



Cyberscope

## Audit Report

# Creath Governance Token

September 2023

Network    ETH

Address    0x0d4C189b7A656C134d8777D60e002C384EAdCA30

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

Severity	Code	Description	Status
●	RTC	Redundant Type Casting	Unresolved
●	L09	Dead Code Elimination	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	4
<b>Findings Breakdown</b>	<b>5</b>
RTC - Redundant Type Casting	6
Description	6
Recommendation	6
L09 - Dead Code Elimination	7
Description	7
Recommendation	8
<b>Functions Analysis</b>	<b>9</b>
<b>Inheritance Graph</b>	<b>11</b>
<b>Flow Graph</b>	<b>12</b>
<b>Summary</b>	<b>13</b>
<b>Disclaimer</b>	<b>14</b>
<b>About Cyberscope</b>	<b>15</b>

## Review

Contract Name	CreathGovernanceToken
Compiler Version	v0.8.19+commit.7dd6d404
Optimization	1 runs
Explorer	<a href="https://etherscan.io/address/0x0d4c189b7a656c134d8777d60e002c384eadca30">https://etherscan.io/address/0x0d4c189b7a656c134d8777d60e002c384eadca30</a>
Address	0x0d4c189b7a656c134d8777d60e002c384eadca30
Network	ETH
Symbol	\$CGT
Decimals	18
Total Supply	100,000,000

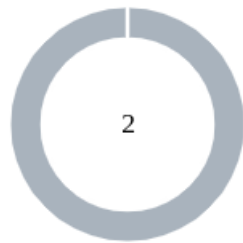
## Audit Updates

Initial Audit	18 Sep 2023 <a href="https://github.com/cyberscope-io/audits/blob/main/2-cgt/v1/token.pdf">https://github.com/cyberscope-io/audits/blob/main/2-cgt/v1/token.pdf</a>
Corrected Phase 2	28 Sep 2023

## Source Files

Filename	SHA256
CreathGovernanceToken.sol	de2605d444af111104ab6325de6252b6999fa8670ad18b2558950f02ce551376

## Findings Breakdown



● Critical	0
● Medium	0
● Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	2	0	0	0

## RTC - Redundant Type Casting

Criticality	Minor / Informative
Location	contracts/CreathGovernanceToken.sol#L506
Status	Unresolved

### Description

The contract is invoking the `_mint` function inside the constructor by using a calculation that includes `decimals`, which is redundantly cast to `uint256`. Given that `decimals` is already of type `uint8`, this explicit type casting is unnecessary and could lead to confusion. Additionally, the value of `decimals` is equal to `18`, making the type casting not only redundant but also potentially gas inefficient.

```
_mint(_distributionWallet, 100000000 * 10  
**uint256(decimals()));
```

### Recommendation

It is recommended to remove the redundant type casting of `uint256` in `decimals` variable. Since `decimals` is already type of `uint8`, the explicit type casting serves no functional purpose and could lead to misunderstandings about the code's intent.

## L09 - Dead Code Elimination

Criticality	Minor / Informative
Location	CreathGovernanceToken.sol#L407
Status	Unresolved

### Description

In Solidity, dead code is code that is written in the contract, but is never executed or reached during normal contract execution. Dead code can occur for a variety of reasons, such as:

- Conditional statements that are always false.
- Functions that are never called.
- Unreachable code (e.g., code that follows a return statement).

Dead code can make a contract more difficult to understand and maintain, and can also increase the size of the contract and the cost of deploying and interacting with it.

```
function _burn(address account, uint256 amount) internal
virtual {
    require(account != address(0), "ERC20: burn from the
zero address");

    _beforeTokenTransfer(account, address(0), amount);

    uint256 accountBalance = _balances[account];
    ...
    _totalSupply -= amount;
}

emit Transfer(account, address(0), amount);

_afterTokenTransfer(account, address(0), amount);
}
```



## Recommendation

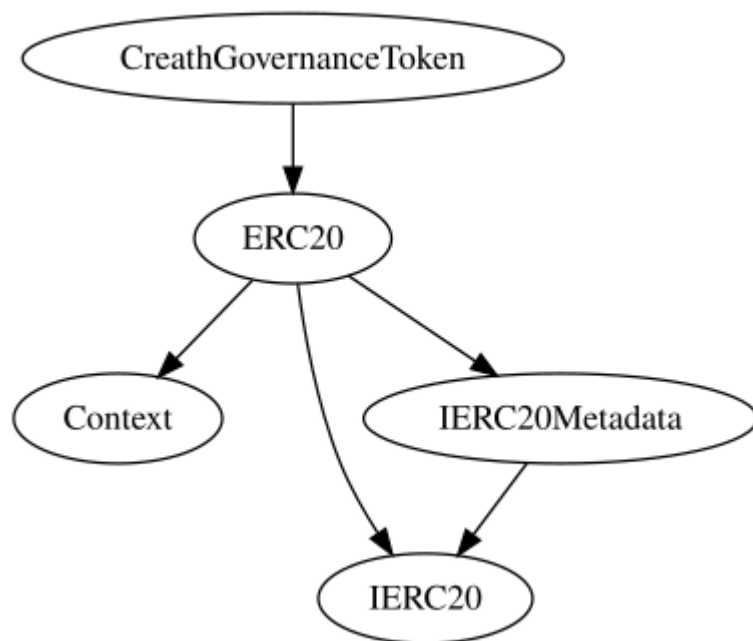
To avoid creating dead code, it's important to carefully consider the logic and flow of the contract and to remove any code that is not needed or that is never executed. This can help improve the clarity and efficiency of the contract.

# Functions Analysis

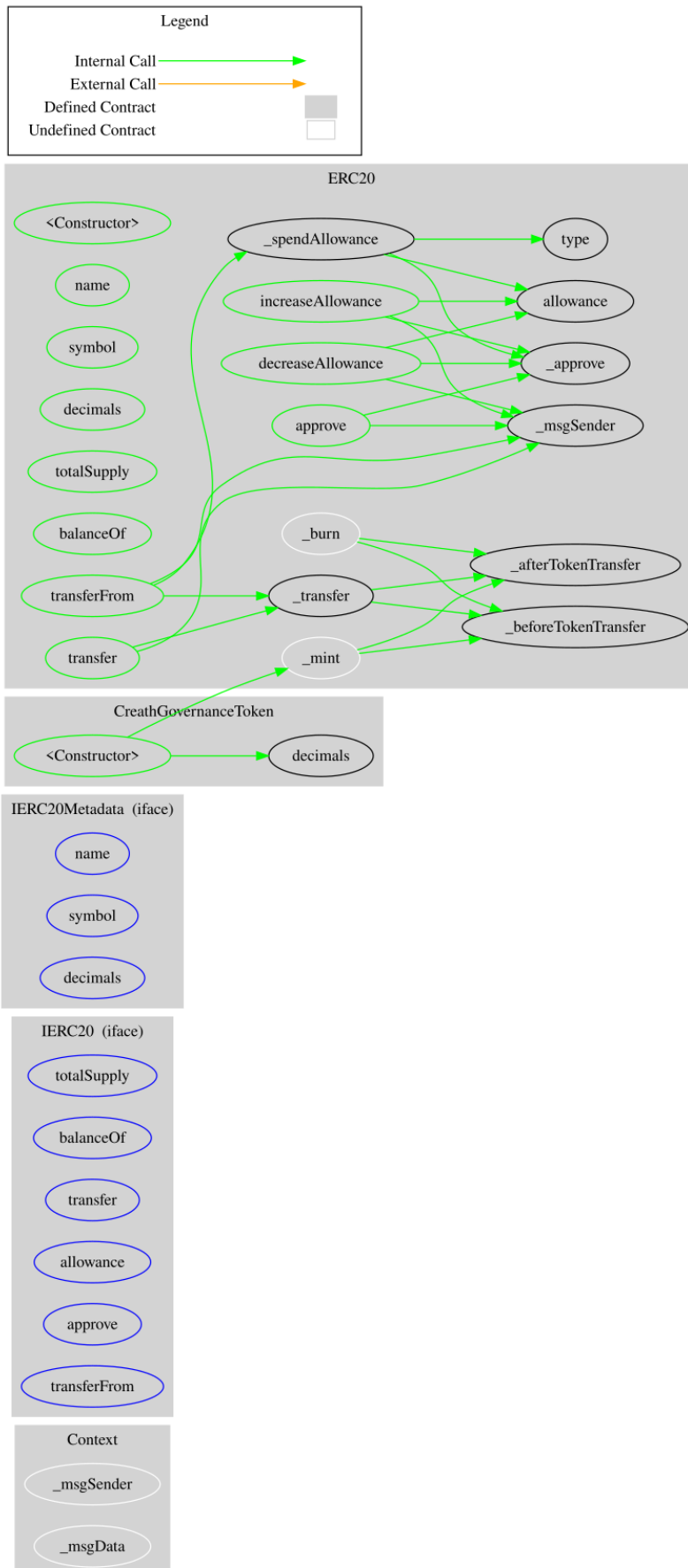
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>ERC20</b>	Implementation	Context, 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	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>CreathGovernanceToken</b>	Implementation	ERC20		
		Public	✓	ERC20

## Inheritance Graph



# Flow Graph



## Summary

Creath Governance Token contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Creath Governance Token is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error 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>