Audit Report for **UltimateTokenOwnable**
Date: 12 February 2024
Audit result: **Passed with High Risk**

**Token Address:** 0x42FFDd33BB079eD662b28206D21387aeC8F1aa16

**Name:** NET FREE COIN

**Symbol:** NFC

**Decimals**: 18

**Network:** BscScan

**Token Type**: BEP-20

**Owner**: 0x22f4bcebBd2f989a450AA51210ceb0f4675578dF

**Deployer:** 0x22f4bcebBd2f989a450AA51210ceb0f4675578dF

**Token Supply:** 100000000000

**Checksum:** Ae1c3a4fbb6e83e8393a57617b5a5b331

**Testnet:**
https://testnet.bscscan.com/address/0x7339440cae557c2b8dded1d8dee3d8d016a0ad6b#code

**Token Overview:**

**Buy Fee:** 0-0%

**Sell Fee:** 0-0%

**Transfer Fee:** 0-0%

**Fee Privilege:** Owner

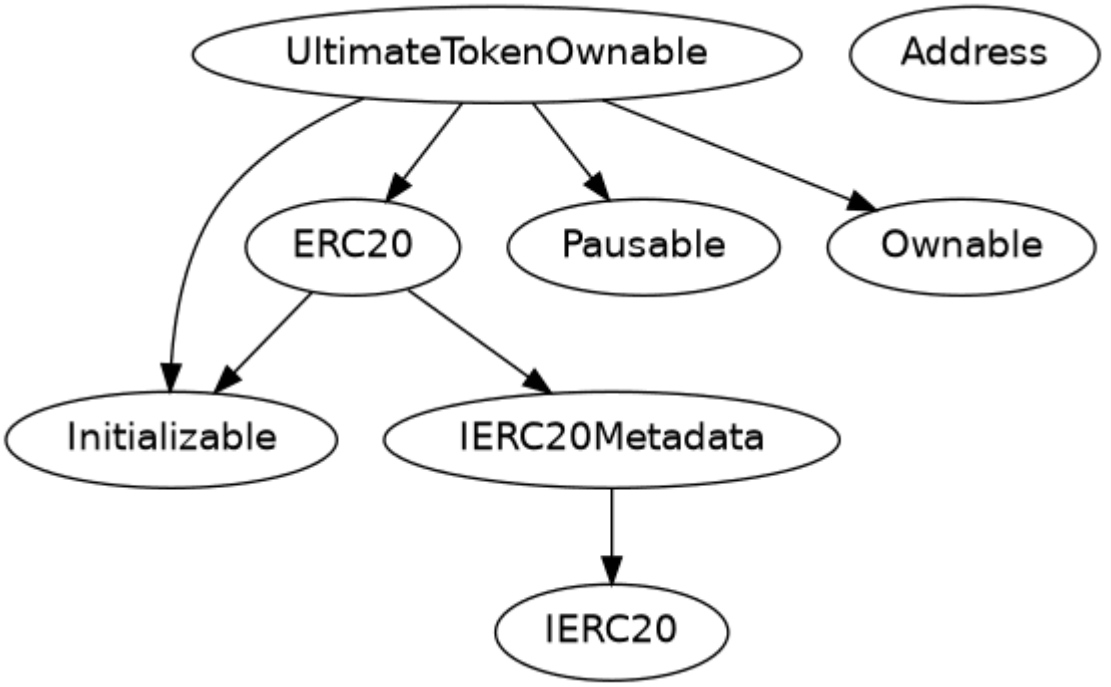
**Ownership:** Owned

**Minting:** No

**Max Tx:** No

**Blacklist:** No

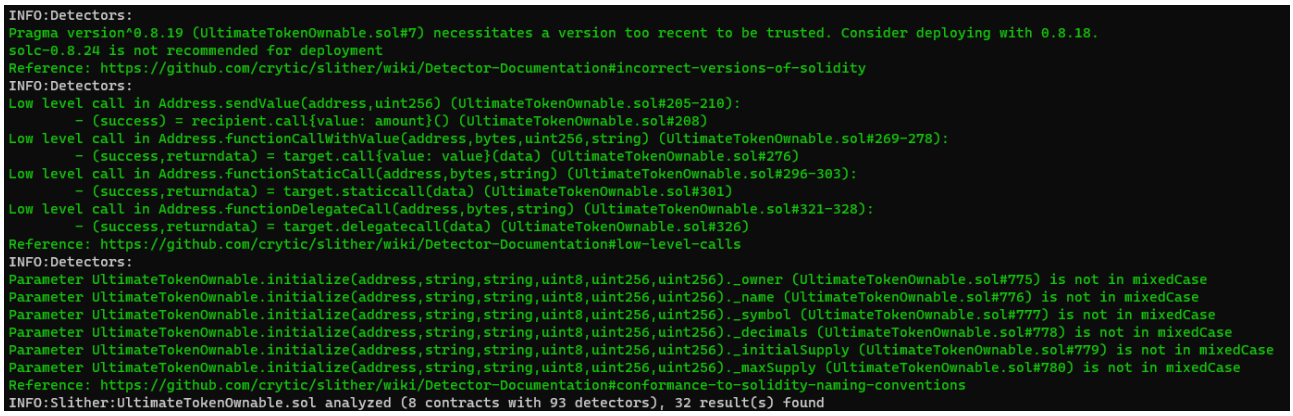
## Inheritance Tree




# Static Analysis

A static analysis of the code was performed using Slither. No issues were found.

```
INFO:Detectors:
UltimateTokenOwnable.initialize(address,string,string,uint8,uint256,uint256)._owner (UltimateTokenOwnable.sol#775) shadows:
        - Ownable._owner (UltimateTokenOwnable.sol#112) (state variable)
UltimateTokenOwnable.initialize(address,string,string,uint8,uint256,uint256)._name (UltimateTokenOwnable.sol#776) shadows:
        - ERC20._name (UltimateTokenOwnable.sol#605) (state variable)
UltimateTokenOwnable.initialize(address,string,string,uint8,uint256,uint256)._symbol (UltimateTokenOwnable.sol#777) shadows:
        - ERC20._symbol (UltimateTokenOwnable.sol#606) (state variable)
UltimateTokenOwnable.initialize(address,string,string,uint8,uint256,uint256)._decimals (UltimateTokenOwnable.sol#778) shadows:
        - ERC20._decimals (UltimateTokenOwnable.sol#607) (state variable)
UltimateTokenOwnable.initialize(address,string,string,uint8,uint256,uint256)._maxSupply (UltimateTokenOwnable.sol#780) shadows:
        - ERC20._maxSupply (UltimateTokenOwnable.sol#603) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Address._revert(bytes,string) (UltimateTokenOwnable.sol#372-384) uses assembly
        - INLINE ASM (UltimateTokenOwnable.sol#377-380)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Address._revert(bytes,string) (UltimateTokenOwnable.sol#372-384) is never used and should be removed
Address.functionCall(address,bytes) (UltimateTokenOwnable.sol#230-232) is never used and should be removed
Address.functionCall(address,bytes,string) (UltimateTokenOwnable.sol#240-246) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (UltimateTokenOwnable.sol#259-261) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (UltimateTokenOwnable.sol#269-278) is never used and should be removed
Address.functionDelegateCall(address,bytes) (UltimateTokenOwnable.sol#311-313) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (UltimateTokenOwnable.sol#321-328) is never used and should be removed
Address.functionStaticCall(address,bytes) (UltimateTokenOwnable.sol#286-288) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (UltimateTokenOwnable.sol#296-303) is never used and should be removed
Address.sendValue(address,uint256) (UltimateTokenOwnable.sol#205-210) is never used and should be removed
Address.verifyCallResult(bool,bytes,string) (UltimateTokenOwnable.sol#360-370) is never used and should be removed
Address.verifyCallResultFromTarget(address,bool,bytes,string) (UltimateTokenOwnable.sol#336-352) is never used and should be removed
Initializable._getInitializedVersion() (UltimateTokenOwnable.sol#561-563) is never used and should be removed
Initializable._isInitializing() (UltimateTokenOwnable.sol#568-570) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.19 (UltimateTokenOwnable.sol#7) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
solc-0.8.24 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) (UltimateTokenOwnable.sol#205-210):
        - (success) = recipient.call{value: amount}() (UltimateTokenOwnable.sol#208)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (UltimateTokenOwnable.sol#269-278):
        - (success,returndata) = target.call{value: value}(data) (UltimateTokenOwnable.sol#276)
Low level call in Address.functionStaticCall(address,bytes,string) (UltimateTokenOwnable.sol#296-303):
        - (success,returndata) = target.staticcall(data) (UltimateTokenOwnable.sol#301)
Low level call in Address.functionDelegateCall(address,bytes,string) (UltimateTokenOwnable.sol#321-328):
        - (success,returndata) = target.delegatecall(data) (UltimateTokenOwnable.sol#326)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
```




# Functional Tests

## Router (PCS V2):

**1- Approve (passed):**
https://testnet.bscscan.com/tx/0xd06433bf328639345385d2642e5e56419033093fdf52cf0924193750ff18e55f

**2- Increase Allowance (passed):**
https://testnet.bscscan.com/tx/0xb9bef52635b500df42f4d9bc22c52c10e27c1a3ba716f4616a90f103859bb761

**3- Decrease Allowance (passed):**
https://testnet.bscscan.com/tx/0x2f6a2965a91f48aa0c00d88daec9fc1b92b33985a0dc87e4307572a30bad0f64

**4- Mint (passed):**
https://testnet.bscscan.com/tx/0xfb35a62594b3f55ad9f11d21054291cf3577373f56d308438c666969bae2c8f3

**5- Pause (passed):**
https://testnet.bscscan.com/tx/0x830ce539c84e65519bc2a656a4444606a34f3dba522b6d02c60b739974ac89c4

## Ownership Privileges:

- The owner can transfer ownership.
- The owner can renounce the ownership.
- The owner can pause/unpause token.
- The owner can mint token.

**Findings:**
**Critical**: 0
**High**: 1
**Medium**: 0
**Low**: 2
**Informational & Optimizations**: 0

**Note: The minting will be possible in the contract but not more than the max total supply which is mentioned in the contract i.e; 100000000000**

# Centralization – The owner can Pause the token.

**Severity**: High
**Function**: pause
**Status:** Open
**Overview:**
The owner can pause the token for an unlimited period of time which can lock the user's token.

```
function pause() public onlyOwner {
        _pause();
    }Suggestion:
```

**Suggestion:**
It is recommended that there should be a locking period.

# Optimization

**Severity**: Informational
**Subject**: Floating Pragma Solidity version
**Status:** Open
**Overview:**
It is considered best practice to pick one compiler version and stick with it. With a floating pragma, contracts may accidentally be deployed using an outdated.

```
pragma solidity ^0.8.19;
```

**Suggestion:**
Adding the latest constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

# Optimization

**Severity**: Optimization
**Subject**: Remove unused code.
**Status:** Open
**Overview:**
Unused variables are allowed in Solidity, and they do. not pose a direct security issue. It is the best practice though to avoid them.

```
function sendValue(address payable recipient, uint256 amount) internal {
        require(address(this).balance >= amount, "Address: insufficient balance");

        (bool success, ) = recipient.call{ value: amount }("");
        require(success, "Address: unable to send value, recipient may have re-
verted");
    }
modifier reinitializer(uint8 version) {
        require(!_initializing && _initialized < version, "Initializable: contract
is already initialized");
        _initialized = version;
        _initializing = true;
        _;
        _initializing = false;
        emit Initialized(version);
    }
function _getInitializedVersion() internal view returns (uint8) {
        return _initialized;
    }
function _isInitializing() internal view returns (bool) {
        return _initializing;
    }
```