



Cyberscope

# Audit Report

## **Wuacoin**

June 2023

Network      BSC

Address      0xa7E5b5B711B99B833546F5682aD143cB6C863E30

Audited by   © cyberscope

# Analysis

● Critical   ● Medium   ● Minor / Informative   ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

# Diagnostics

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	TMI	Transfer Methods Inconsistency	Unresolved

# Table of Contents

<b>Analysis</b>	<b>1</b>
<b>Diagnostics</b>	<b>2</b>
<b>Table of Contents</b>	<b>3</b>
<b>Review</b>	<b>4</b>
Audit Updates	4
Source Files	5
<b>Findings Breakdown</b>	<b>6</b>
TMI - Transfer Methods Inconsistency	7
Description	7
Recommendation	8
<b>Functions Analysis</b>	<b>9</b>
<b>Inheritance Graph</b>	<b>10</b>
<b>Flow Graph</b>	<b>11</b>
<b>Summary</b>	<b>12</b>
<b>Disclaimer</b>	<b>13</b>
<b>About Cyberscope</b>	<b>14</b>

## Review

Contract Name	WuaoCoin
Compiler Version	v0.8.19+commit.7dd6d404
Optimization	200 runs
Explorer	<a href="https://bscscan.com/address/0xa7e5b5b711b99b833546f5682ad143cb6c863e30">https://bscscan.com/address/0xa7e5b5b711b99b833546f5682ad143cb6c863e30</a>
Address	0xa7e5b5b711b99b833546f5682ad143cb6c863e30
Network	BSC
Symbol	WUAO
Decimals	18
Total Supply	100,000,000

## Audit Updates

Initial Audit	01 Jun 2023 <a href="https://github.com/cyberscope-io/audits/blob/main/v1/wuao/BS C.pdf">https://github.com/cyberscope-io/audits/blob/main/v1/wuao/BS C.pdf</a>
Corrected Phase 2	07 Jun 2023 <a href="https://github.com/cyberscope-io/audits/blob/main/v2/wuao/BS C.pdf">https://github.com/cyberscope-io/audits/blob/main/v2/wuao/BS C.pdf</a>
Corrected Phase 3	13 Jun 2023

## Source Files

Filename	SHA256
<b>contracts/WUAO_AUDI.sol</b>	c3bcb134fc1ab2c655c6ebc9d8a46b3da17efa641d93562de5d9dc47f7509d12

## Findings Breakdown



● Critical	0
● Medium	0
● Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	1	0	0	0

## TMI - Transfer Methods Inconsistency

Criticality	Minor / Informative
Location	WuaoCoin.sol#L39,52
Status	Unresolved

### Description

The contract exhibits an inconsistency between the `transfer` and `transferFrom` methods in terms of validation checks. In particular, the `transferFrom` method includes a crucial validation step to ensure that the sender possesses a balance equal to or greater than the amount being transferred. However, the `transfer` method lacks this validation check altogether. Consequently, if the `transfer` method is invoked with an amount that surpasses the sender's balance, the operation `sub(balances[msg.sender], tokens)` will result in an underflow, ultimately leading to the transaction being reverted.

```
function transfer(address to, uint tokens) override public returns (bool success) {
    balances[msg.sender] = sub(balances[msg.sender],tokens);
    balances[to] = add(balances[to],tokens);
    emit Transfer(msg.sender, to, tokens);
    success = true;
}

function transferFrom(address from, address to, uint tokens) override public returns (bool success) {
    require(allowed[from][msg.sender]>=tokens,"Spender without balance allowed");
    require(balances[from] > tokens,"From without balance!");
    allowed[from][msg.sender] = sub(allowed[from][msg.sender],tokens);
    balances[from] = sub(balances[from],tokens);
    balances[to] = add(balances[to],tokens);
    emit Transfer(from, to, tokens);
    success = true;
}
```



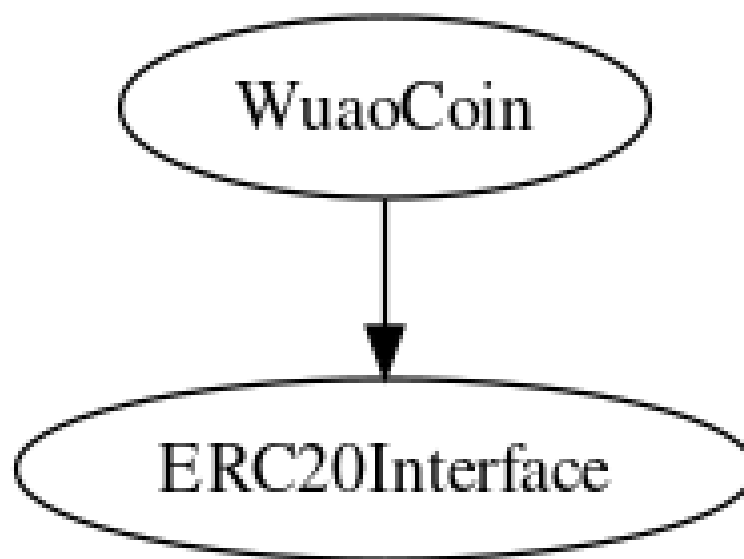
## Recommendation

The team is advised to align the validation checks in both the `transfer` and `transferFrom` methods. By incorporating the same validation logic in the `transfer` method, it will prevent transactions with excessive amounts from being processed and avoid potential underflow issues. This adjustment will help maintain consistency across the contract's functionalities and enhance the overall reliability and security of the token transfer mechanisms.

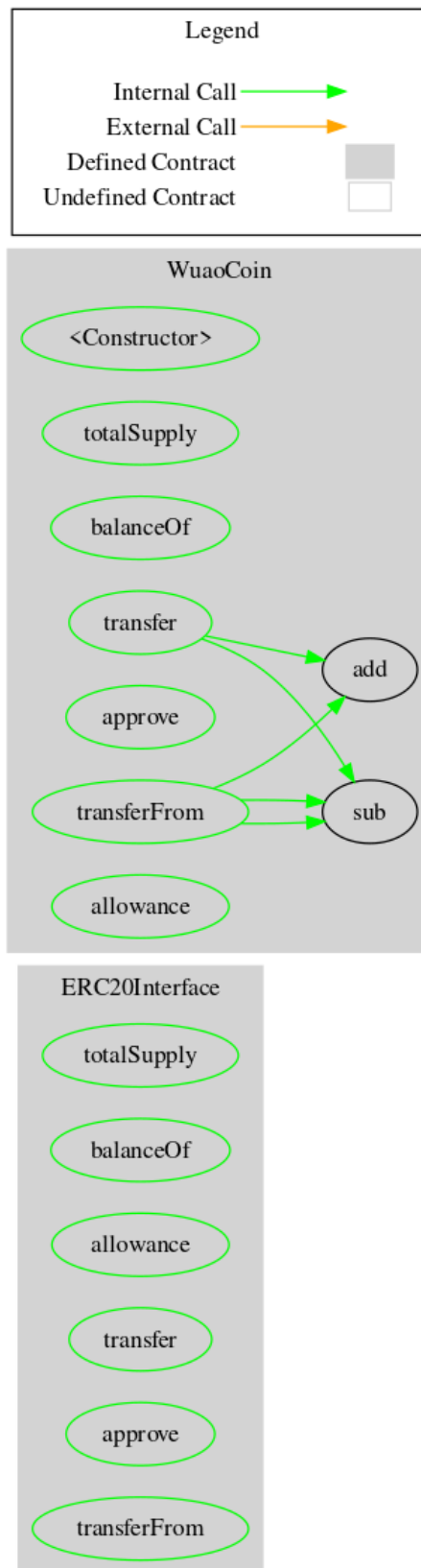
## Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>ERC20Interface</b>	Implementation			
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
<b>WuaoCoin</b>	Implementation	ERC20Interface		
		Public	✓	-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	allowance	Public		-
	add	Internal		
	sub	Internal		

## Inheritance Graph



# Flow Graph



## Summary

Wuacoin contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. Wuacoin is an interesting project that has a friendly and growing community. The Smart Contract may face some issues because of the approval threshold. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does 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' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment 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. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

## About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



**The Cyberscope team**

<https://www.cyberscope.io>