AUDIT REPORT

DATE APRIL 19TH

FOR STAKE MONEY

Solid Group Auditing Service
Telegram: @solid_1
Twitter: https://twitter.com/solid_group_1

Disclaimer

SolidGroup reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. Solid group do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’…)
SolidGroup Audits do not provide any warranty or guarantee **regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors. SolidGroup Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.**
SolidGroup Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. **SolidGroup’s position is that each company and individual are responsible for their own due diligence and continuous security.** SolidGroup in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Overview

Network: Binance Smart Chain
Website: https://www.stakemoney.io/
Twitter Group: https://twitter.com/stakemoneybsc
Telegram Group: http://t.me/StakeMoneyBSC

Description

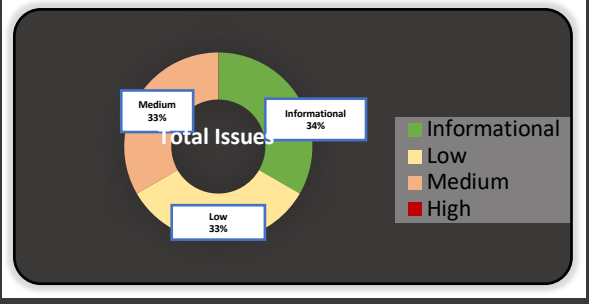
$Money is a Binance Smart Chain yield farming protocol using a completely decentralized approach.

Files in Scope

Contract Name	Contract Address (BSC)
Money.sol	0x23a50FE32b1D29A86A4FddC5d61C9733f2A4Ed2A

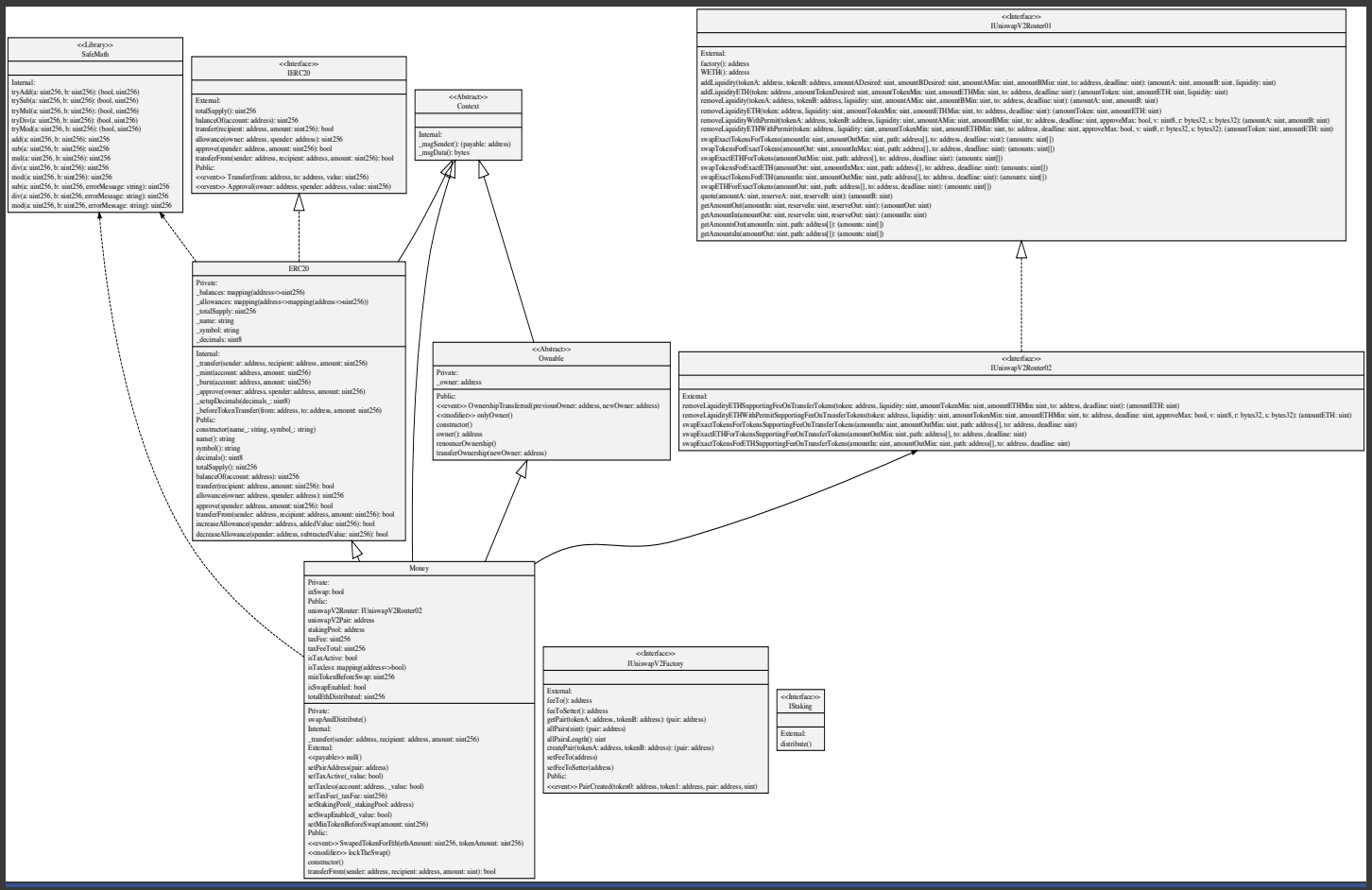
Vulnerability Summary

Informational severity Issues	1
Low severity issues	1
Medium severity issues	1
High severity issues	0



UML

Money.sol



BEP-20's Conformance

This test checks for BEP-20's conformance.

- All the functions are present
- All the events are present
- Functions return the correct type
- Functions that must be view are view
- Events' parameters are correctly indexed
- The functions emit the events
- Derived contracts do not break the conformance

Function	present	type	Correct Return value	events	
totalSupply	✅	✅ view	✅		
balanceOf(address)	✅	✅ view	✅		
transfer(address,uint256)	✅	✅ external	✅	✅ Transfer	
transferFrom(address, address, uint256)	✅	✅ external	✅	✅ Transfer	
approve(address,uint256)	✅	✅ external	✅	✅ Approval	
allowance(address, address)	✅	✅ view	✅		
name	✅	✅ view	✅		
symbol	✅	✅ view	✅		

Check Events:

✅ Transfer

✅ Approve

General:

✅ No external mint function

✅ No Volatile Code

The contract that was tested is the token's contract: Money.sol

General Notes

Owner Capabilities:

- The owner can exempt addresses from tax fees (by calling setTaxless ())
- The owner can set the staking pool address (setStakingPool ()). Once the owner set the stakingPool address it cannot be modified.
- The owner can control whether tax is taken or not (setTaxActive ())
- The owner can control whether to send ETH to the staking contract (setSwapEnabled ())
- The tokens accumulated from fees are sold on PancakeSwap and distributed to all stakers proportional to their holdings.
- The owner can stop the BNB distribution to stakers (By calling setSwapEnabled)
- The owner can change the minimum amount of total fees before distribution to stakers.

Money.sol

Issue #1:

Type	Severity	Location
Lack of events	Informational	PSWAP.sol

Description:

The functions setTaxActive, setTaxless, setStakingPool, setSwapEnabled, and setMinTokensBeforeSwap change the state of the contract, without emitting events.

Recommendation:

Our recommendation is to add events in critical parts of the contract, such us when setting the amount of % to be taken for swap, when address is exempted from tax fees, and when you set the staking pool address and etc'..
Events are great for integrating with DApps in the future and also for the integration with Blockchain explorers.

Issue #2:

Type	Severity	Location
Owner capabilities	Low	Money.sol

Description:

The owner can determine the amount of % to be taken for tax fee. By calling setTaxFee().

Recommendation:

Our recommendation is to have a minimum or at least maximum limit for the setter function.

Issue #3:

Type	Severity	Location
Owner capabilities	● Medium	Money.sol

Description:

The function “transferFrom” enables the stakingPool contract to transfer on behalf of any address, without his allowance. If the stakingPool is an address controlled by the owner, the owner can transfer any amount of tokens from any address to any address.

```
    function transferFrom(address sender, address recipient, uint amount) public override returns
(bool) {
        _transfer(sender, recipient, amount);
        // Solid: IF it is the staking pool he can take everything???
        if(_msgSender() == stakingPool) return true;

        _approve(sender, _msgSender(), allowance(sender,_msgSender()).sub(amount, "MONEY: transfer
amount exceeds allowance"));
        return true;
    }
```

Recommendation:

Our recommendation is to remove this line immediately. A better approach would be to call approve before staking.

Team Response

The team decided not to address the issue described above. We did our own tests for investors to make sure this behavior won’t be used maliciously. Once the owner sets the stakingPool address (By calling setStakingPoolf function) it cannot be modified. Currently stakingPool value is an address of a contract which is verified on bscscan. The stakingPool contract was audited and cannot be used maliciously by the owner. The only aspect that was audited at this time of writing is the possibility for the owner to use this behavior maliciously and not the full functionality of the stakingPool contract.

Summary

S

● Informational severity Issues	1
● Low severity issues	1
● Medium severity issues	1
● High severity issues	0