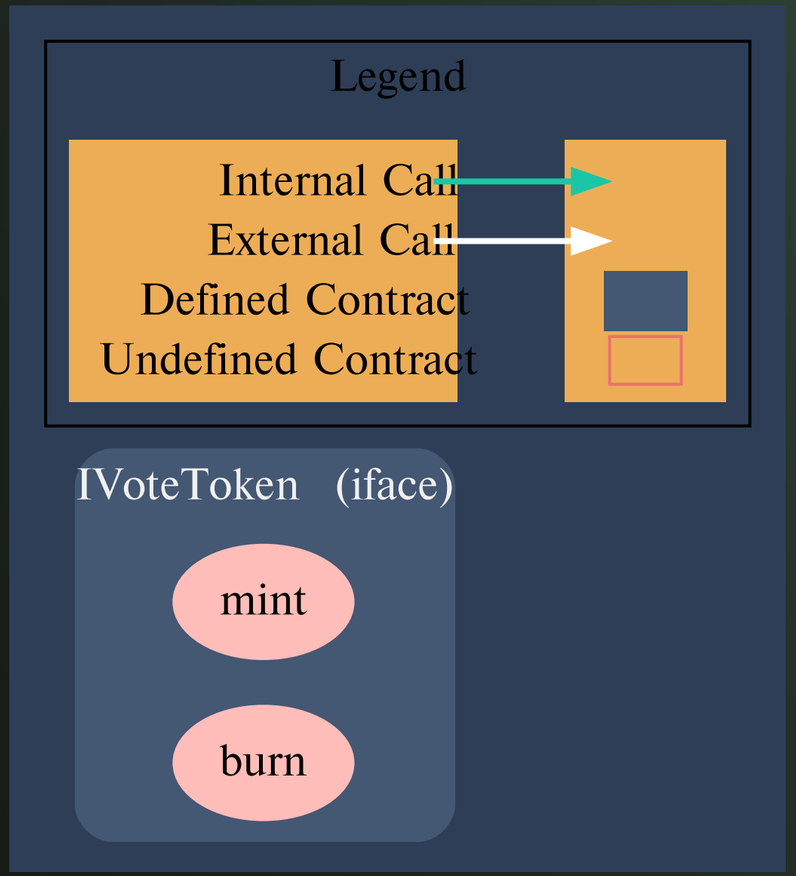


Pic. 2.8.
IReserveInterestRateStrategy.sol

STRUCTURE OF CONTRACT
IVOTETOKEN.SOL

Contract methods analysis

Vulnerabilities not detected

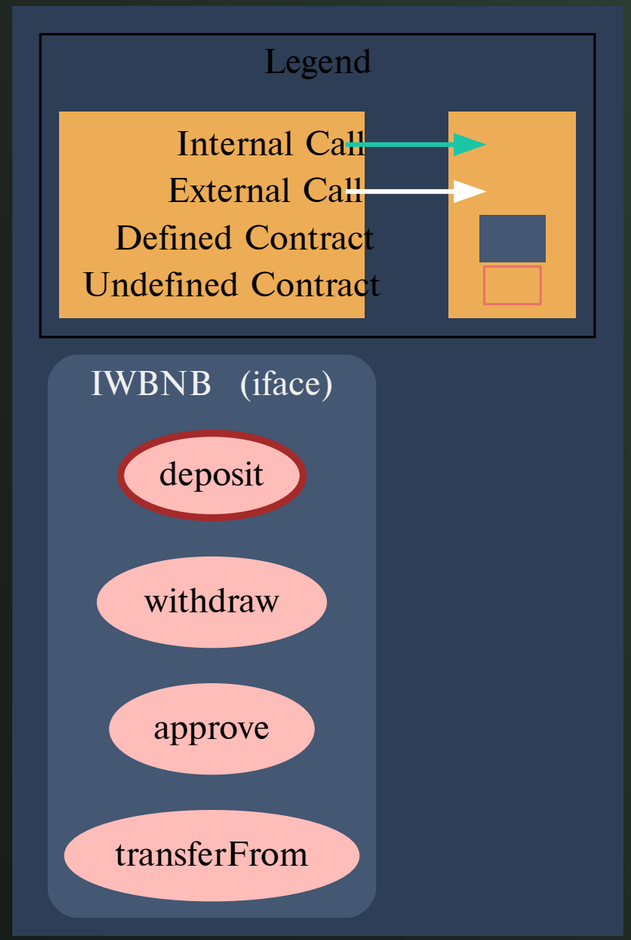


Pic 2.9.
IVoteToken.sol

STRUCTURE OF CONTRACT IWBNB.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 3.0.
IWBNB.sol

STRUCTURE OF CONTRACT IWBNBGATEWAY.SOL

Contract methods analysis

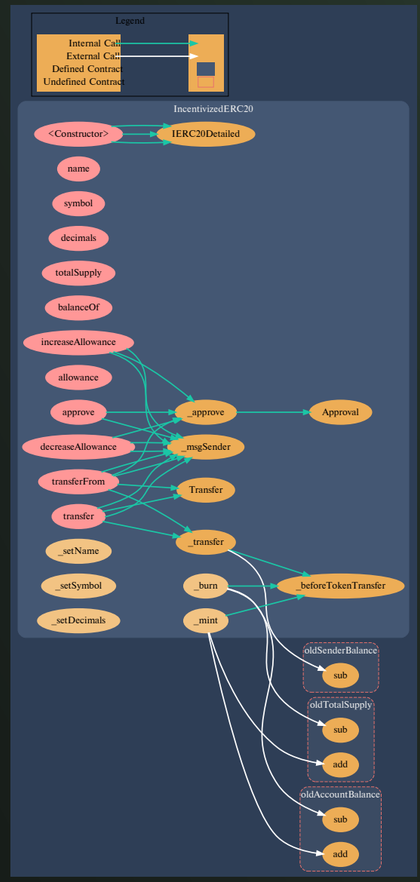
Vulnerabilities not detected

Pic. 3.1.
IWBNBGateway.sol

STRUCTURE OF CONTRACT INCENTIVIZEDERC20.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 3.2.
IncentivizedERC20.sol

STRUCTURE OF CONTRACT
LPPOOL.SOL

Contract methods analysis

initPool()
Vulnerabilities not detected

updateAssetDegrade()
Vulnerabilities not detected

updateAssetActive()
Vulnerabilities not detected

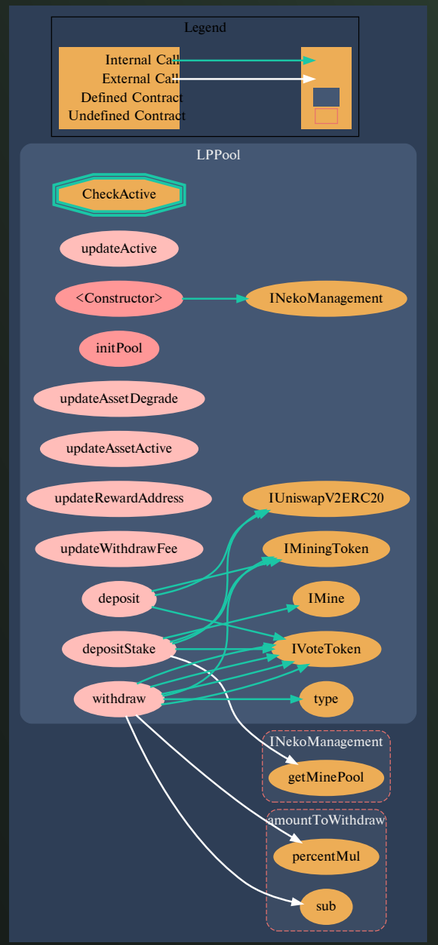
updateRewardAddress()
Vulnerabilities not detected

updateWithdrawFee()
Vulnerabilities not detected

deposit()
Vulnerabilities not detected

depositStake()
Vulnerabilities not detected

withdraw()
Vulnerabilities not detected



Pic 3.3.
LPPool.sol

STRUCTURE OF CONTRACT MAINPOOL.SOL

Contract methods analysis

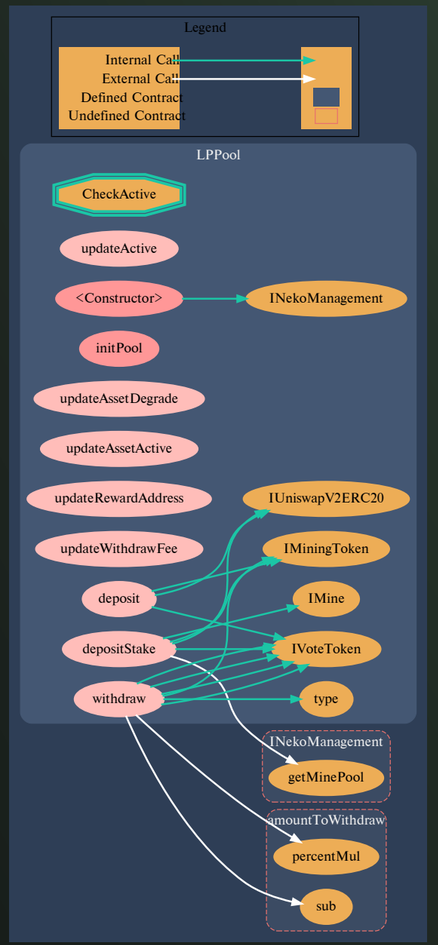
updateActive()
Vulnerabilities not detected

updateRewardAddress()
Vulnerabilities not detected

getReserveData()
Vulnerabilities not detected

getReserveBoolInfo()
Vulnerabilities not detected

getReserveUintInfo()
Vulnerabilities not detected



Pic 3.4.
MainPool.sol

getReserveAddressInfo()
Vulnerabilities not detected

deposit()
Vulnerabilities not detected

depositStake()
Vulnerabilities not detected

_deposit()
Vulnerabilities not detected

withdraw()
Vulnerabilities not detected

borrow()
Vulnerabilities not detected

repay()
Vulnerabilities not detected

liquidationCall()
Vulnerabilities not detected

restore()
Vulnerabilities not detected

finalizeTransfer()
Vulnerabilities not detected

getUserLiquidation()
Vulnerabilities not detected

getUserAccountData()
Vulnerabilities not detected

getUserFrozen()
Vulnerabilities not detected

getReservesList()
Vulnerabilities not detected

getUserConfiguration()
Vulnerabilities not detected

STRUCTURE OF CONTRACT MINE.SOL

Contract methods analysis

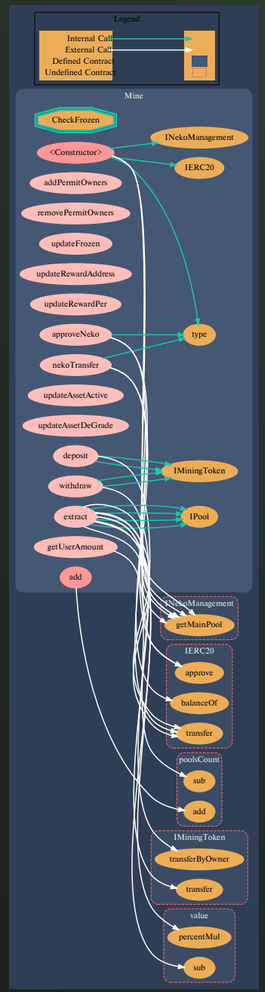
addPermitOwners()
Vulnerabilities not detected

removePermitOwners()
Vulnerabilities not detected

updateFrozen()
Vulnerabilities not detected

updateRewardAddress()
Vulnerabilities not detected

updateRewardPer()
Vulnerabilities not detected



Pic 3.5.
Mine.sol

nekoTransfer()
Vulnerabilities not detected

approveNeko()
Vulnerabilities not detected

updateAssetActive()
Vulnerabilities not detected

updateAssetDeGrade()
Vulnerabilities not detected

getUserAmount()
Vulnerabilities not detected

add()
Vulnerabilities not detected

deposit()
Vulnerabilities not detected

withdraw()
Vulnerabilities not detected

extract()
Vulnerabilities not detected

STRUCTURE OF CONTRACT MININGTOKEN.SOL

Contract methods analysis

burn()
Vulnerabilities not detected

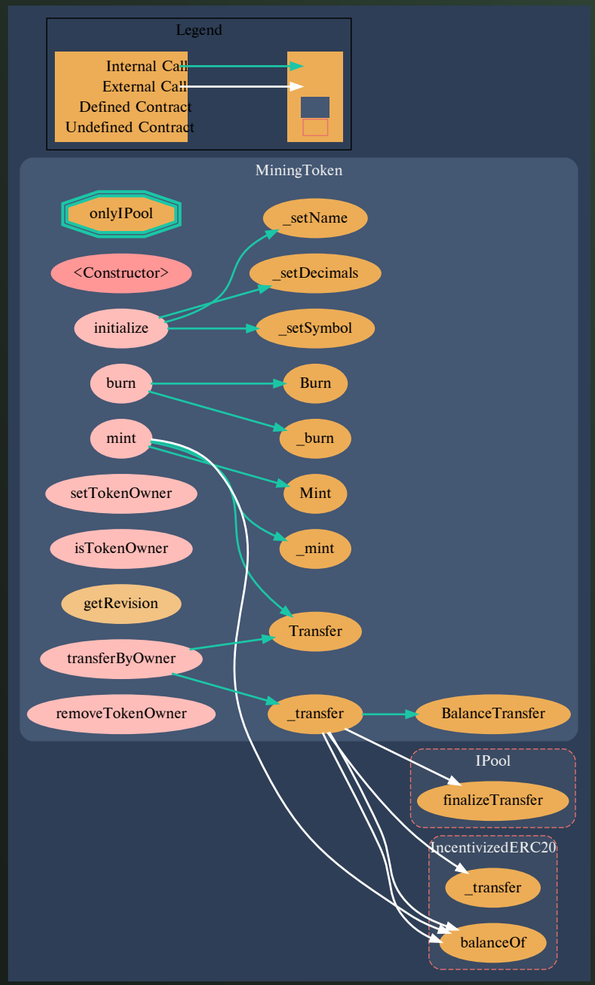
mint()
Vulnerabilities not detected

setTokenOwner()
Vulnerabilities not detected

isTokenOwner()
Vulnerabilities not detected

transferByOwner()
Vulnerabilities not detected

_transfer()
Vulnerabilities not detected



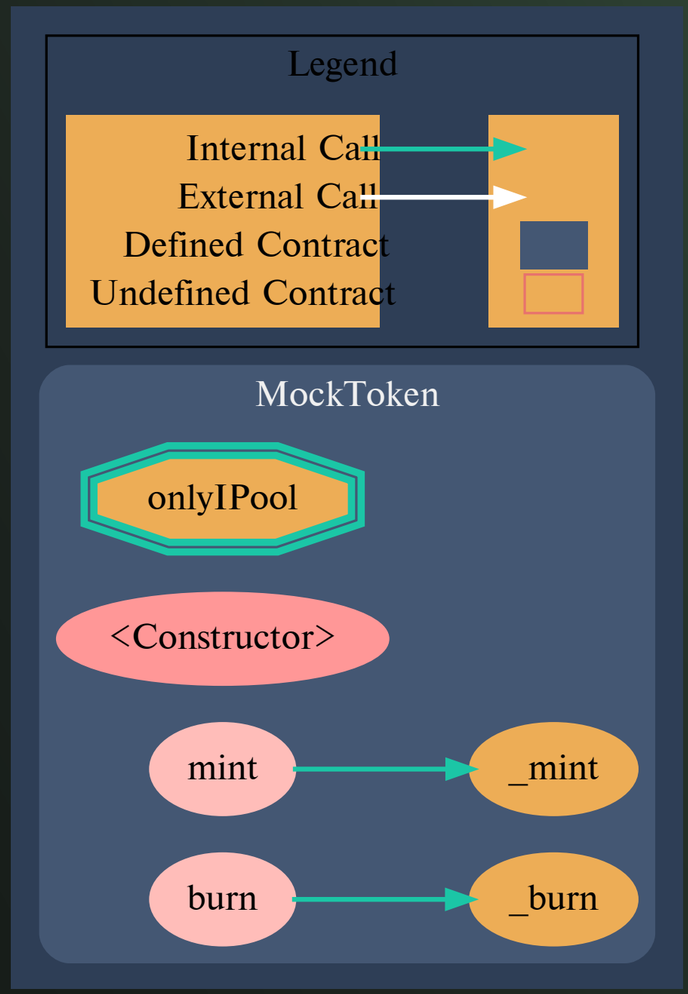
Pic 3.6.
MiningToken.sol

STRUCTURE OF CONTRACT
MOCKTOKEN.SOL

Contract methods analysis

mint()
Vulnerabilities not detected

burn()
Vulnerabilities not detected



Pic 3.7.
MockToken.sol

STRUCTURE OF CONTRACT NEKOMANAGEMENT.SOL

Contract methods analysis

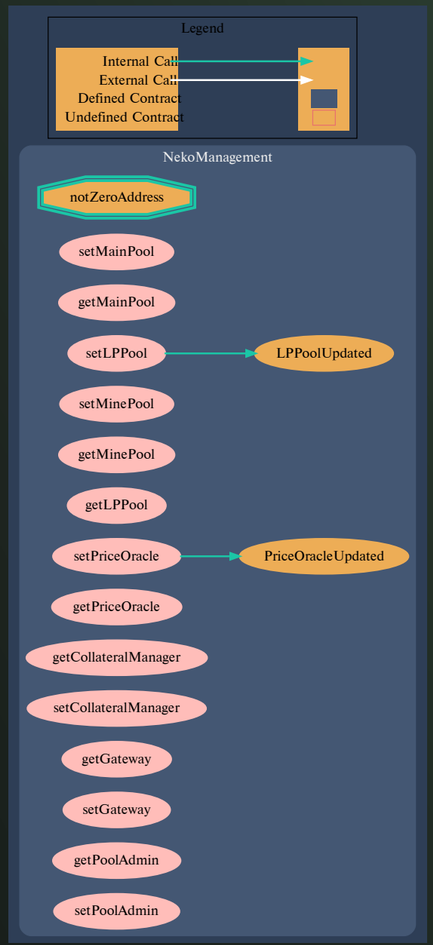
setMainPool()
Vulnerabilities not detected

getMainPool()
Vulnerabilities not detected

setLPPool()
Vulnerabilities not detected

setMinePool()
Vulnerabilities not detected

getMinePool()
Vulnerabilities not detected



Pic. 3.8.
NekoManagement.sol

getLPPool()
Vulnerabilities not detected

setPriceOracle()
Vulnerabilities not detected

getPriceOracle()
Vulnerabilities not detected

getCollateralManager()
Vulnerabilities not detected

setCollateralManager()
Vulnerabilities not detected

getGateway()
Vulnerabilities not detected

setGateway()
Vulnerabilities not detected

getPoolAdmin()
Vulnerabilities not detected

setPoolAdmin()
Vulnerabilities not detected

STRUCTURE OF CONTRACT PANCAKEASSETPRICE.SOL

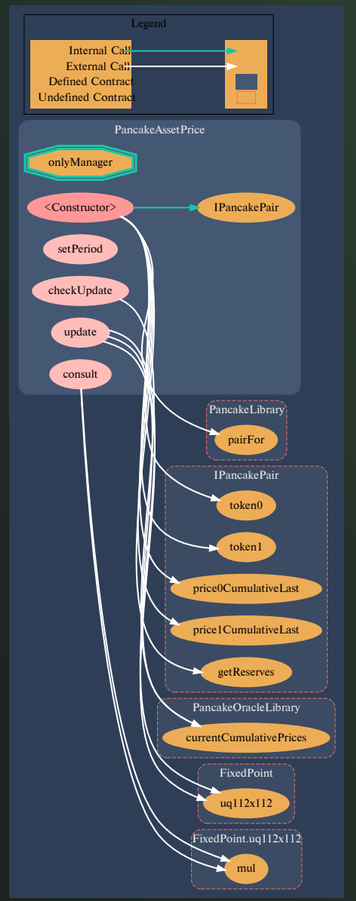
Contract methods analysis

setPeriod()
Vulnerabilities not detected

checkUpdate()
Vulnerabilities not detected

update()
Vulnerabilities not detected

consult()
Vulnerabilities not detected



Pic. 3.9.
PancakeAssetPrice.sol

STRUCTURE OF CONTRACT PANCAKELIBRARY.SOL

Contract methods analysis

sortTokens()
Vulnerabilities not detected

pairFor()
Vulnerabilities not detected

getReserves()
Vulnerabilities not detected

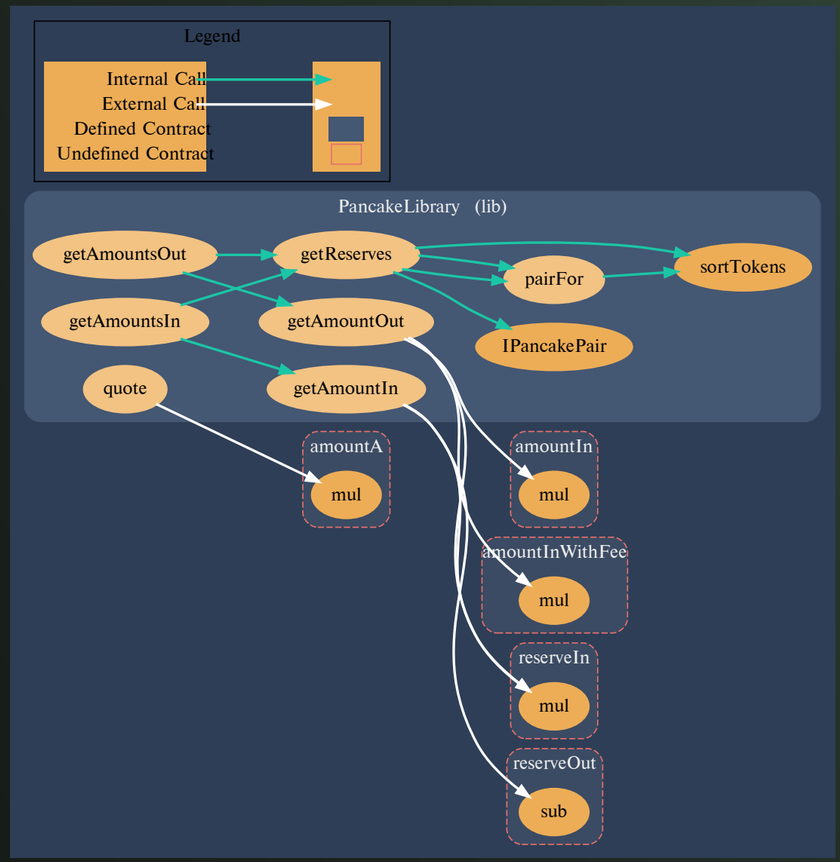
quote()
Vulnerabilities not detected

getAmountOut()
Vulnerabilities not detected

getAmountIn()
Vulnerabilities not detected

getAmountsOut()
Vulnerabilities not detected

getAmountsIn()
Vulnerabilities not detected



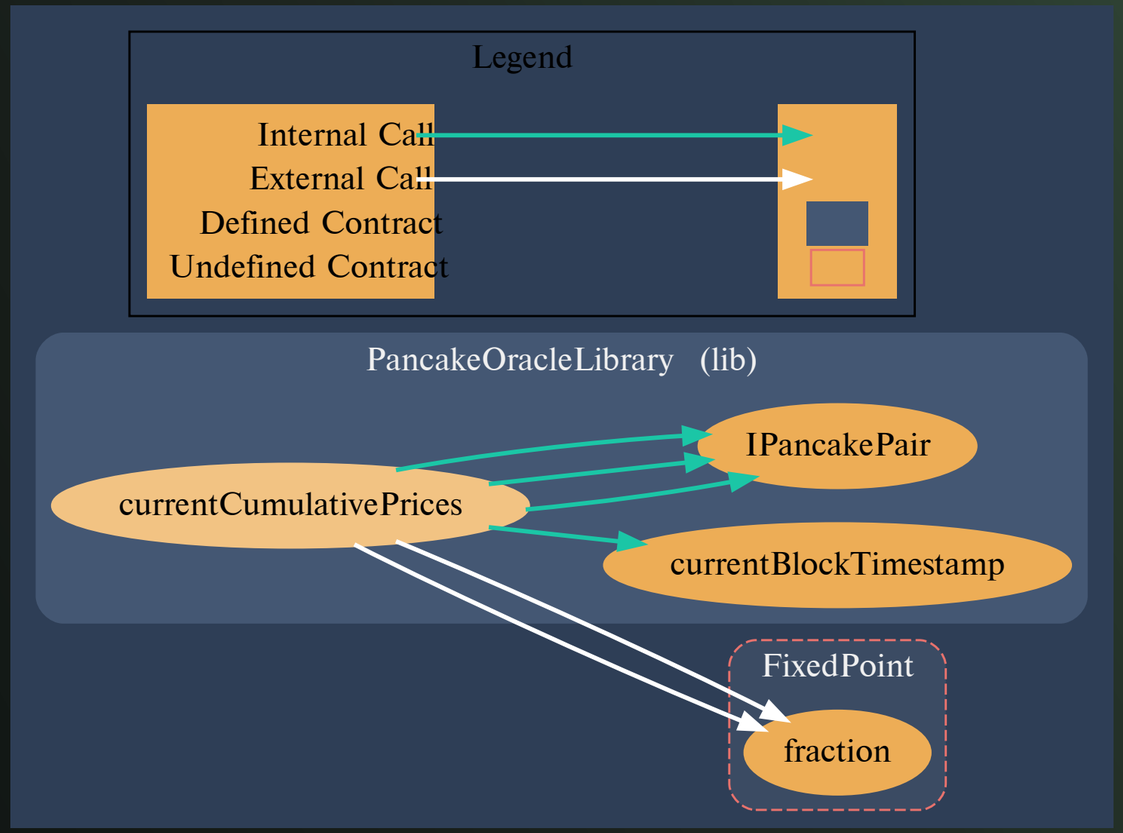
Pic. 4.0.
PancakeLibrary.sol

STRUCTURE OF CONTRACT PANCAKEORACLELIBRARY.SOL

Contract methods analysis

currentBlockTimestamp()
Vulnerabilities not detected

currentCumulativePrices()
Vulnerabilities not detected



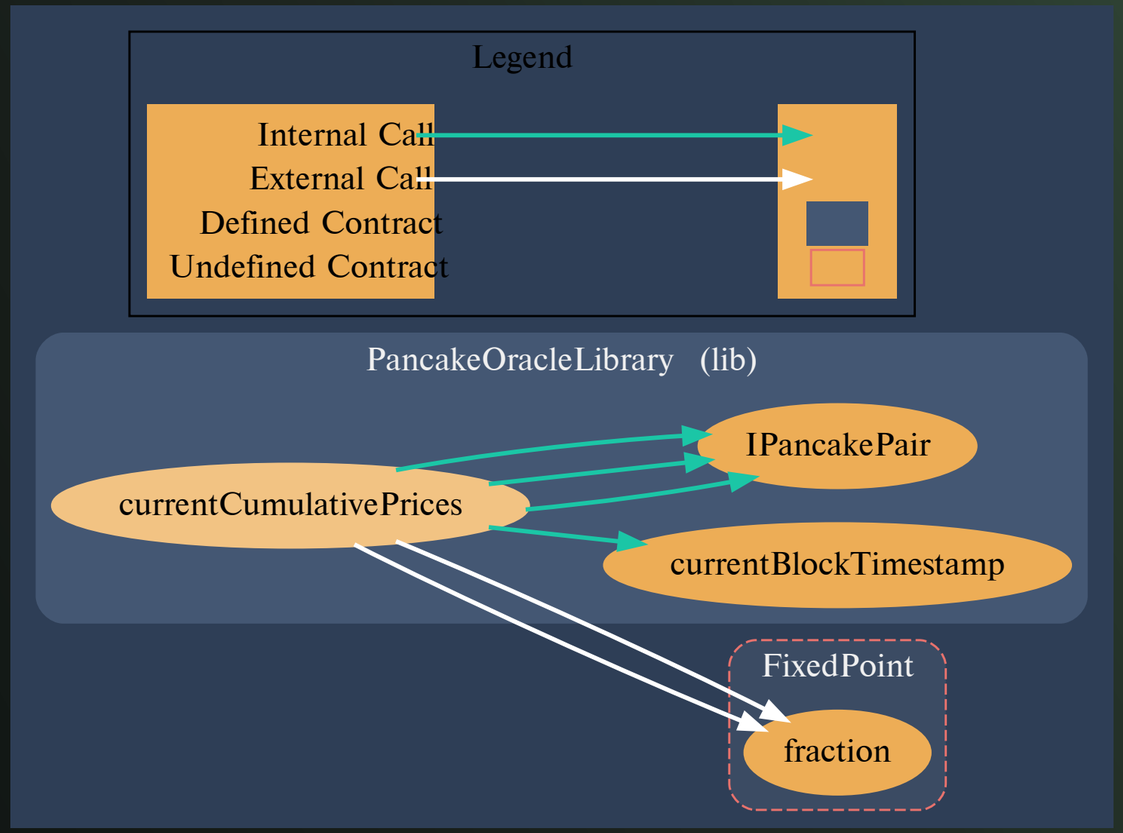
Pic. 4.1.
PancakeOracleLibrary.sol

STRUCTURE OF CONTRACT PANCAKEORACLELIBRARY.SOL

Contract methods analysis

liquidationCall()
Vulnerabilities not detected

_calculateAvailableCollateralToLiquidate()
Vulnerabilities not detected



Pic. 4.2.
PancakeOracleLibrary.sol

STRUCTURE OF CONTRACT POOLSTORAGE.SOL

Contract methods analysis

initPoolReserves()
Vulnerabilities not detected

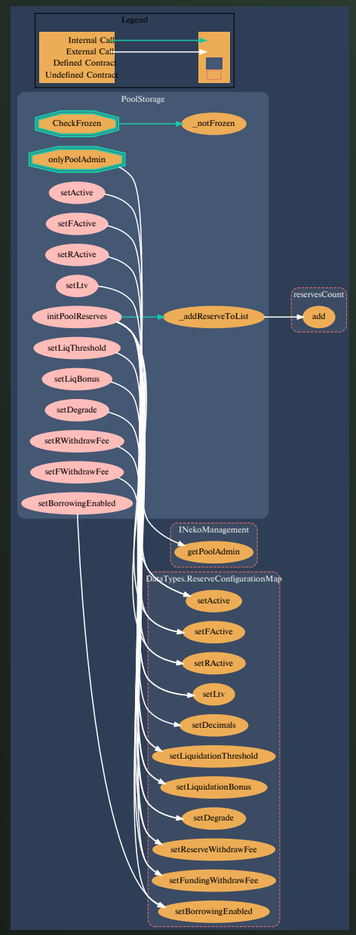
setDegrade()
Vulnerabilities not detected

setRWithdrawFee()
Vulnerabilities not detected

setFWithdrawFee()
Vulnerabilities not detected

setBorrowingEnabled()
Vulnerabilities not detected

setActive()
Vulnerabilities not detected



Pic. 4.3.
PoolStorage.sol

STRUCTURE OF CONTRACT PRICEORACLEMANAGER.SOL

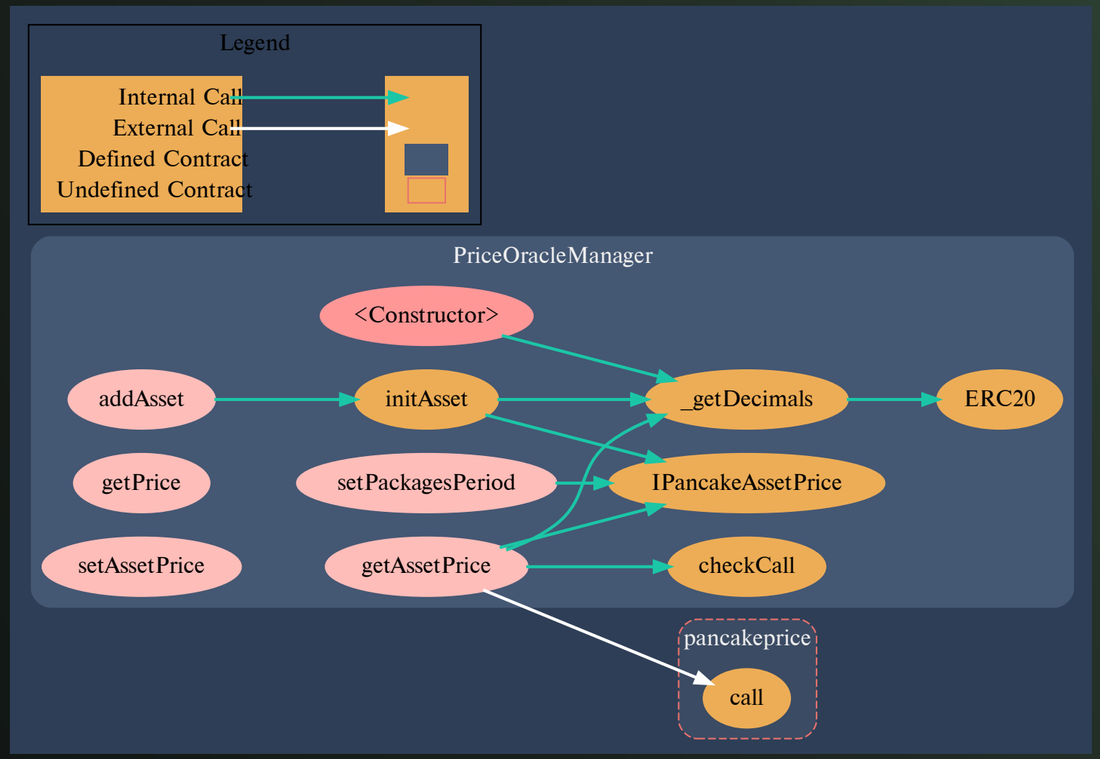
Contract methods analysis

addAsset()
Vulnerabilities not detected

initAsset()
Vulnerabilities not detected

getAssetPrice()
Vulnerabilities not detected

checkCall()
Vulnerabilities not detected



Pic. 4.4.
PriceOracleManager.sol

getPrice()
Vulnerabilities not detected

setPackagesPeriod()
Vulnerabilities not detected

setAssetPrice()
Vulnerabilities not detected

_getDecimals()
Vulnerabilities not detected

STRUCTURE OF CONTRACT RESERVECONFIGURATIONEX.SOL

Contract methods analysis

setLtv()
This function is important for the contract logic and it should emit an event

getLtv()
Vulnerabilities not detected

setLiquidationThreshold()
This function is important for the contract logic and it should emit an event

getLiquidationThreshold()
Vulnerabilities not detected

setFundingWithdrawFee()
This function is important for the contract logic and it should emit an event

Pic 4.5.
ReserveConfigurationEX.sol

getFundingWithdrawFee()
Vulnerabilities not detected

setReserveWithdrawFee()
This function is important for the contract logic and it should emit an event

getReserveWithdrawFee()
Vulnerabilities not detected

setLiquidationBonus()
This function is important for the contract logic and it should emit an event

getLiquidationBonus()
Vulnerabilities not detected

setDecimals()
This function is important for the contract logic and it should emit an event

getDecimals()
Vulnerabilities not detected

setActive()
This function is important for the contract logic and it should emit an event

setFActive()
Vulnerabilities not detected

setRActive()
Vulnerabilities not detected

setDegrade()
This function is important for the contract logic and it should emit an event

getDegrade()
Vulnerabilities not detected

getFActive()
Vulnerabilities not detected

getRActive()
Vulnerabilities not detected

setDegrade()
This function is important for the contract logic and it should emit an event

getDegrade()
Vulnerabilities not detected

getActive()
Vulnerabilities not detected

getFActive()
Vulnerabilities not detected

getRActive()
Vulnerabilities not detected

setBorrowingEnabled()
This function is important for the contract logic and it should emit an event

getBorrowingEnabled()
Vulnerabilities not detected

getFlags()
Vulnerabilities not detected

getParams()
Vulnerabilities not detected

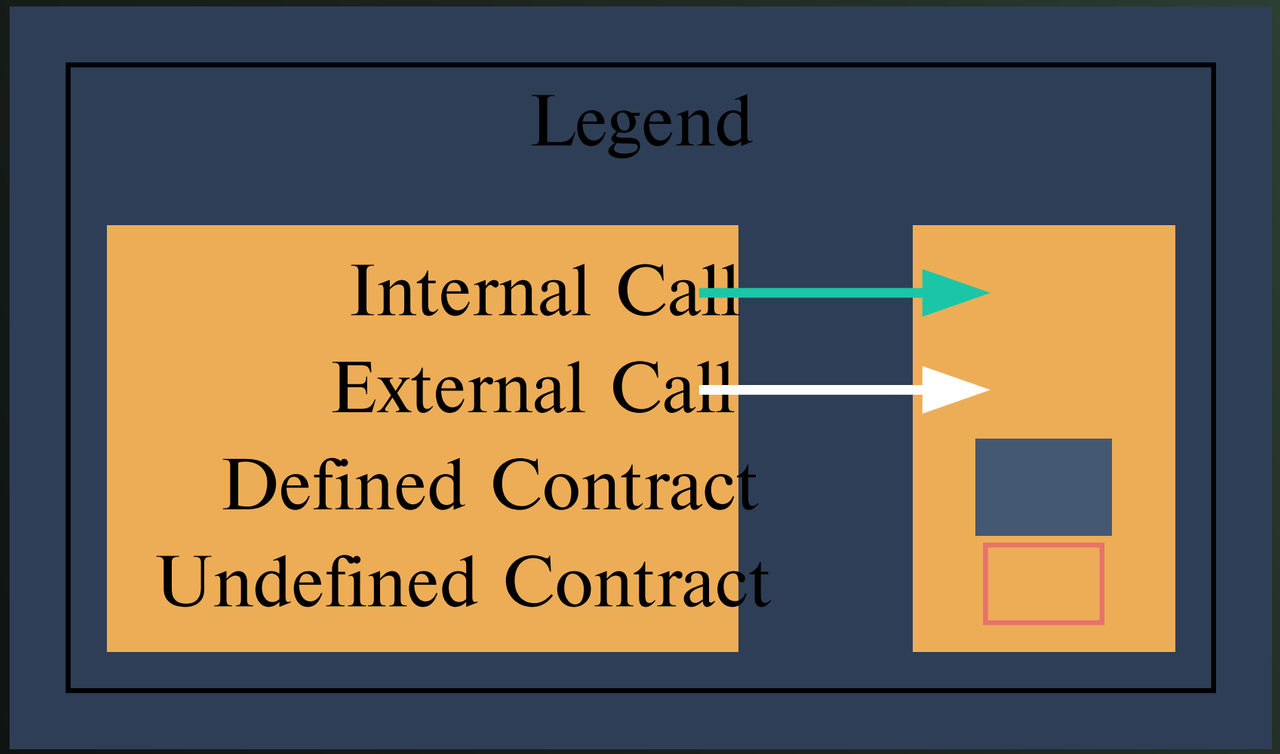
getParamsMemory()
Vulnerabilities not detected

getFlagsMemory()
Vulnerabilities not detected

STRUCTURE OF CONTRACT
RESERVELOGIC.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 4.6.
ReserveLogic.sol

STRUCTURE OF CONTRACT RESERVETOKEN.SOL

Contract methods analysis

burn()
Vulnerabilities not detected

mint()
Vulnerabilities not detected

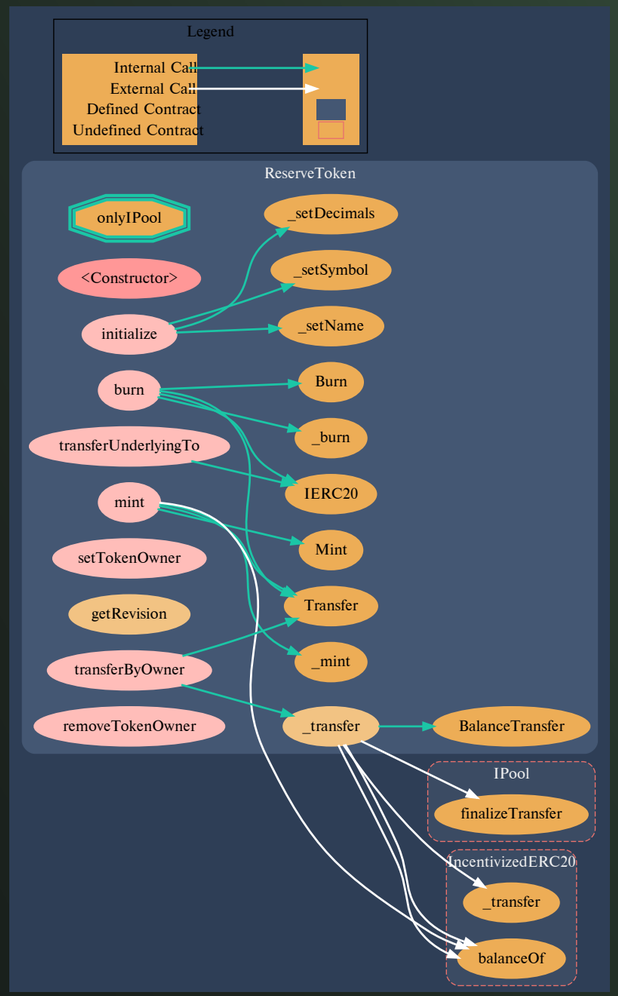
transferUnderlyingTo()
Vulnerabilities not detected

_transfer()
Vulnerabilities not detected

setTokenOwner()
Vulnerabilities not detected

transferByOwner()
Vulnerabilities not detected

removeTokenOwner()
Vulnerabilities not detected



Pic 4.7.
ReserveToken.sol

STRUCTURE OF CONTRACT USERCONFIGURATION.SOL

Contract methods analysis

setBorrowing()
Vulnerabilities not detected

setUsingAsCollateral()
Vulnerabilities not detected

isUsingAsCollateralOrBorrowing()
Vulnerabilities not detected

isBorrowing()
Vulnerabilities not detected

isUsingAsCollateral()
Vulnerabilities not detected

isBorrowingAny()
Vulnerabilities not detected

isEmpty()
Vulnerabilities not detected

setFrozen()
Vulnerabilities not detected

getFrozen()
Vulnerabilities not detected

getFrozensArray()
Vulnerabilities not detected

Pic. 4.8.
UserConfiguration.sol

STRUCTURE OF CONTRACT VALIDATIONLOGIC.SOL

Contract methods analysis

validateActive()
Vulnerabilities not detected

validateDeposit()
Vulnerabilities not detected

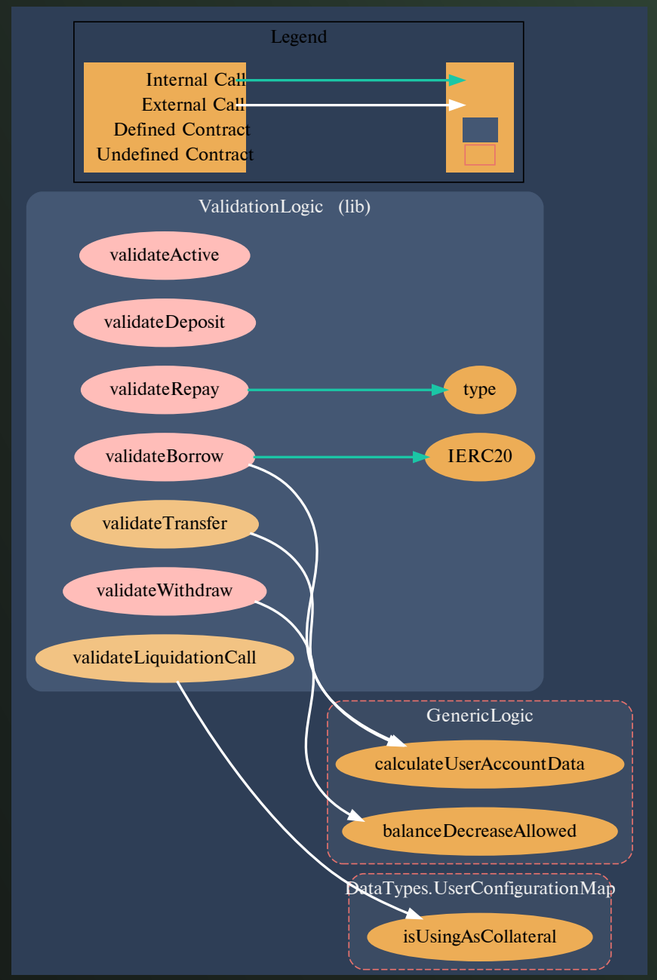
validateWithdraw()
Vulnerabilities not detected

validateBorrow()
Vulnerabilities not detected

validateRepay()
Vulnerabilities not detected

validateLiquidationCall()
Vulnerabilities not detected

validateTransfer()
Vulnerabilities not detected



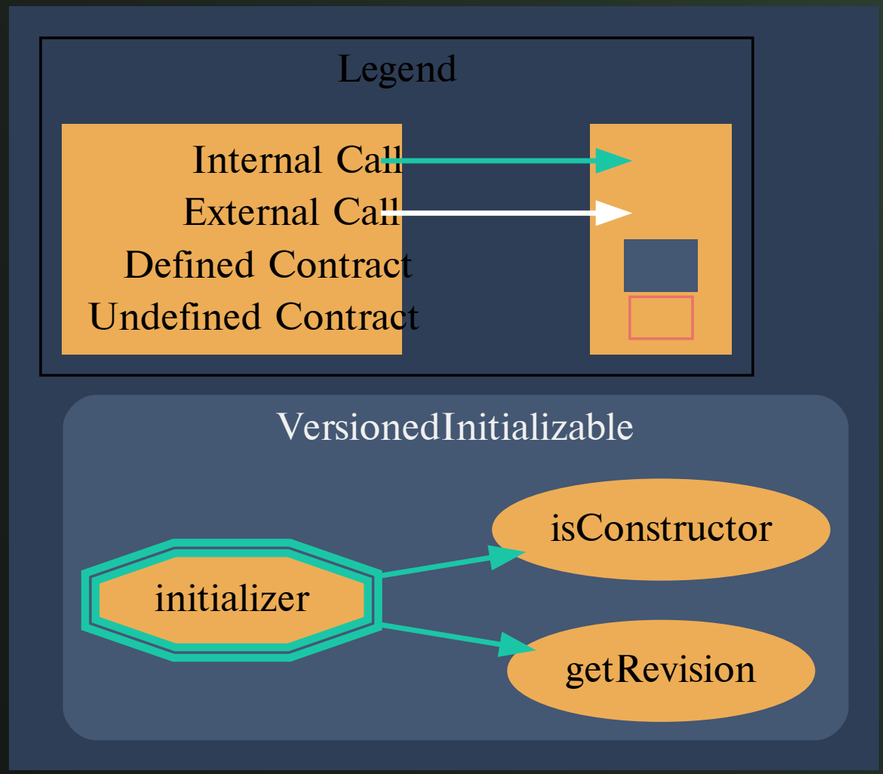
Pic. 4.9.
ValidationLogic.sol

STRUCTURE OF CONTRACT
VERSIONEDINITIALIZABLE.SOL

Contract methods analysis

getRevision()
Vulnerabilities not detected

isConstructor()
Vulnerabilities not detected



Pic. 5.0.
VersionedInitializable.sol

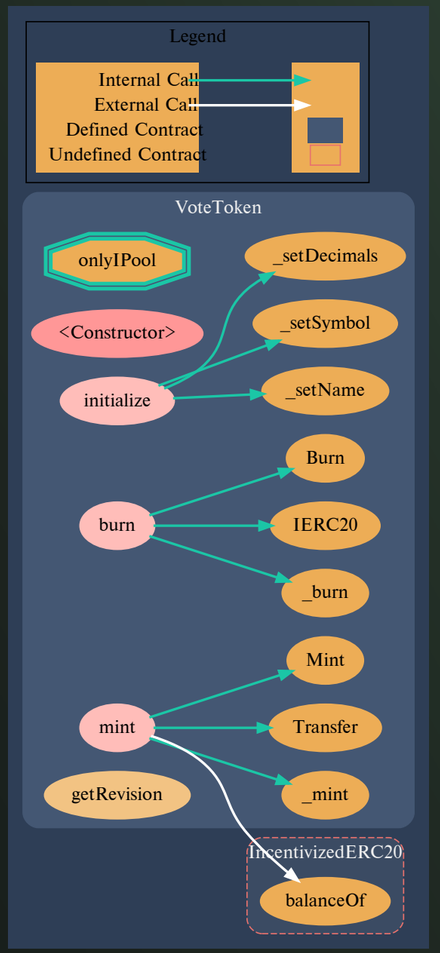
STRUCTURE OF CONTRACT VOTETOKEN.SOL

Contract methods analysis

burn()
Vulnerabilities not detected

mint()
Vulnerabilities not detected

getRevision()
Vulnerabilities not detected



Pic. 5.1.
VoteToken.sol

STRUCTURE OF CONTRACT
WBNB.SOL

Contract methods analysis

deposit()
Vulnerabilities not detected

withdraw()
Vulnerabilities not detected

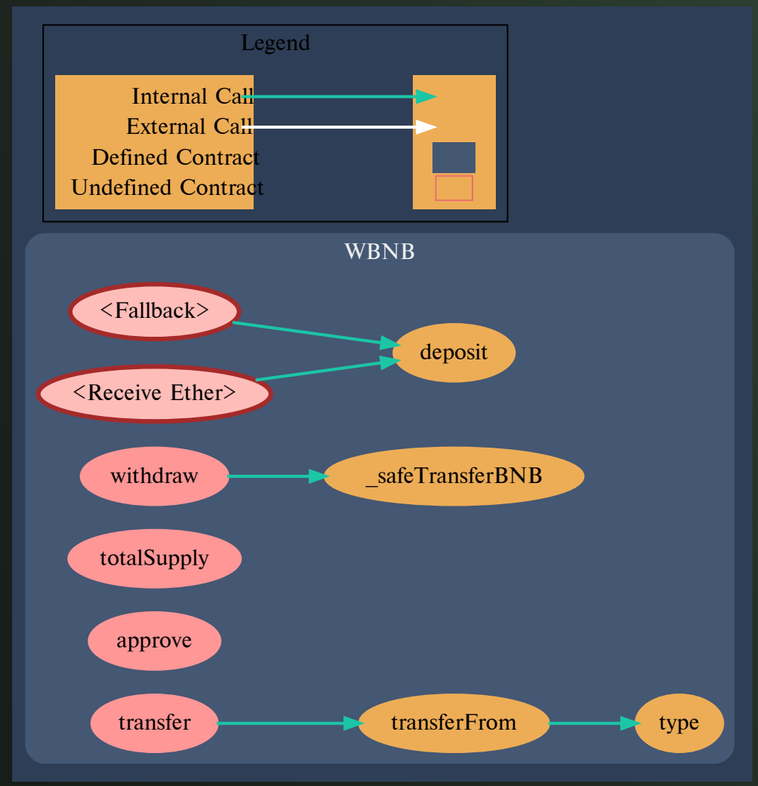
_safeTransferBNB()
Vulnerabilities not detected

totalSupply()
Vulnerabilities not detected

approve()
Vulnerabilities not detected

transfer()
Vulnerabilities not detected

transferFrom()
Vulnerabilities not detected



Pic. 5.2.
WBNB.sol

STRUCTURE OF CONTRACT WBNBGATEWAY.SOL

Contract methods analysis

depositBNB()
Vulnerabilities not detected

depositStakeBNB()
Vulnerabilities not detected

withdrawBNB()
Vulnerabilities not detected

repayBNB()
Vulnerabilities not detected

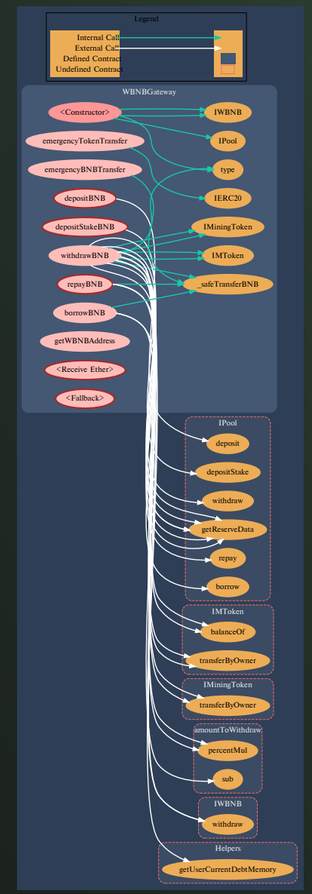
borrowBNB()
Vulnerabilities not detected

_safeTransferBNB(
Vulnerabilities not detected

emergencyTokenTransfer()
Vulnerabilities not detected

emergencyBNBTransfer()
Vulnerabilities not detected

getWBNBAddress()
Vulnerabilities not detected

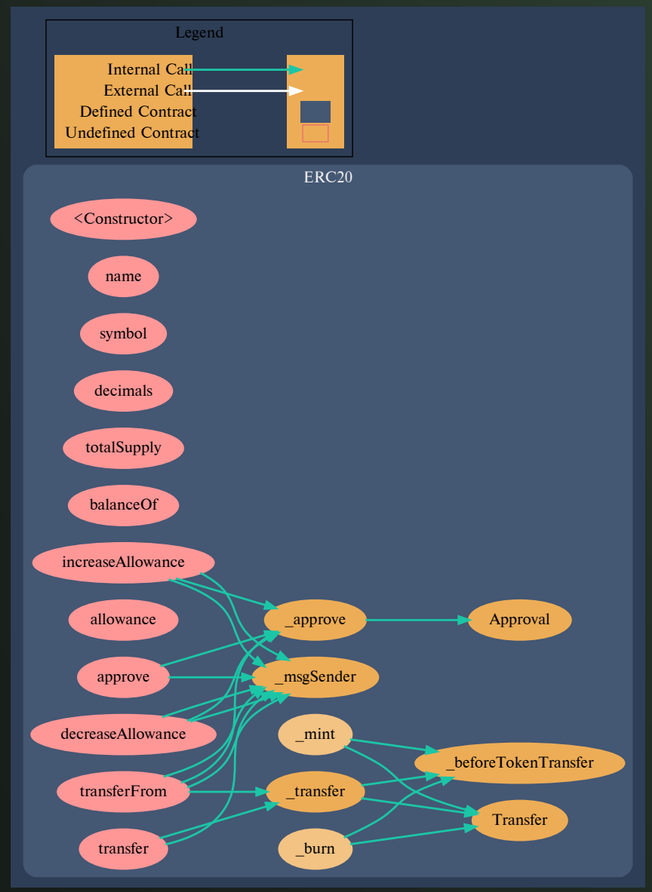


Pic. 5.3.
WBNBGateway.sol

STRUCTURE OF CONTRACT
BEP20.SOL

Contract methods analysis

Vulnerabilities not detected

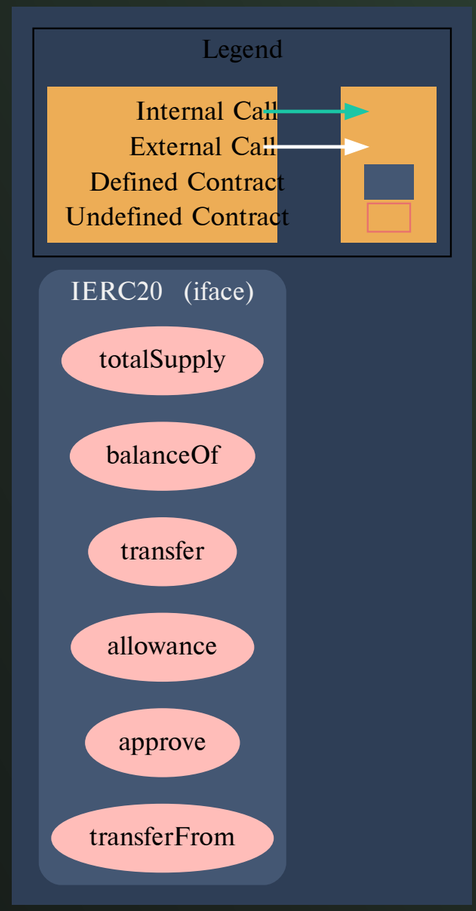


Pic. 5.4.
BEP20.sol

STRUCTURE OF CONTRACT
IBEP20.SOL

Contract methods analysis

Vulnerabilities not detected

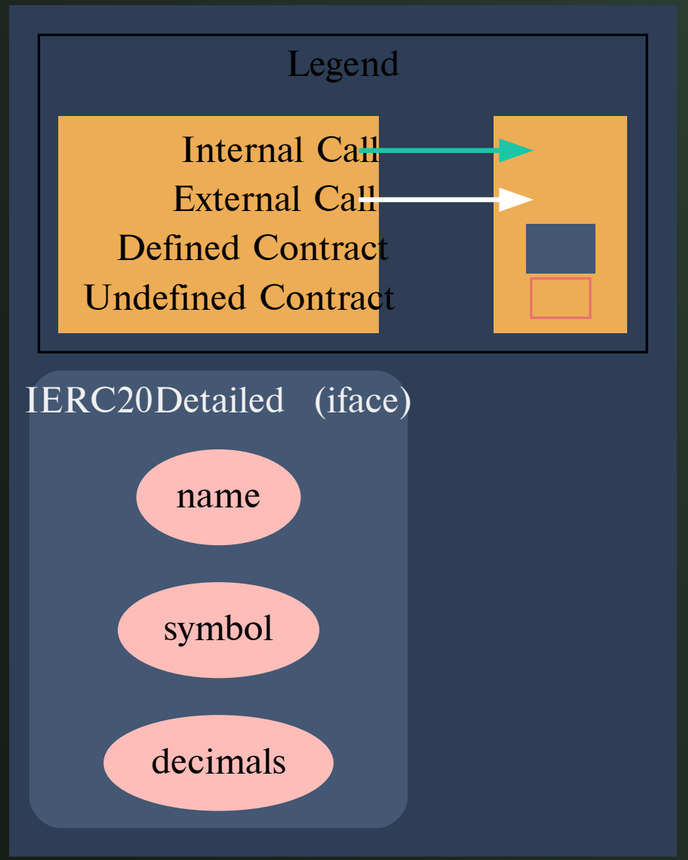


Pic. 5.5.
IBEP20.sol

STRUCTURE OF CONTRACT
IBEP20DETAILED.SOL

Contract methods analysis

Vulnerabilities not detected

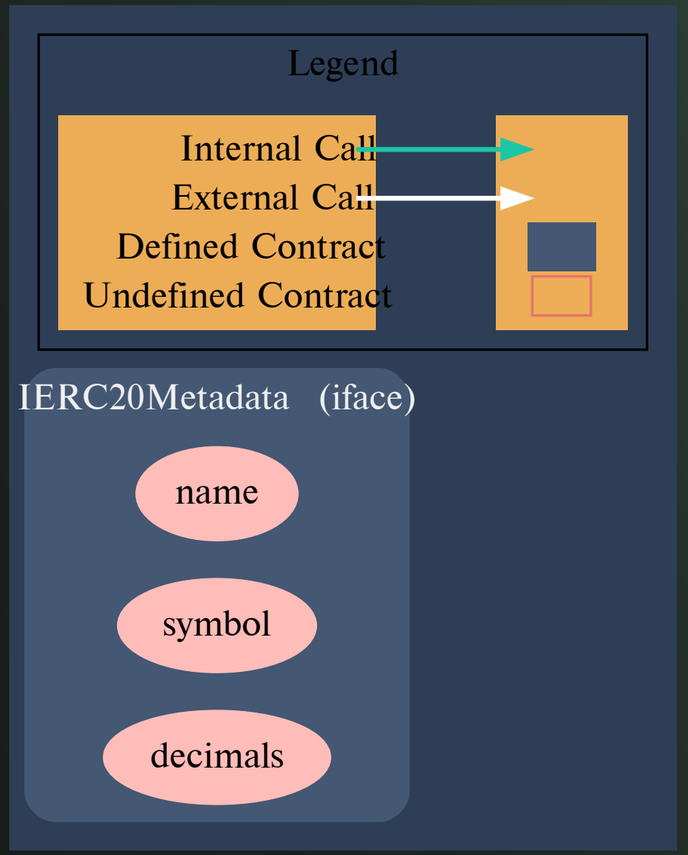


Pic. 5.6.
IBEP20Detailed.sol

STRUCTURE OF CONTRACT
IBEP20METADATA.SOL

Contract methods analysis

Vulnerabilities not detected

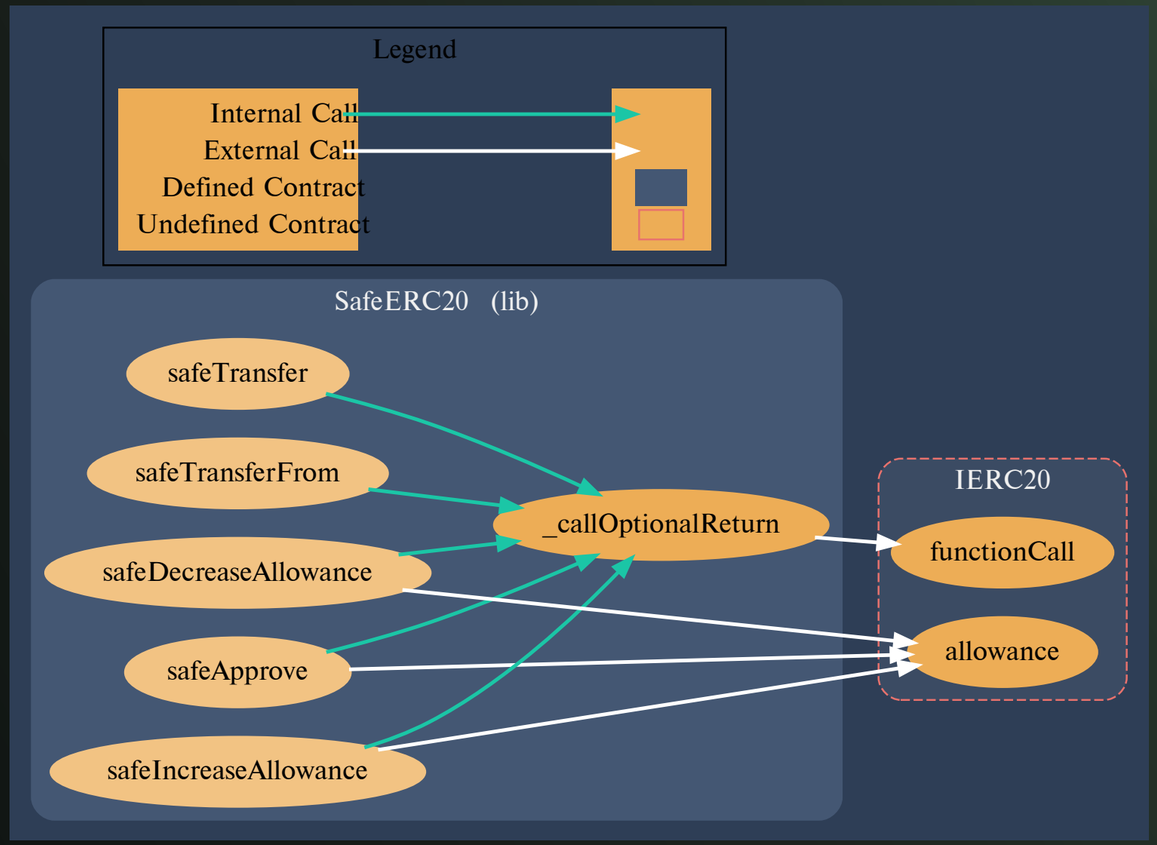


Pic. 5.7.
IBEP20Metadata.sol

STRUCTURE OF CONTRACT
SAFEBEP20.SOL

Contract methods analysis

Vulnerabilities not detected



Pic. 5.8.
SafeBEP20.sol

GET IN TOUCH

info@smartstate.tech
smartstate.tech