



Cyberscope

Audit Report

**JC Coin**

February 2024

Network    ETH

Address    0x03a9d7c8caf836de35666c5f7e317306b54fdd4e

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
●	BT	Burns Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

# Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	RRS	Redundant Require Statement	Unresolved
●	RSML	Redundant SafeMath Library	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>
RRS - Redundant Require Statement	7
Description	7
Recommendation	7
RSML - Redundant SafeMath Library	8
Description	8
Recommendation	8
<b>Functions Analysis</b>	<b>9</b>
<b>Inheritance Graph</b>	<b>12</b>
<b>Flow Graph</b>	<b>13</b>
<b>Summary</b>	<b>14</b>
<b>Disclaimer</b>	<b>15</b>
<b>About Cyberscope</b>	<b>16</b>

## Review

<b>Contract Name</b>	JCCoin
<b>Compiler Version</b>	v0.8.22+commit.4fc1097e
<b>Optimization</b>	200 runs
<b>Explorer</b>	<a href="https://etherscan.io/address/0x03a9d7c8caf836de35666c5f7e317306b54fdd4e">https://etherscan.io/address/0x03a9d7c8caf836de35666c5f7e317306b54fdd4e</a>
<b>Address</b>	0x03a9d7c8caf836de35666c5f7e317306b54fdd4e
<b>Network</b>	ETH
<b>Symbol</b>	JCC
<b>Decimals</b>	18
<b>Total Supply</b>	500,000,000,000
<b>Badge Eligibility</b>	Yes

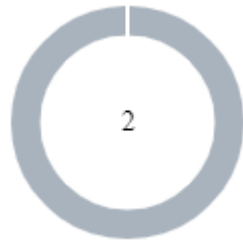
## Audit Updates

<b>Initial Audit</b>	23 Jan 2024 <a href="https://github.com/cyberscope-io/audits/blob/main/jcc/v1/audit.pdf">https://github.com/cyberscope-io/audits/blob/main/jcc/v1/audit.pdf</a>
<b>Corrected Phase 2</b>	16 Feb 2024

## Source Files

Filename	SHA256
JCCoin.sol	ad5a0e432c85cd5b69bbbac06d7660bfe4aa3c8f77713316793e5b5438a4e075

# Findings Breakdown



- Critical 0
- Medium 0
- Minor / Informative 2

Severity	Unresolved	Acknowledged	Resolved	Other
<span style="color: red;">●</span> Critical	0	0	0	0
<span style="color: gold;">●</span> Medium	0	0	0	0
<span style="color: grey;">●</span> Minor / Informative	2	0	0	0

## RRS - Redundant Require Statement

<b>Criticality</b>	Minor / Informative
<b>Location</b>	JCCoin.sol#L58
<b>Status</b>	Unresolved

### Description

The contract utilizes a `require` statement within the `add` function aiming to prevent overflow errors. This function is designed based on the SafeMath library's principles. In Solidity version 0.8.0 and later, arithmetic operations revert on overflow and underflow, making the overflow check within the function redundant. This redundancy could lead to extra gas costs and increased complexity without providing additional security.

```
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    require(c >= a, "SafeMath: addition overflow");
    return c;
}
```

### Recommendation

It is recommended to remove the `require` statement from the `add` function since the contract is using a Solidity pragma version equal to or greater than 0.8.0. By doing so, the contract will leverage the built-in overflow and underflow checks provided by the Solidity language itself, simplifying the code and reducing gas consumption. This change will uphold the contract's integrity in handling arithmetic operations while optimizing for efficiency and cost-effectiveness.



## RSML - Redundant SafeMath Library

<b>Criticality</b>	Minor / Informative
<b>Location</b>	JCCoin.sol
<b>Status</b>	Unresolved

### Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, overhead and increases gas consumption unnecessarily.

```
library SafeMath {...}
```

### Recommendation

The team is advised to remove the SafeMath library. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change on

<https://docs.soliditylang.org/en/v0.8.16/080-breaking-changes.html#solidity-v0-8-0-breaking-changes>.

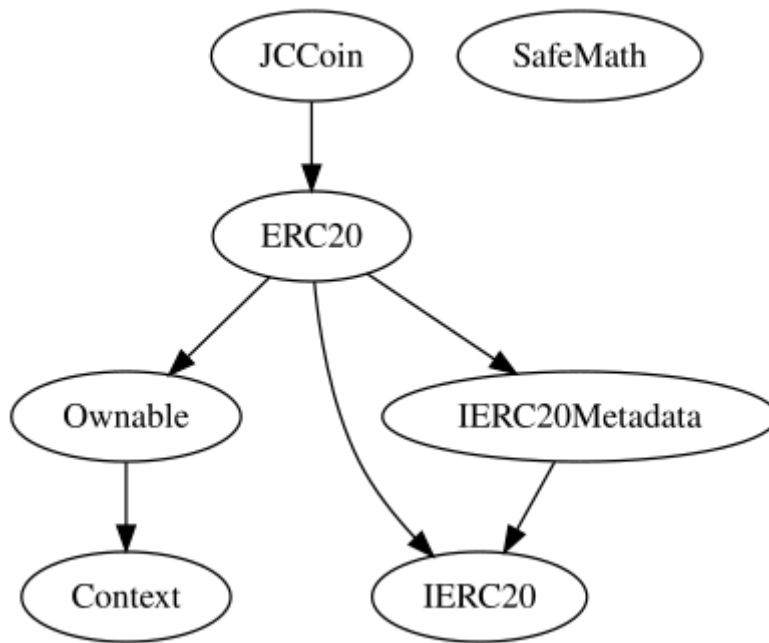
# Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>Ownable</b>	Implementation	Context		
		Public	✓	-
	owner	Public		-
	transferOwnership	Public	✓	onlyOwner
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	Library			

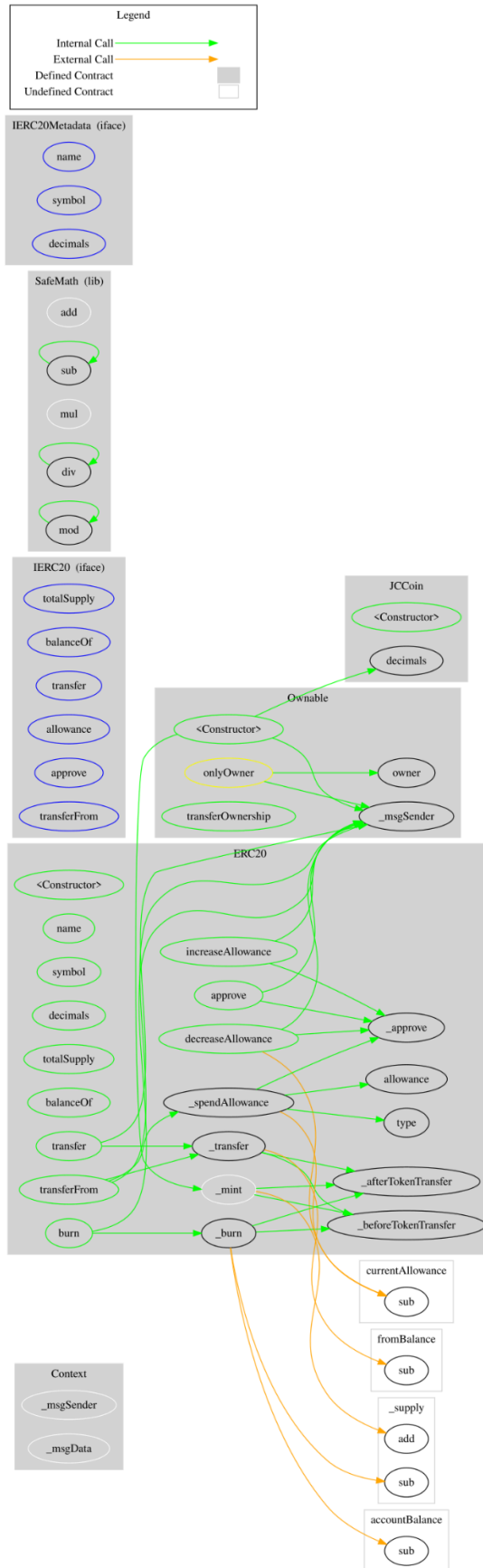
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>ERC20</b>	Implementation	Ownable, IERC20, IERC20Meta data		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-

	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	burn	Public	✓	onlyOwner
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>JCCoin</b>	Implementation	ERC20		
		Public	✓	ERC20

# Inheritance Graph



# Flow Graph



## Summary

JC Coin contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. JC Coin is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors or critical issues. 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>