SolidLens

Smart Contract Security Audit

for

Polkadrop

Project Details

- **Name of the audited project:** Polkadrop

- **Type:** BEP20 Token

- **Blockchain:** Binance Smart Chain

- **Contract Address:** 0x5Cc16D33A655b7BC92Ede0a6C7D46D318fF02D01

- **Website:** www.polkadrop.online

- **Telegram:** https://t.me/polkadrop

Disclaimer

SolidLens does smart contact audit for the purpose of finding the security related issues within the smart contract. SolidLens doesn’t say that project is legit or scam and doesn’t guarantee that project will not remove liquidity from the DEX or scam exit.

SolidLens doesn’t hold any responsibility if project removes liquidity, team sells their tokens or exit scam. Investors should not take a decision of investing or not based on this report. It is purely with the individual’s decision and cannot claim against SolidLens.

Though SolidLens team does their best to identify any of the cyber security issues within the smart contract, SolidLens doesn’t take any responsibility for any losses or any trading activity.

This audit report cannot be considered as investment advice, and it is just information purpose only.

By reading this report, you are agreeing to the terms of this disclaimer.

Token **Information**

- Name: **Polkadrop**

- Symbol: **DDROP**

- Type: **BEP20**

- Total Supply: **100,000,000,000**

- Token Address: **0x5Cc16D33A655b7BC92Ede0a6C7D46D318fF02D01**

- Contract Deployer: 0x8b81faaccfcbb4f5d79c4932866cff465cc33f6b

- Contract Owner (at the time of audit):0x8b81faaccfcbb4f5d79c4932866cff465cc33f6b

- Total number of holders: 4

Contract Information

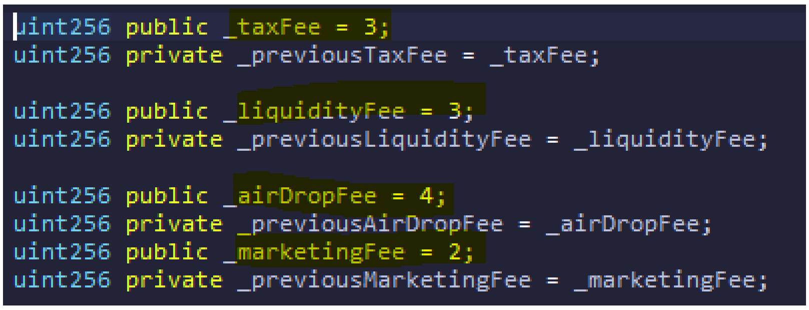
- Contract Name: **Polkadrop**
- Compiler Version: ^0.8.5
- Contract Address: 0x8b81faaccfcbb4f5d79c4932866cff465cc33f6b
- Contract Verification:

  https://bscscan.com/address/0x5Cc16D33A655b7BC92Ede0a6C7D46D318fF02D01
- Optimization Enabled: Yes with 200 runs
- Contract Created Tx:

  https://bscscan.com/tx/0x9d729dff09dc9d3d2d544320806ab0c266047aec684f76bc879b89149f0db7d0

Main Functionality: Binance Pegged Polkadot $DOT as reward distribution and same token reflection

- Contract takes 12% of tokens as tax for every transfer
- Tax is divided as below



```
uint256 public _taxFee = 3;
uint256 private _previousTaxFee = _taxFee;

uint256 public _liquidityFee = 3;
uint256 private _previousLiquidityFee = _liquidityFee;

uint256 public _airDropFee = 4;
uint256 private _previousAirDropFee = _airDropFee;
uint256 public _marketingFee = 2;
uint256 private _previousMarketingFee = _marketingFee;
```

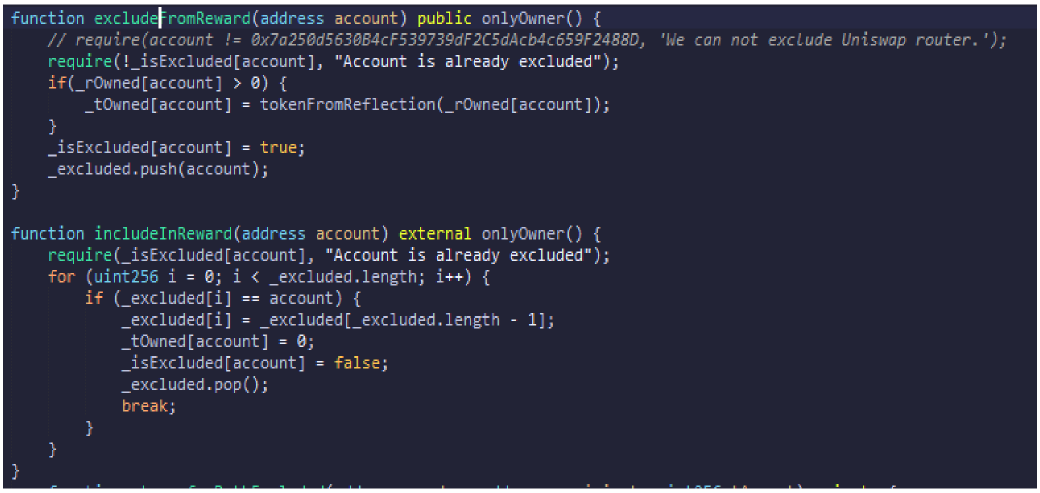
- _airDropFee, which is 4%, swapped to **$DOT BEP20** token and distributed to token holders
- Tax fees are publicly visible variables and can be seen by anyone

Issues Validation and Status

Issue	Review	Result
Compiler Errors	Done	Passed
Integer Overflow and underflow	Done	Passed
Outdated compiler version	Done	Passed
Re-entrancy	Done	Passed
Standard Token implementation	Done	Passed
State variable default visibility	Done	Passed
Timestamp dependency	Done	Passed
Ordering of transactions	Done	Passed
Deprecated functions usage	Done	Passed
Pausing of contract	Done	Passed
Usage of assert, revert, require	Done	Passed
Authorization by tx.origin	Done	Passed
Unprotected SELFDESTRUCT Instruction	Done	Passed
Unchecked Call Return Variable	Done	Passed
Incorrect constructor name	Done	Passed

Contract General Checks

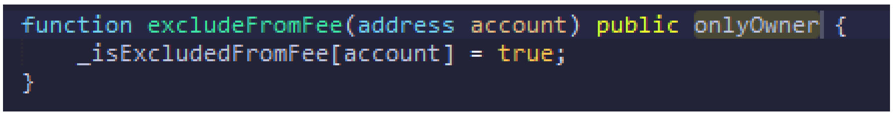
- **Standard Token implementation:** Polkadrop implements standard BEP20 token contract functions as below:
    - totalSupply: gives total supply of the token
    - balanceOf: provides balance of the given account
    - transfer: transfer to the recipient for the amount specified
    - allowance: giving allowance to the spender
    - approve: approves given amount to spend by the spender
    - transferFrom: transfers from sender to recipient for the amount specified
- **Minting of new tokens:** No more new tokens can be minted. Total supply of 100 billion tokens were minted at the time of contract creation and sent to contract creator
- **Contract Pausing:** No functionality to pause the contract from being accessed
- **Ownership Privileges:** If ownership is not renounced
    - Can exclude or include any address from receiving rewards



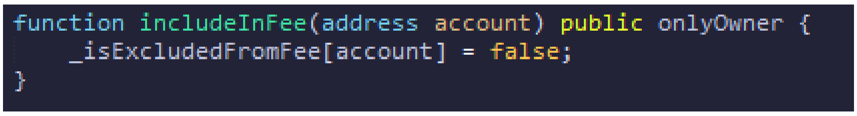
```
function excludeFromReward(address account) public onlyOwner() {
    // require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'We can not exclude Uniswap router.');
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

function includeInReward(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- Can exclude or include any address from transaction fee

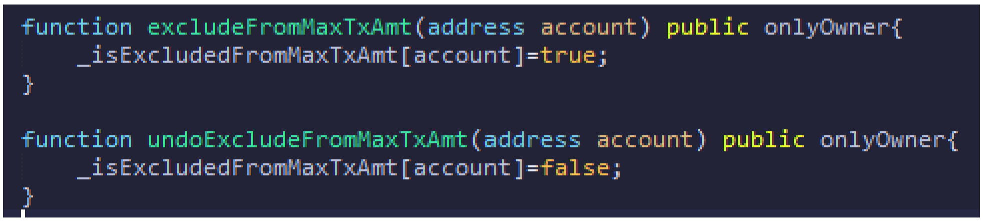


```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}
```



```
function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```

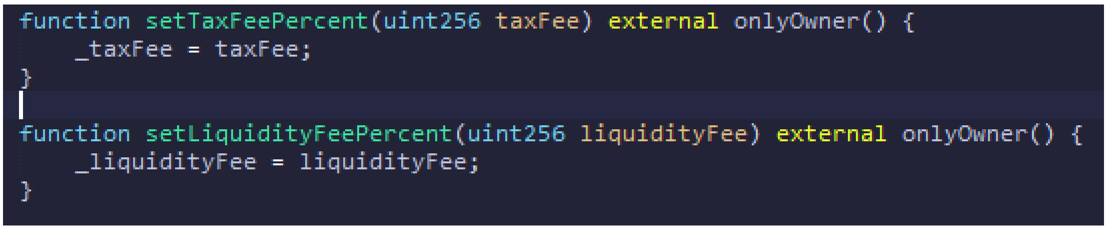
- Can exclude or include any address from max transaction amount



```
function excludeFromMaxTxAmt(address account) public onlyOwner{
    _isExcludedFromMaxTxAmt[account]=true;
}

function undoExcludeFromMaxTxAmt(address account) public onlyOwner{
    _isExcludedFromMaxTxAmt[account]=false;
}
```

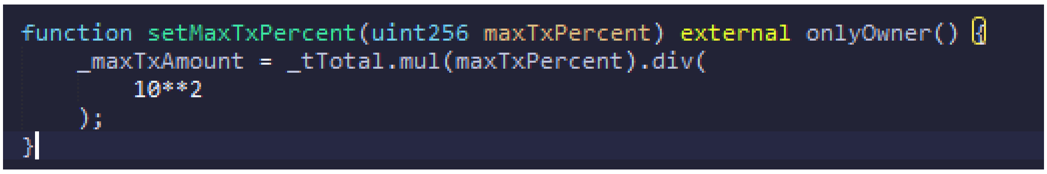
- ➢ Can set any value to various tax fees



```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}

function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}
```

- ➢ Can change max transaction amount to any percentage



```
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner() {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(
        10**2
    );
}
```

❖ Ownership Renounce:

- ➢ Current owner can renounce ownership by calling **renounceOwnership**() function.
- ➢ Ownership can be transferred by the current owner
- ➢ There is no lock/unlock of ownership functionality

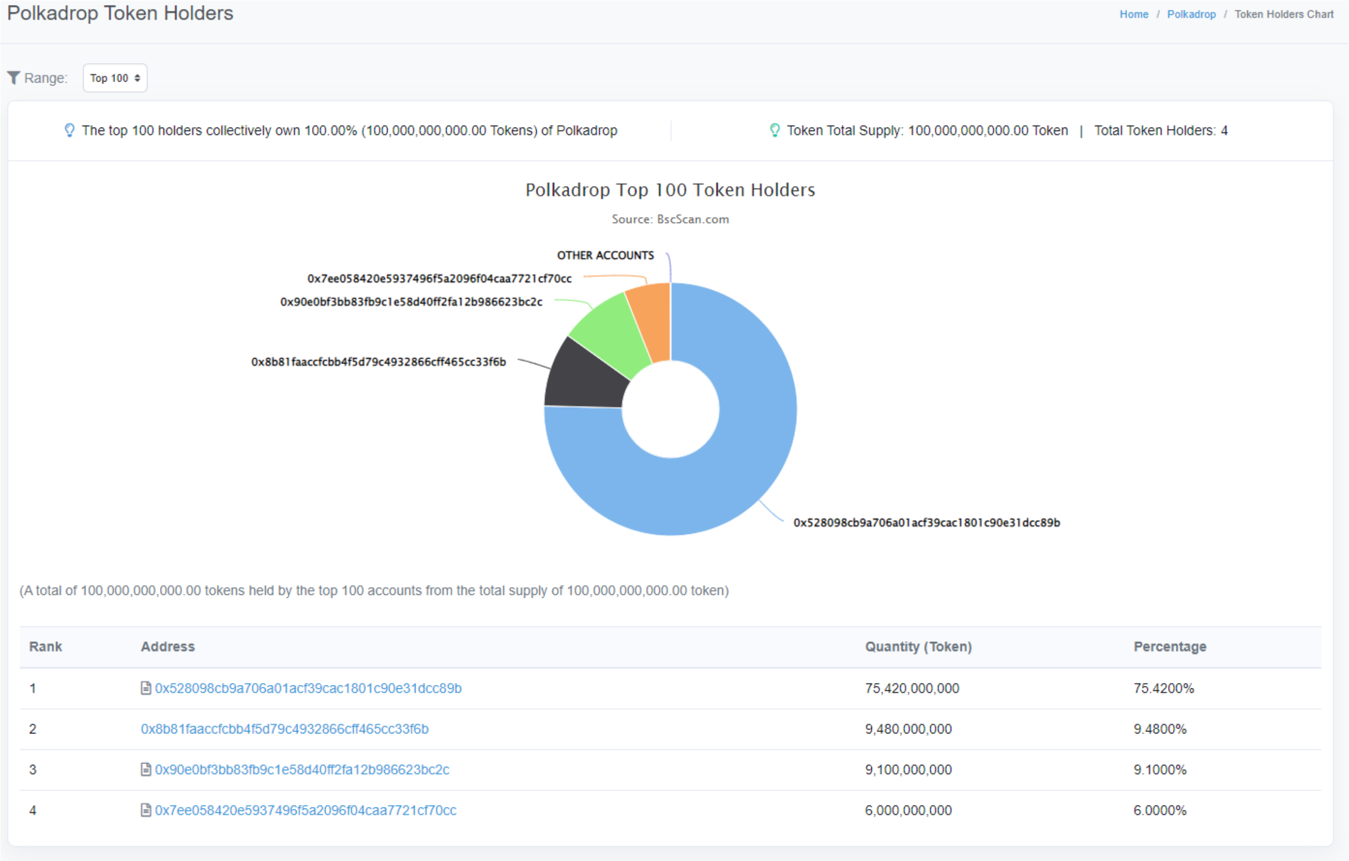
❖ Moderator access:

- ➢ Current owner can add any address as moderator before renouncing ownership
- ➢ Moderator has some limited privileges like add or remove moderator, enable/disable swaps for liquidity & rewards, enable/disable auto rewards calculation, enable/disable buy back and burn
- ➢ Can withdraw BNB, native token, reward token from the contract balance

Top 100 Token Holders

(Get the up-to-date holder list here:

https://bscscan.com/token/tokenholderchart/0x5Cc16D33A655b7BC92Ede0a6C7D46D318fF02D01)



Home / Polkadrop / Token Holders Chart
Range:
Top 100
OTHER ACCOUNTS
0x7ee058420e5937496f5a2096f04caa7721cf70cc
0x90e0bf3bb83fb9c1e58d40ff2fa12b986623bc2c
0x8b81faaccfcbb4f5d79c4932866cff465cc33f6b
0x528098cb9a706a01acf39cac1801c90e31dcc89b

Polkadrop Token Holders

The top 100 holders collectively own 100.00% (100,000,000,000.00 Tokens) of Polkadrop

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 4

Polkadrop Top 100 Token Holders

Source: BscScan.com

(A total of 100,000,000,000.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x528098cb9a706a01acf39cac1801c90e31dcc89b	75,420,000,000	75.4200%
2	0x8b81faaccfcbb4f5d79c4932866cff465cc33f6b	9,480,000,000	9.4800%
3	0x90e0bf3bb83fb9c1e58d40ff2fa12b986623bc2c	9,100,000,000	9.1000%
4	0x7ee058420e5937496f5a2096f04caa7721cf70cc	6,000,000,000	6.0000%

Audit Summary

SolidLens team performed the audit by manually reviewing line-by-line source code of the contract and ran some automated reviews and tests.

The focus for the audit review was to find security related issues and vulnerabilities within the contract source code.

Report Date: 11/26/2021

Rating: **Low Risk**

Results: **Passed**

About SolidLens

SolidLens is a blockchain security and smart contract auditing services company, incorporated by group of blockchain engineers and cyber security experts.

Contact Us:

Website: www.solidlens.com Telegram: @solidlens