

Submitted audit for **PRTCLS** token at 14 September 2023

Audit result : **Passed**

Token Address : 0xC97C55aD0F4EAc55DC3a1f83003248Bd6410d1d3

Name: Particles

Symbol: PRTCLS

Decimals: 9

Network: Binance smart chain

Token Type: BEP20

Owner: 0xAAE811DA55c262468569bA9b56BaFB081c194710

Deployer: 0xAAE811DA55c262468569bA9b56BaFB081c194710

Token Supply: 100,000,000

Checksum:

ab673ab3b0b2ac9b227c0dc8ce447cbbbed914f67

Testnet version:

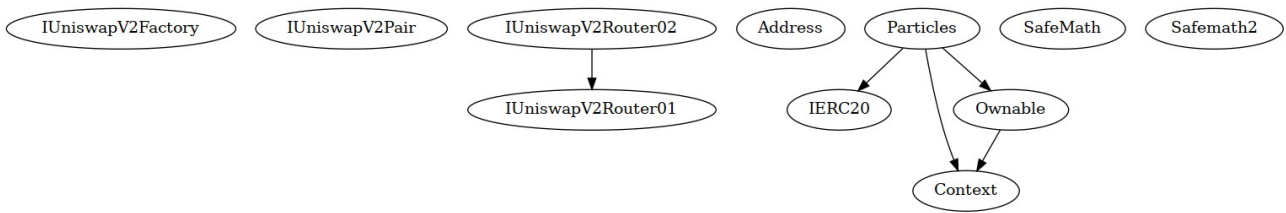
The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/token/0xeD67d3Ba7eb98c9A23C2112523607fe3eBEA1b6a>

Tools:

1. Manual Review: The code has undergone a line-by-line review by the **Ace** team.
2. BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.
3. Slither: The code has undergone static analysis using Slither.

Inheritance Tree



Contract Assessment

```

Contract |      Type      |      Bases      |      |      |
|:-----:|:-----:|:-----:|:-----:|:-----:|
|      L      | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
|
||||| |
| **IUniswapV2Factory** | Interface | |||
| L | feeTo | External ! | | NO! |
| L | feeToSetter | External ! | | NO! |
| L | getPair | External ! | | NO! |
| L | allPairs | External ! | | NO! |
| L | allPairsLength | External ! | | NO! |
| L | createPair | External ! | | NO! |
| L | setFeeTo | External ! | | NO! |
| L | setFeeToSetter | External ! | | NO! |
|||||
| **IUniswapV2Pair** | Interface | |||
| L | name | External ! | | NO! |
| L | symbol | External ! | | NO! |
| L | decimals | External ! | | NO! |
| L | totalSupply | External ! | | NO! |
| L | balanceOf | External ! | | NO! |
| L | allowance | External ! | | NO! |
| L | approve | External ! | | NO! |
| L | transfer | External ! | | NO! |
| L | transferFrom | External ! | | NO! |
| L | DOMAIN_SEPARATOR | External ! | | NO! |
| L | PERMIT_TYPEHASH | External ! | | NO! |
| L | nonces | External ! | | NO! |
| L | permit | External ! | | NO! |
| L | MINIMUM_LIQUIDITY | External ! | | NO! |
| L | factory | External ! | | NO! |
| L | token0 | External ! | | NO! |
| L | token1 | External ! | | NO! |
| L | getReserves | External ! | | NO! |
| L | price0CumulativeLast | External ! | | NO! |

```

```

|  L | price1CumulativeLast | External ! | |NO! |
|  L | kLast | External ! | |NO! |
|  L | mint | External ! | |NO! |
|  L | burn | External ! | |NO! |
|  L | swap | External ! | |NO! |
|  L | skim | External ! | |NO! |
|  L | sync | External ! | |NO! |
|  L | initialize | External ! | |NO! |

```

```
|||||
```

```

| **IUniswapV2Router01** | Interface | |||
|  L | factory | External ! | |NO! |
|  L | WETH | External ! | |NO! |
|  L | addLiquidity | External ! | |NO! |
|  L | addLiquidityETH | External ! | |NO! |
|  L | removeLiquidity | External ! | |NO! |
|  L | removeLiquidityETH | External ! | |NO! |
|  L | removeLiquidityWithPermit | External ! | |NO! |
|  L | removeLiquidityETHWithPermit | External ! | |NO! |
|  L | swapExactTokensForTokens | External ! | |NO! |
|  L | swapTokensForExactTokens | External ! | |NO! |
|  L | swapExactETHForTokens | External ! | |NO! |
|  L | swapTokensForExactETH | External ! | |NO! |
|  L | swapExactTokensForETH | External ! | |NO! |
|  L | swapETHForExactTokens | External ! | |NO! |
|  L | quote | External ! | |NO! |
|  L | getAmountOut | External ! | |NO! |
|  L | getAmountIn | External ! | |NO! |
|  L | getAmountsOut | External ! | |NO! |
|  L | getAmountsIn | External ! | |NO! |

```

```
|||||
```

```

| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
|  L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | |NO! |
|  L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! |
|    |NO! |
|  L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | |
NO! |
|  L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | |NO! |
|
|  L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | |NO! |
|

```

```
|||||
```

```

| **Address** | Library | |||
|  L | isContract | Internal 0 | ||
|  L | sendValue | Internal 0 | ||
|  L | functionCall | Internal 0 | ||

```

```

| L | functionCall | Internal 0 | |
| L | functionCallWithValue | Internal 0 | |
| L | functionCallWithValue | Internal 0 | |
| L | _functionCallWithValue | Private | |

```

```
|||||
```

```

| **IERC20** | Interface | |||
| L | totalSupply | External ! | |NO!|
| L | balanceOf | External ! | |NO!|
| L | transfer | External ! | |NO!|
| L | allowance | External ! | |NO!|
| L | approve | External ! | |NO!|
| L | transferFrom | External ! | |NO!|

```

```
|||||
```

```

| **SafeMath** | Library | |||
| L | add | Internal 0 | |
| L | sub | Internal 0 | |
| L | sub | Internal 0 | |
| L | mul | Internal 0 | |
| L | div | Internal 0 | |
| L | div | Internal 0 | |
| L | mod | Internal 0 | |
| L | mod | Internal 0 | |

```

```
|||||
```

```

| **Safemath2** | Library | |||
| L | add | Internal 0 | |
| L | sub | Internal 0 | |
| L | sub | Internal 0 | |
| L | mul | Internal 0 | |
| L | div | Internal 0 | |
| L | div | Internal 0 | |
| L | mod | Internal 0 | |
| L | mod | Internal 0 | |

```

```
|||||
```

```

| **Context** | Implementation | |||
| L | _msgSender | Internal 0 | |
| L | _msgData | Internal 0 | |

```

```
|||||
```

```

| **Ownable** | Implementation | Context |||
| L | <Constructor> | Public ! | |NO!|
| L | owner | Public ! | |NO!|
| L | renounceOwnership | Public ! | |onlyOwner|
| L | transferOwnership | Public ! | |onlyOwner|
| L | getUnlockTime | Public ! | |NO!|
| L | lock | Public ! | |onlyOwner|
| L | unlock | Public ! | |NO!|

```

```

||||| |
| **Particles** | Implementation | Context, IERC20, Ownable |||
| L | <Constructor> | Public ! | |NO! |
| L | name | Public ! | |NO! |
| L | symbol | Public ! | |NO! |
| L | decimals | Public ! | |NO! |
| L | totalSupply | Public ! | |NO! |
| L | balanceOf | Public ! | |NO! |
| L | transfer | Public ! | |NO! |
| L | allowance | Public ! | |NO! |
| L | approve | Public ! | |NO! |
| L | transferFrom | Public ! | |NO! |
| L | increaseAllowance | Public ! | |NO! |
| L | decreaseAllowance | Public ! | |NO! |
| L | isExcludedFromFee | Public ! | |NO! |
| L | excludeFromFee | External ! | |onlyOwner |
| L | includeInFee | External ! | |onlyOwner |
| L | _approve | Private | |
| L | _transfer | Private | |
| L | isExcludedFromMaxTx | Public ! | |NO! |
| L | excludeFromMaxTx | External ! | |onlyOwner |
| L | includeInMaxTx | External ! | |onlyOwner |
| L | swapAndLiquify | Private | |lockTheSwap |
| L | swapTokensForEth | Private | |
| L | addLiquidity | Private | |
| L | _tokenTransfer | Private | |
| L | _transferStandard | Private | |
| L | transferStandard | External ! | |onlyOwner |
| L | setMaxTxPercent | External ! | |onlyOwner |
| L | maxTxPercent | Public ! | |NO! |
| L | isExcludedFromMaxTxPercent | Public ! | |NO! |
| L | setSwapAndLiquifyEnabled | Public ! | |onlyOwner |
| L | withdrawETH | External ! | |onlyOwner |
| L | withdrawERC20 | External ! | |onlyOwner |
| L | deposit | External ! | |NO! |

```

Legend

```

| Symbol | Meaning |
|:-----:|:-----|
|         | Function can modify state |
|         | Function is payable |

```

Static Analysis

an static analysis of the code were performed using slither. No issues were found

```
INFO:Detectors:
Pragma version^0.6.12 (contracts/Token.sol#2) allows old versions
solc-0.6.12 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#383-395):
- (success) = recipient.call(value: amount)() (contracts/Token.sol#390)
Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#480-508):
- (success,returndata) = target.call(value: weiValue)(data) (contracts/Token.sol#489-491)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#66) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#68) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#99) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Token.sol#141) is not in mixedCase
Parameter Particles.setSwapAndLiquifyEnabled(bool)._enabled (contracts/Token.sol#1264) is not in mixedCase
Variable Particles._maxTxAmount (contracts/Token.sol#992) is not in mixedCase
Variable Particles._maxTxPercent (contracts/Token.sol#993) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (contracts/Token.sol#910)" inContext (contracts/Token.sol#904-913)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#146) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#147)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
Particles.slitherConstructorVariables() (contracts/Token.sol#976-1291) uses literals with too many digits:
- _totalSupply = 1000000000 * 10 ** 9 (contracts/Token.sol#987)
Particles.slitherConstructorVariables() (contracts/Token.sol#976-1291) uses literals with too many digits:
- _maxTxAmount = 500000 * 10 ** 9 (contracts/Token.sol#992)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
Particles._excluded (contracts/Token.sol#985) is never used in Particles (contracts/Token.sol#976-1291)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable
INFO:Detectors:
Particles._decimals (contracts/Token.sol#990) should be constant
Particles._maxTxPercent (contracts/Token.sol#993) should be constant
Particles._name (contracts/Token.sol#988) should be constant
Particles._symbol (contracts/Token.sol#989) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Slither:contracts/Token.sol analyzed (11 contracts with 88 detectors), 52 result(s) found
```

•

Functional Tests

Router (PCS V2):

1- Adding liquidity (passed):

[https://testnet.bscscan.com/tx/](https://testnet.bscscan.com/tx/0x0c2851312d3714c00a0e2bfdb347630c6e75675a909d6f19774a920958884613)

0x0c2851312d3714c00a0e2bfdb347630c6e75675a909d6f19774a920958884613

2- Buying (0% tax) (passed):

[https://testnet.bscscan.com/tx/](https://testnet.bscscan.com/tx/0x83d25185d0f14fc444e1a51ccbed8c18ba476b9fe0bd0abf7aba6b5dc2f78403)

0x83d25185d0f14fc444e1a51ccbed8c18ba476b9fe0bd0abf7aba6b5dc2f78403

3- Selling (0% tax) (passed):

[https://testnet.bscscan.com/tx/](https://testnet.bscscan.com/tx/0xc630c1827f7f69a49d8b45b42982e03b24b219fdc9a2b188a263145d0c7ba809)

0xc630c1827f7f69a49d8b45b42982e03b24b219fdc9a2b188a263145d0c7ba809

4- Transferring (0% tax) (passed):

[https://testnet.bscscan.com/tx/](https://testnet.bscscan.com/tx/0x002eb567c40fdda860706c9e6c588299a2ca8d089a1ed0ba9cc3756712e68030)

0x002eb567c40fdda860706c9e6c588299a2ca8d089a1ed0ba9cc3756712e68030

Summary:

- **Owner is able to not able to set buy/sell/transfer fees**
- Owner is not able to blacklist an arbitrary wallet
- Owner is not able to disable trades
- Owner is not able to mint new tokens
- Owner is not able to set maximum wallet and maximum buy/sell/transfer limits
- **Owner must enable trades manually**

Findings:**Critical:** 0**High :** 2**Medium:** 0**Low:** 0**Suggestions & Optimizations:** 0