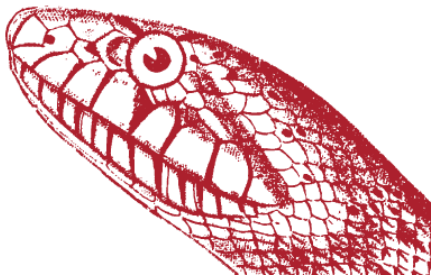
SLITHER

Drip Network Technical Audit



SLITHER

Drip Network Technical Audit

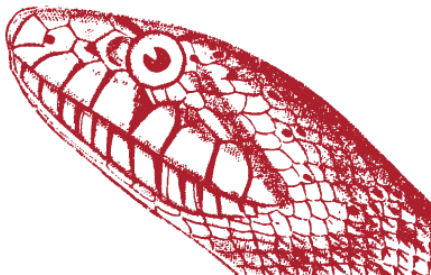
SUMMARY

DRIP NETWORK IS THE FIRST EVER DEFLATIONARY DAILY ROI PLATFORM DEVELOPED BY FOREX_SHARK, BB AND TEAM.

THE DRIP PLATFORM INCLUDES A SWAP CONTACT (BNB/DRIP DEX), A STAKING CONTRACT (THE FAUCET) AND A LIQUIDITY CONTRACT (RESERVOIR).

THE HIGHLIGHTS OF THE PLATFORM INCLUDE:

- NATIVE (AND PANCAKESWAP) LIQUIDITY
- A COMPOUNDABLE 1% DAILY RETURN ON INVESTMENT UP TO 365%
- DEFLATIONARY REWARD SYSTEM
- A FULL TEAM BUILDING REFERRAL SYSTEM
- TEAM AIRDROP MECHANICS
- WHALE TAX

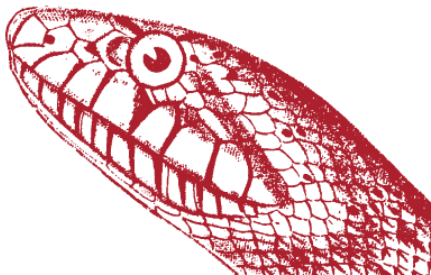


SLITHER

Drip Network Technical Audit

RESULTS

Vulnerability Category	Notes	Result
Arbitrary Storage Write	N/A	PASS
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Integer Over/Underflow	N/A	PASS
Multiple Sends	N/A	PASS
Suicide	N/A	PASS
State Change External Calls	N/A	PASS
Unchecked Retval	N/A	PASS
User Supplied Assertion	N/A	PASS
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety		**PASS**



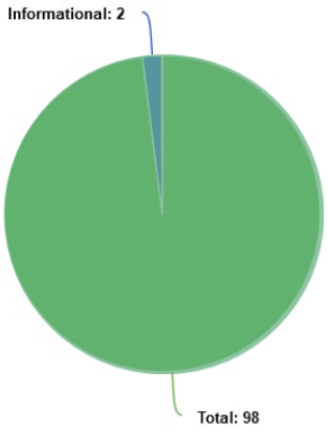
SLITHER

Drip Network Technical Audit

RESULTS

Issues | Risk Summary

	FOUND	RESOLVED	PARTIALLY RESOLVED	ACKNOWLEDGED (NO CHANGE MADE)
High	-	-	-	-
Medium	-	-	-	-
Low	-	-	-	-
Informational	2	-	-	2
Total	2	-	-	2



ISSUE CLARIFICATION

ISSUE 1:

```
DRIPTOKEN.SETACCOUNTCUSTOMTAX(ADDRESS,UINT8) (CONTRACTS/DRIPTOKEN.SOL#553-557) CONTAINS A
TAUTOLOGY OR CONTRADICTION:
        - REQUIRE(BOOL,STRING)(TAXRATE >= 0 && TAXRATE <= 100,INVALID TAX AMOUNT)
          (CONTRACTS/DRIPTOKEN.SOL#554)
```

EXPLANATION:

THIS WARNING HAS NO IMPACT ON THE FUNCTIONALITY OR POSSIBLE UNDESIRED CONTRACT STATE.

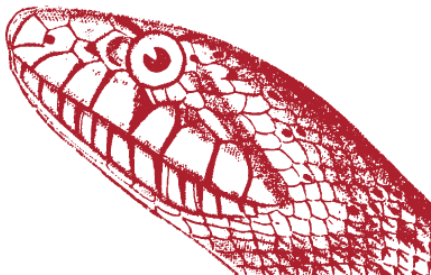
STATEMENT 'TAXRATE >= 0' WILL ALWAYS RESULT IN TRUE.

ISSUE 2:

```
DRIPTOKEN.SETVAULTADDRESS(ADDRESS)._NEWVAULTADDRESS (CONTRACTS/DRIPTOKEN.SOL#404) LACKS A
ZERO-CHECK ON:
                - VAULTADDRESS = _NEWVAULTADDRESS (CONTRACTS/DRIPTOKEN.SOL#405)
```

EXPLANATION:

THIS WARNING HAS NO IMPACT SINCE THE VAULT ADDRESS CAN BE UPDATED WITH SUBSEQUENT FUNCTION CALLS.



CONTRACT: FUNCTION GRAPH

DripToken

Public Functions:
- setVaultAddress(address)
- mint(address,uint256)
- finishMinting()
- transferFrom(address,address,uint256)
- transfer(address,uint256)
- calculateTransferTaxes(address,uint256)
- remainingMintableSupply()
- cap()
- mintedSupply()
- statsOf(address)
- mintedBy(address)
- setAccountCustomTax(address,uint8)
- removeAccountCustomTax(address)
- excludeAccount(address)
- includeAccount(address)
- isExcluded(address)

Private Functions:
- calculateTransactionTax(uint256,uint8)

Public Variables:
- name
- symbol
- decimals
- MAX_INT
- targetSupply
- totalTxs
- players
- vaultAddress

Private Variables:
- mintedSupply_
- stats
- taxDefault
- _customTaxRate
- _hasCustomTax
- _isExcluded
- _excluded

SafeMath

Private Functions:
- mul(uint256,uint256)
- div(uint256,uint256)
- sub(uint256,uint256)
- add(uint256,uint256)

MintableToken

Public Functions:
- mint(address,uint256)
- finishMinting()

Modifiers:
- canMint()

Public Variables:
- mintingFinished

Whitelist

Public Functions:
- addAddressToWhitelist(address)
- addAddressesToWhitelist(address[])
- removeAddressFromWhitelist(address)
- removeAddressesFromWhitelist(address[])

Modifiers:
- onlyWhitelisted()

Public Variables:
- whitelist

Ownable

Public Functions:
- transferOwnership(address)

Modifiers:
- onlyOwner()

Public Variables:
- owner

StandardToken

Public Functions:
- transferFrom(address,address,uint256)
- approve(address,uint256)
- allowance(address,address)
- increaseApproval(address,uint256)
- decreaseApproval(address,uint256)

Private Variables:
- allowed

'totalSupply()' collides in inherited contracts BEP20Basic, BasicToken where BasicToken is chosen. 'balanceOf(address)' collides in inherited contracts BEP20Basic, BasicToken where BasicToken is chosen. 'transfer(address,uint256)' collides in inherited contracts BEP20Basic, BasicToken where BasicToken is chosen.

BEP20

Public Functions:
- allowance(address,address)
- transferFrom(address,address,uint256)
- approve(address,uint256)

BasicToken

Public Functions:
- totalSupply()
- transfer(address,uint256)
- balanceOf(address)

Private Variables:
- balances
- totalSupply_

BEP20Basic

Public Functions:
- totalSupply()
- balanceOf(address)
- transfer(address,uint256)

CONTRACT: FUNCTION SUMMARY

CONTRACT OWNABLE
CONTRACT VARS: ['OWNER']
INHERITANCE:: []

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
CONSTRUCTOR()	PUBLIC	[]	['MSG.SENDER']	['OWNER']	[]	[]
TRANSFEROWNERSHIP(ADDRESS)	PUBLIC	['ONLYOWNER']	['OWNER']	['OWNER']	['ONLYOWNER', 'REQUIRE(BOOL)']	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
ONLYOWNER()	INTERNAL	['OWNER', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]

CONTRACT WHITELIST
CONTRACT VARS: ['OWNER', 'WHITELIST']
INHERITANCE:: ['OWNABLE']

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
CONSTRUCTOR()	PUBLIC	[]	['MSG.SENDER']	['OWNER']	[]	[]
TRANSFEROWNERSHIP(ADDRESS)	PUBLIC	['ONLYOWNER']	['OWNER']	['OWNER']	['ONLYOWNER', 'REQUIRE(BOOL)']	[]
ADDADDRESSTOWHITELIST(ADDRESS)	PUBLIC	['ONLYOWNER']	['WHITELIST']	['WHITELIST']	['ONLYOWNER']	[]
ADDADDRESSESTOWHITELIST(ADDRESS[])	PUBLIC	['ONLYOWNER']	[]	[]	['ADDADDRESSTOWHITELIST', 'ONLYOWNER']	[]
REMOVEADDRESSFROMWHITELIST(ADDRESS)	PUBLIC	['ONLYOWNER']	['WHITELIST']	['WHITELIST']	['ONLYOWNER']	[]
REMOVEADDRESSESFROMWHITELIST(ADDRESS[])	PUBLIC	['ONLYOWNER']	[]	[]	['REMOVEADDRESSFROMWHITELIST', 'ONLYOWNER']	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
ONLYOWNER()	INTERNAL	['OWNER', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]
ONLYWHITELISTED()	INTERNAL	['WHITELIST', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]

CONTRACT: FUNCTION SUMMARY

CONTRACT SAFEMATH
CONTRACT VARS: []
INHERITANCE:: []

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
MUL(UINT256,UINT256)	INTERNAL	[]	[]	[]	['ASSERT(BOOL)']	[]
DIV(UINT256,UINT256)	INTERNAL	[]	[]	[]	[]	[]
SUB(UINT256,UINT256)	INTERNAL	[]	[]	[]	['ASSERT(BOOL)']	[]
ADD(UINT256,UINT256)	INTERNAL	[]	[]	[]	['ASSERT(BOOL)']	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS

CONTRACT BEP20BASIC
CONTRACT VARS: []
INHERITANCE:: []

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
TOTALSUPPLY()	EXTERNAL	[]	[]	[]	[]	[]
BALANCEOF(ADDRESS)	EXTERNAL	[]	[]	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	EXTERNAL	[]	[]	[]	[]	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS

CONTRACT: FUNCTION SUMMARY

CONTRACT BASICTOKEN
CONTRACT VARS: ['BALANCES', 'TOTALSUPPLY_']
INHERITANCE:: ['BEP20BASIC']

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
TOTALSUPPLY()	EXTERNAL	[]	[]	[]	[]	[]
BALANCEOF(ADDRESS)	EXTERNAL	[]	[]	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	EXTERNAL	[]	[]	[]	[]	[]
TOTALSUPPLY()	PUBLIC	[]	['TOTALSUPPLY_']	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	PUBLIC	[]	['BALANCES', 'MSG.SENDER']	['BALANCES']	['REQUIRE(BOOL)']	['BALANCES[_TO].ADD(_VALUE)', 'BALANCES[MSG.SENDER].SUB(_VALUE)']
BALANCEOF(ADDRESS)	PUBLIC	[]	['BALANCES']	[]	[]	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS

CONTRACT BEP20
CONTRACT VARS: []
INHERITANCE:: ['BEP20BASIC']

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
TOTALSUPPLY()	EXTERNAL	[]	[]	[]	[]	[]
BALANCEOF(ADDRESS)	EXTERNAL	[]	[]	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	EXTERNAL	[]	[]	[]	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	[]	[]	[]	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS

CONTRACT: FUNCTION SUMMARY

CONTRACT STANDARDTOKEN
CONTRACT VARS: ['BALANCES', 'TOTALSUPPLY_', 'ALLOWED']
INHERITANCE:: ['BASICTOKEN', 'BEP20', 'BEP20BASIC']

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
TOTALSUPPLY()	PUBLIC	[]	['TOTALSUPPLY_']	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	PUBLIC	[]	['BALANCES', 'MSG.SENDER']	['BALANCES']	['REQUIRE(BOOL)']	['BALANCES[_TO].ADD(_VALUE)', 'BALANCES[MSG.SENDER].SUB(_VALUE)']
BALANCEOF(ADDRESS)	PUBLIC	[]	['BALANCES']	[]	[]	[]
TOTALSUPPLY()	EXTERNAL	[]	[]	[]	[]	[]
BALANCEOF(ADDRESS)	EXTERNAL	[]	[]	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	EXTERNAL	[]	[]	[]	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	[]	[]	[]	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'BALANCES']	['ALLOWED', 'BALANCES']	['REQUIRE(BOOL)']	['ALLOWED[_FROM][MSG.SENDER].SUB(_VALUE)', 'BALANCES[_TO].ADD(_VALUE)']
			['MSG.SENDER']			['BALANCES[_FROM].SUB(_VALUE)']
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	['MSG.SENDER']	['ALLOWED']	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	['ALLOWED']	[]	[]	[]
INCREASEAPPROVAL(ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'MSG.SENDER']	['ALLOWED']	[]	['ALLOWED[MSG.SENDER][_SPENDER].ADD(_ADDEDVALUE)']
DECREASEAPPROVAL(ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'MSG.SENDER']	['ALLOWED']	[]	['OLDVALUE.SUB(_SUBTRACTEDVALUE)']

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS

CONTRACT: FUNCTION SUMMARY

CONTRACT MINTABLETOKEN
CONTRACT VARS: ['BALANCES', 'TOTALSUPPLY_', 'ALLOWED', 'OWNER', 'WHITELIST', 'MINTINGFINISHED']
INHERITANCE:: ['WHITELIST', 'OWNABLE', 'STANDARDTOKEN', 'BASICTOKEN', 'BEP20', 'BEP20BASIC']

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
ADDADDRESSTOWHITELIST(ADDRESS)	PUBLIC	['ONLYOWNER']	['WHITELIST']	['WHITELIST']	['ONLYOWNER']	[]
ADDADDRESSESTOWHITELIST(ADDRESS[])	PUBLIC	['ONLYOWNER']	[]	[]	['ADDADDRESSTOWHITELIST', 'ONLYOWNER']	[]
REMOVEADDRESSFROMWHITELIST(ADDRESS)	PUBLIC	['ONLYOWNER']	['WHITELIST']	['WHITELIST']	['ONLYOWNER']	[]
REMOVEADDRESSESFROMWHITELIST(ADDRESS[])	PUBLIC	['ONLYOWNER']	[]	[]	['REMOVEADDRESSFROMWHITELIST', 'ONLYOWNER']	[]
CONSTRUCTOR()	PUBLIC	[]	['MSG.SENDER']	['OWNER']	[]	[]
TRANSFEROWNERSHIP(ADDRESS)	PUBLIC	['ONLYOWNER']	['OWNER']	['OWNER']	['ONLYOWNER', 'REQUIRE(BOOL)']	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'BALANCES'] ['MSG.SENDER']	['ALLOWED', 'BALANCES']	['REQUIRE(BOOL)']	['ALLOWED[_FROM][MSG.SENDER].SUB(_VALUE)', 'BALANCES[_TO].ADD(_VALUE)'] ['BALANCES[_FROM].SUB(_VALUE)']
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	['MSG.SENDER']	['ALLOWED']	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	['ALLOWED']	[]	[]	[]
INCREASEAPPROVAL(ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'MSG.SENDER']	['ALLOWED']	[]	['ALLOWED[MSG.SENDER][_SPENDER].ADD(_ADDEDVALUE)']
DECREASEAPPROVAL(ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'MSG.SENDER']	['ALLOWED']	[]	['OLDVALUE.SUB(_SUBTRACTEDVALUE)']
TOTALSUPPLY()	PUBLIC	[]	['TOTALSUPPLY_']	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	PUBLIC	[]	['BALANCES', 'MSG.SENDER']	['BALANCES']	['REQUIRE(BOOL)']	['BALANCES[MSG.SENDER].SUB(_VALUE)', 'BALANCES[_TO].ADD(_VALUE)']
BALANCEOF(ADDRESS)	PUBLIC	[]	['BALANCES']	[]	[]	[]
TOTALSUPPLY()	EXTERNAL	[]	[]	[]	[]	[]
BALANCEOF(ADDRESS)	EXTERNAL	[]	[]	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	EXTERNAL	[]	[]	[]	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	[]	[]	[]	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
MINT(ADDRESS,UINT256)	PUBLIC	['ONLYWHITELISTED', 'CANMINT']	['BALANCES', 'TOTALSUPPLY_']	['BALANCES', 'TOTALSUPPLY_']	['ONLYWHITELISTED', 'CANMINT'] ['REQUIRE(BOOL)']	['BALANCES[_TO].ADD(_AMOUNT)', 'TOTALSUPPLY_.ADD(_AMOUNT)']
FINISHMINTING()	PUBLIC	['ONLYWHITELISTED', 'CANMINT']	[]	['MINTINGFINISHED']	['ONLYWHITELISTED', 'CANMINT']	[]
SLITHERCONSTRUCTORVARIABLES()	INTERNAL	[]	[]	['MINTINGFINISHED']	[]	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
ONLYWHITELISTED()	INTERNAL	['WHITELIST', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]
ONLYOWNER()	INTERNAL	['OWNER', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]
CANMINT()	INTERNAL	['MINTINGFINISHED']	[]	['REQUIRE(BOOL)']	[]

INFO:SLITHER:./CONTRACTS/DRIPTOKEN.SOL ANALYZED (9 CONTRACTS)

CONTRACT: FUNCTION SUMMARY

```
CONTRACT DRIPTOKEN
CONTRACT VARS: ['BALANCES', 'TOTALSUPPLY_', 'ALLOWED', 'OWNER', 'WHITELIST', 'MINTINGFINISHED', 'NAME', 'SYMBOL', 'DECIMALS', 'MAX_INT', 'TARGETSUPPLY', 'TOTALTXS', 'PLAYERS', 'MINTEDSUPPLY_', 'STATS',
'VAULTADDRESS', 'TAXDEFAULT', '_CUSTOMTAXRATE', '_HASCUSTOMTAX', '_ISEXCLUDED', '_EXCLUDED']
INHERITANCE:: ['MINTABLETOKEN', 'WHITELIST', 'OWNABLE', 'STANDARDTOKEN', 'BASICTOKEN', 'BEP20', 'BEP20BASIC']
```

FUNCTION	VISIBILITY	MODIFIERS	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
MINT(ADDRESS,UINT256)	PUBLIC	['ONLYWHITELISTED', 'CANMINT']	['BALANCES', 'TOTALSUPPLY_']	['BALANCES', 'TOTALSUPPLY_']	['CANMINT', 'ONLYWHITELISTED'] ['REQUIRE(BOOL)']	['TOTALSUPPLY_.ADD(_AMOUNT)', 'BALANCES[_TO].ADD(_AMOUNT)']
FINISHMINTING()	PUBLIC	['ONLYWHITELISTED', 'CANMINT']	[]	['MINTINGFINISHED']	['CANMINT', 'ONLYWHITELISTED']	[]
ADDADDRESSTOWHITELIST(ADDRESS)	PUBLIC	['ONLYOWNER']	['WHITELIST']	['WHITELIST']	['ONLYOWNER']	[]
ADDADDRESSESTOWHITELIST(ADDRESS[])	PUBLIC	['ONLYOWNER']	[]	[]	['ADDADDRESSTOWHITELIST', 'ONLYOWNER']	[]
REMOVEADDRESSFROMWHITELIST(ADDRESS)	PUBLIC	['ONLYOWNER']	['WHITELIST']	['WHITELIST']	['ONLYOWNER']	[]
REMOVEADDRESSESFROMWHITELIST(ADDRESS[])	PUBLIC	['ONLYOWNER']	[]	[]	['ONLYOWNER', 'REMOVEADDRESSFROMWHITELIST']	[]
CONSTRUCTOR()	PUBLIC	[]	['MSG.SENDER']	['OWNER']	[]	[]
TRANSFEROWNERSHIP(ADDRESS)	PUBLIC	['ONLYOWNER']	['OWNER']	['OWNER']	['ONLYOWNER', 'REQUIRE(BOOL)']	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'BALANCES'] ['MSG.SENDER']	['ALLOWED', 'BALANCES']	['REQUIRE(BOOL)']	['BALANCES[_TO].ADD(_VALUE)', 'BALANCES[_FROM].SUB(_VALUE)'] ['ALLOWED[_FROM][MSG.SENDER].SUB(_VALUE)']
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	['MSG.SENDER']	['ALLOWED']	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	['ALLOWED']	[]	[]	[]
INCREASEAPPROVAL(ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'MSG.SENDER']	['ALLOWED']	[]	['ALLOWED[MSG.SENDER][_SPENDER].ADD(_ADDEDVALUE)']
DECREASEAPPROVAL(ADDRESS,UINT256)	PUBLIC	[]	['ALLOWED', 'MSG.SENDER']	['ALLOWED']	[]	['OLDVALUE.SUB(_SUBTRACTEDVALUE)']
TOTALSUPPLY()	PUBLIC	[]	['TOTALSUPPLY_']	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	PUBLIC	[]	['BALANCES', 'MSG.SENDER']	['BALANCES']	['REQUIRE(BOOL)']	['BALANCES[MSG.SENDER].SUB(_VALUE)', 'BALANCES[_TO].ADD(_VALUE)']
BALANCEOF(ADDRESS)	PUBLIC	[]	['BALANCES']	[]	[]	[]
TOTALSUPPLY()	EXTERNAL	[]	[]	[]	[]	[]
BALANCEOF(ADDRESS)	EXTERNAL	[]	[]	[]	[]	[]
TRANSFER(ADDRESS,UINT256)	EXTERNAL	[]	[]	[]	[]	[]
ALLOWANCE(ADDRESS,ADDRESS)	PUBLIC	[]	[]	[]	[]	[]
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
APPROVE(ADDRESS,UINT256)	PUBLIC	[]	[]	[]	[]	[]
CONSTRUCTOR(UINT256)	PUBLIC	[]	['OWNER']	[]	['ADDADDRESSTOWHITELIST', 'MINT'] ['', 'REMOVEADDRESSFROMWHITELIST'] ['ONLYOWNER']	[]
SETVAULTADDRESS(ADDRESS)	PUBLIC	['ONLYOWNER']	[]	['VAULTADDRESS']	['ONLYOWNER']	[]
MINT(ADDRESS,UINT256)	PUBLIC	[]	['MINTEDSUPPLY_', 'PLAYERS'] ['STATS', 'TARGETSUPPLY'] ['TOTALTXS']	['MINTEDSUPPLY_', 'MINTINGFINISHED'] ['PLAYERS', 'STATS'] ['TOTALTXS']	['MINT']	['MINTEDSUPPLY_.ADD(_AMOUNT)', 'MINTEDSUPPLY_.ADD(_AMOUNT)']
FINISHMINTING()	PUBLIC	['ONLYOWNER', 'CANMINT']	[]	[]	['CANMINT', 'ONLYOWNER']	[]
CALCULATETRANSACTIONTAX(UINT256,UINT8)	INTERNAL	[]	[]	[]	[]	['_VALUE.MUL(SAFEMATH.SUB(100,_TAX)).DIV(100)', '_VALUE.MUL(_TAX)'] ['_VALUE.MUL(SAFEMATH.SUB(100,_TAX))', '_VALUE.MUL(_TAX).DIV(100)'] ['SAFEMATH.SUB(100,_TAX)']
TRANSFERFROM(ADDRESS,ADDRESS,UINT256)	PUBLIC	[]	['PLAYERS', 'STATS'] ['TOTALTXS', 'VAULTADDRESS']	['PLAYERS', 'STATS'] ['TOTALTXS']	['CALCULATETRANSFERTAXES', 'REQUIRE(BOOL)'] ['TRANSFERFROM']	[]
TRANSFER(ADDRESS,UINT256)	PUBLIC	[]	['PLAYERS', 'STATS'] ['TOTALTXS', 'VAULTADDRESS'] ['MSG.SENDER']	['PLAYERS', 'STATS'] ['TOTALTXS']	['CALCULATETRANSFERTAXES', 'TRANSFER'] ['REQUIRE(BOOL)']	[]
CALCULATETRANSFERTAXES(ADDRESS,UINT256)	PUBLIC	[]	['_CUSTOMTAXRATE', '_HASCUSTOMTAX'] ['_ISEXCLUDED', 'TAXDEFAULT']	[]	['CALCULATETRANSACTIONTAX']	[]
REMAININGMINTABLESUPPLY()	PUBLIC	[]	['MINTEDSUPPLY_', 'TARGETSUPPLY']	[]	[]	['TARGETSUPPLY.SUB(MINTEDSUPPLY_)']
CAP()	PUBLIC	[]	['TARGETSUPPLY']	[]	[]	[]
MINTEDSUPPLY()	PUBLIC	[]	['MINTEDSUPPLY_']	[]	[]	[]
STATSOF(ADDRESS)	PUBLIC	[]	['STATS']	[]	['BALANCEOF']	[]
MINTEDBY(ADDRESS)	PUBLIC	[]	['STATS']	[]	[]	[]
SETACCOUNTCUSTOMTAX(ADDRESS,UINT8)	EXTERNAL	['ONLYOWNER']	[]	['_CUSTOMTAXRATE', '_HASCUSTOMTAX']	['REQUIRE(BOOL,STRING)', 'ONLYOWNER']	[]
REMOVEACCOUNTCUSTOMTAX(ADDRESS)	EXTERNAL	['ONLYOWNER']	[]	['_HASCUSTOMTAX']	['ONLYOWNER']	[]
EXCLUDEACCOUNT(ADDRESS)	EXTERNAL	['ONLYOWNER']	['_EXCLUDED', '_ISEXCLUDED']	['_EXCLUDED', '_ISEXCLUDED']	['REQUIRE(BOOL,STRING)', 'ONLYOWNER']	['_EXCLUDED.PUSH(ACCOUNT)']
INCLUDEACCOUNT(ADDRESS)	EXTERNAL	['ONLYOWNER']	['_EXCLUDED', '_ISEXCLUDED']	['_EXCLUDED', '_ISEXCLUDED']	['REQUIRE(BOOL,STRING)', 'ONLYOWNER']	[]
ISEXCLUDED(ADDRESS)	PUBLIC	[]	['_ISEXCLUDED']	[]	[]	[]
SLITHERCONSTRUCTORVARIABLES()	INTERNAL	[]	[]	['MINTINGFINISHED']	[]	[]
SLITHERCONSTRUCTORCONSTANTVARIABLES()	INTERNAL	[]	['MAX_INT']	['MAX_INT', 'DECIMALS'] ['NAME', 'SYMBOL'] ['TARGETSUPPLY', 'TAXDEFAULT']	[]	[]

MODIFIERS	VISIBILITY	READ	WRITE	INTERNAL CALLS	EXTERNAL CALLS
CANMINT()	INTERNAL	['MINTINGFINISHED']	[]	['REQUIRE(BOOL)']	[]
ONLYWHITELISTED()	INTERNAL	['WHITELIST', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]
ONLYOWNER()	INTERNAL	['OWNER', 'MSG.SENDER']	[]	['REQUIRE(BOOL,STRING)']	[]

```
INFO:SLITHER:./CONTRACTS/DRIPTOKEN.SOL ANALYZED (9 CONTRACTS)
```

SLITHER

Drip Network Technical Audit

DRIP CONTRACT: CONTRACT SUMMARY

+ Contract Ownable
- From Ownable
- constructor() (public)
- transferOwnership(address) (public)

+ Contract Whitelist
- From Ownable
- constructor() (public)
- transferOwnership(address) (public)
- From Whitelist
- addAddressToWhitelist(address) (public)
- addAddressesToWhitelist(address[]) (public)
- removeAddressFromWhitelist(address) (public)
- removeAddressesFromWhitelist(address[]) (public)

+ Contract SafeMath (Most derived contract)
- From SafeMath
- add(uint256,uint256) (internal)
- div(uint256,uint256) (internal)
- mul(uint256,uint256) (internal)
- sub(uint256,uint256) (internal)

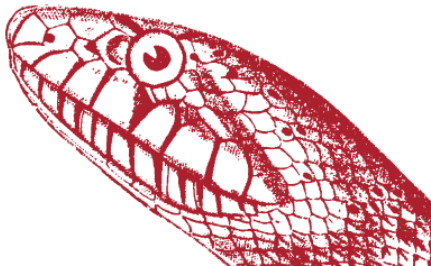
+ Contract BEP20Basic
- From BEP20Basic
- balanceOf(address) (external)
- totalSupply() (external)
- transfer(address,uint256) (external)

+ Contract BasicToken
- From BasicToken
- balanceOf(address) (public)
- totalSupply() (public)
- transfer(address,uint256) (public)

+ Contract BEP20
- From BEP20Basic
- balanceOf(address) (external)
- totalSupply() (external)
- transfer(address,uint256) (external)
- From BEP20
- allowance(address,address) (public)
- approve(address,uint256) (public)
- transferFrom(address,address,uint256) (public)

+ Contract DripToken (Most derived contract)
- From Whitelist
- addAddressToWhitelist(address) (public)
- addAddressesToWhitelist(address[]) (public)
- removeAddressFromWhitelist(address) (public)
- removeAddressesFromWhitelist(address[]) (public)
- From Ownable
- constructor() (public)
- transferOwnership(address) (public)
- From StandardToken
- allowance(address,address) (public)
- approve(address,uint256) (public)
- decreaseApproval(address,uint256) (public)
- increaseApproval(address,uint256) (public)
- From BasicToken
- balanceOf(address) (public)
- totalSupply() (public)
- From DripToken
- calculateTransactionTax(uint256,uint8) (internal)
- calculateTransferTaxes(address,uint256) (public)
- cap() (public)
- constructor(uint256) (public)
- excludeAccount(address) (external)
- finishMinting() (public)
- includeAccount(address) (external)
- isExcluded(address) (public)
- mint(address,uint256) (public)
- mintedBy(address) (public)
- mintedSupply() (public)
- remainingMintableSupply() (public)
- removeAccountCustomTax(address) (external)
- setAccountCustomTax(address,uint8) (external)
- setVaultAddress(address) (public)
- statsOf(address) (public)
- transfer(address,uint256) (public)
- transferFrom(address,address,uint256) (public)

INFO:Slither:./contracts/dripToken.sol analyzed (9 contracts)

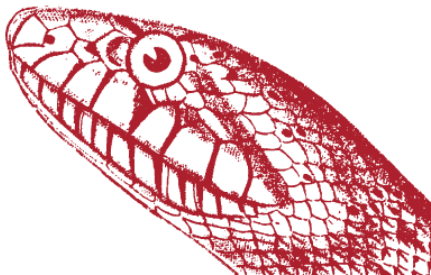


SLITHER

Drip Network Technical Audit

DRIP CONTRACT: CONTRACT SUMMARY

```
Number of lines: 584 (+ 0 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 9 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 16
Number of informational issues: 32
Number of low issues: 1
Number of medium issues: 1
Number of high issues: 0

ERCs: ERC20

+-----------+-------------+-------+--------------+--------------+----------+
|    Name   | # functions |  ERCS |  ERC20 info  | Complex code | Features |
+-----------+-------------+-------+--------------+--------------+----------+
|  SafeMath |      4      |       | Deflationary |      No      |          |
| DripToken |      42     | ERC20 |   Staking    |      No      |          |
|           |             |       |    Token     |              |          |
+-----------+-------------+-------+--------------+--------------+----------+
INFO:Slither:./contracts/dripToken.sol analyzed (9 contracts)
```



SLITHER

Drip Network Technical Audit

DRIP CONTRACT: CONTRACT SUMMARY

Child_Contract -> Immediate_Base_Contracts [Not_Immediate_Base_Contracts]
+ Ownable

+ Whitelist
 -> Ownable

+ SafeMath

+ BEP20Basic

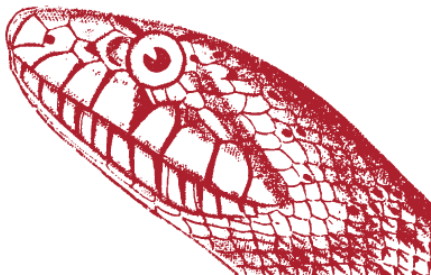
+ BasicToken
 -> BEP20Basic

+ BEP20
 -> BEP20Basic

+ StandardToken
 -> BEP20, BasicToken
, [BEP20Basic]

+ MintableToken
 -> StandardToken, Whitelist
, [Ownable, BasicToken, BEP20, BEP20Basic]

+ DripToken
 -> MintableToken
, [Whitelist, Ownable, StandardToken, BasicToken, BEP20, BEP20Basic]

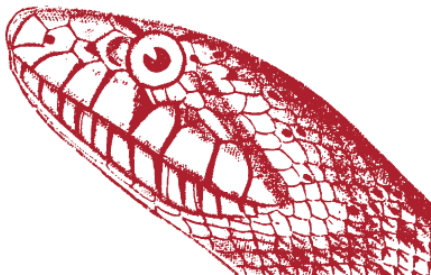


SLITHER

Drip Network Technical Audit

DRIP CONTRACT: CONTRACT SUMMARY

```
Base_Contract -> Immediate_Child_Contracts
 [Not_Immediate_Child_Contracts]

+ Ownable
 -> Whitelist
, [MintableToken, DripToken]

+ Whitelist
 -> MintableToken
, [DripToken]

+ SafeMath

+ BEP20Basic
 -> BasicToken, BEP20
, [StandardToken, MintableToken, DripToken]

+ BasicToken
 -> StandardToken
, [MintableToken, DripToken]

+ BEP20
 -> StandardToken
, [MintableToken, DripToken]

+ StandardToken
 -> MintableToken
, [DripToken]

+ MintableToken
 -> DripToken

+ DripToken

INFO:Slither:./contracts/dripToken.sol analyzed
(9 contracts)
```

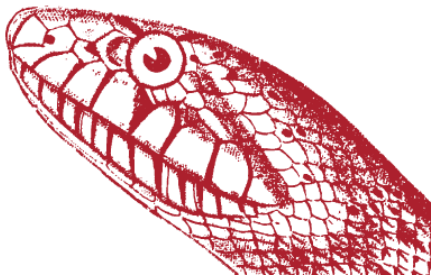


SLITHER

Drip Network Technical Audit

DRIP CONTRACT: CONTRACT SUMMARY

```
DripToken.setAccountCustomTax(address,uint8) (contracts/dripToken.sol#553-557) contains a tautology or contradiction:
        - require(bool,string)(taxRate >= 0 && taxRate <= 100,Invalid tax amount) (contracts/dripToken.sol#554)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#tautology-or-contradiction
INFO:Detectors:
DripToken.setVaultAddress(address)._newVaultAddress (contracts/dripToken.sol#404) lacks a zero-check on :
                - vaultAddress = _newVaultAddress (contracts/dripToken.sol#405)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Pragma version^0.4.25 (contracts/dripToken.sol#1) allows old versions
solc-0.4.25 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter BasicToken.transfer(address,uint256)._to (contracts/dripToken.sol#197) is not in mixedCase
Parameter BasicToken.transfer(address,uint256)._value (contracts/dripToken.sol#197) is not in mixedCase
Parameter BasicToken.balanceOf(address)._owner (contracts/dripToken.sol#212) is not in mixedCase
Parameter StandardToken.transferFrom(address,address,uint256)._from (contracts/dripToken.sol#248) is not in mixedCase
Parameter StandardToken.transferFrom(address,address,uint256)._to (contracts/dripToken.sol#248) is not in mixedCase
Parameter StandardToken.transferFrom(address,address,uint256)._value (contracts/dripToken.sol#248) is not in mixedCase
Parameter StandardToken.approve(address,uint256)._spender (contracts/dripToken.sol#270) is not in mixedCase
Parameter StandardToken.approve(address,uint256)._value (contracts/dripToken.sol#270) is not in mixedCase
Parameter StandardToken.allowance(address,address)._owner (contracts/dripToken.sol#282) is not in mixedCase
Parameter StandardToken.allowance(address,address)._spender (contracts/dripToken.sol#282) is not in mixedCase
Parameter StandardToken.increaseApproval(address,uint256)._spender (contracts/dripToken.sol#296) is not in mixedCase
Parameter StandardToken.increaseApproval(address,uint256)._addedValue (contracts/dripToken.sol#296) is not in mixedCase
Parameter StandardToken.decreaseApproval(address,uint256)._spender (contracts/dripToken.sol#312) is not in mixedCase
Parameter StandardToken.decreaseApproval(address,uint256)._subtractedValue (contracts/dripToken.sol#312) is not in mixedCase
Parameter MintableToken.mint(address,uint256)._to (contracts/dripToken.sol#347) is not in mixedCase
Parameter MintableToken.mint(address,uint256)._amount (contracts/dripToken.sol#347) is not in mixedCase
Parameter DripToken.setVaultAddress(address)._newVaultAddress (contracts/dripToken.sol#404) is not in mixedCase
Parameter DripToken.mint(address,uint256)._to (contracts/dripToken.sol#414) is not in mixedCase
Parameter DripToken.mint(address,uint256)._amount (contracts/dripToken.sol#414) is not in mixedCase
Parameter DripToken.calculateTransactionTax(uint256,uint8)._value (contracts/dripToken.sol#451) is not in mixedCase
Parameter DripToken.calculateTransactionTax(uint256,uint8)._tax (contracts/dripToken.sol#451) is not in mixedCase
Parameter DripToken.transferFrom(address,address,uint256)._from (contracts/dripToken.sol#458) is not in mixedCase
Parameter DripToken.transferFrom(address,address,uint256)._to (contracts/dripToken.sol#458) is not in mixedCase
Parameter DripToken.transferFrom(address,address,uint256)._value (contracts/dripToken.sol#458) is not in mixedCase
Parameter DripToken.transfer(address,uint256)._to (contracts/dripToken.sol#484) is not in mixedCase
Parameter DripToken.transfer(address,uint256)._value (contracts/dripToken.sol#484) is not in mixedCase
Parameter DripToken.calculateTransferTaxes(address,uint256)._from (contracts/dripToken.sol#507) is not in mixedCase
Parameter DripToken.calculateTransferTaxes(address,uint256)._value (contracts/dripToken.sol#507) is not in mixedCase
Constant DripToken.targetSupply (contracts/dripToken.sol#378) is not in UPPER_CASE_WITH_UNDERSCORES
```

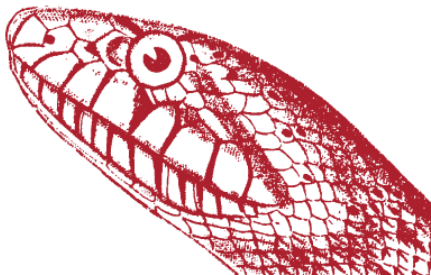


SLITHER

Drip Network Technical Audit

DRIP CONTRACT: CONTRACT SUMMARY

```
Constant DripToken.taxDefault (contracts/dripToken.sol#386) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (contracts/dripToken.sol#37-41)
addAddressesToWhitelist(address[]) should be declared external:
        - Whitelist.addAddressesToWhitelist(address[]) (contracts/dripToken.sol#78-84)
removeAddressesFromWhitelist(address[]) should be declared external:
        - Whitelist.removeAddressesFromWhitelist(address[]) (contracts/dripToken.sol#106-112)
totalSupply() should be declared external:
        - BasicToken.totalSupply() (contracts/dripToken.sol#188-190)
allowance(address,address) should be declared external:
        - BEP20.allowance(address,address) (contracts/dripToken.sol#223)
        - StandardToken.allowance(address,address) (contracts/dripToken.sol#282-284)
approve(address,uint256) should be declared external:
        - BEP20.approve(address,uint256) (contracts/dripToken.sol#227)
        - StandardToken.approve(address,uint256) (contracts/dripToken.sol#270-274)
increaseApproval(address,uint256) should be declared external:
        - StandardToken.increaseApproval(address,uint256) (contracts/dripToken.sol#296-300)
decreaseApproval(address,uint256) should be declared external:
        - StandardToken.decreaseApproval(address,uint256) (contracts/dripToken.sol#312-321)
finishMinting() should be declared external:
        - DripToken.finishMinting() (contracts/dripToken.sol#447-449)
        - MintableToken.finishMinting() (contracts/dripToken.sol#360-364)
setVaultAddress(address) should be declared external:
        - DripToken.setVaultAddress(address) (contracts/dripToken.sol#404-406)
remainingMintableSupply() should be declared external:
        - DripToken.remainingMintableSupply() (contracts/dripToken.sol#525-527)
cap() should be declared external:
        - DripToken.cap() (contracts/dripToken.sol#532-534)
mintedSupply() should be declared external:
        - DripToken.mintedSupply() (contracts/dripToken.sol#539-541)
statsOf(address) should be declared external:
        - DripToken.statsOf(address) (contracts/dripToken.sol#544-546)
mintedBy(address) should be declared external:
        - DripToken.mintedBy(address) (contracts/dripToken.sol#549-551)
isExcluded(address) should be declared external:
        - DripToken.isExcluded(address) (contracts/dripToken.sol#581-583)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-
external
INFO:Slither:./contracts/dripToken.sol analyzed (9 contracts with 75 detectors), 50 result(s) found
```



SLITHER

Drip Network Technical Audit

THANK YOU