



# Cyberscope

## Audit Report

# Gary

May 2023

Network    BSC

Address    0x62a13eA6b285fd6C3261B82797669E78146BB0b1

Audited by    © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Review</b>	<b>2</b>
Audit Updates	2
Source Files	3
<b>Findings Breakdown</b>	<b>4</b>
<b>Analysis</b>	<b>5</b>
<b>Diagnostics</b>	<b>6</b>
L19 - Stable Compiler Version	7
Description	7
Recommendation	7
<b>Functions Analysis</b>	<b>8</b>
<b>Inheritance Graph</b>	<b>9</b>
<b>Flow Graph</b>	<b>10</b>
<b>Summary</b>	<b>11</b>
<b>Disclaimer</b>	<b>12</b>
<b>About Cyberscope</b>	<b>13</b>

## Review

Contract Name	GaryToken
Compiler Version	v0.8.18+commit.87f61d96
Optimization	200 runs
Explorer	<a href="https://bscscan.com/address/0x62a13ea6b285fd6c3261b82797669e78146bb0b1">https://bscscan.com/address/0x62a13ea6b285fd6c3261b82797669e78146bb0b1</a>
Address	0x62a13ea6b285fd6c3261b82797669e78146bb0b1
Network	BSC
Symbol	GARY
Decimals	18
Total Supply	8,888,888,888

## Audit Updates

Initial Audit	24 May 2023
---------------	-------------

## Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249a a4df6024fbfaa94f79ab2f44f3231
@openzeppelin/contracts/token/ERC20/ERC20.sol	bce14c3fd3b1a668529e375f6b70ffdf9cef 8c4e410ae99608be5964d98fa701
@openzeppelin/contracts/token/ERC20/extensions/ IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166 689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db800 3d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a2 3a4baa0b5bd9add9fb6d6a1549814a
contracts/Gary.sol	6a4f9dd1356bd8ac0c1ba1a556caac7834 d8428b12500a4fef82861d0b29fa90

## 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

# Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

# Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	L19	Stable Compiler Version	Unresolved

## L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	contracts/Gary.sol#L2
Status	Unresolved

### Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.18;
```

### Recommendation

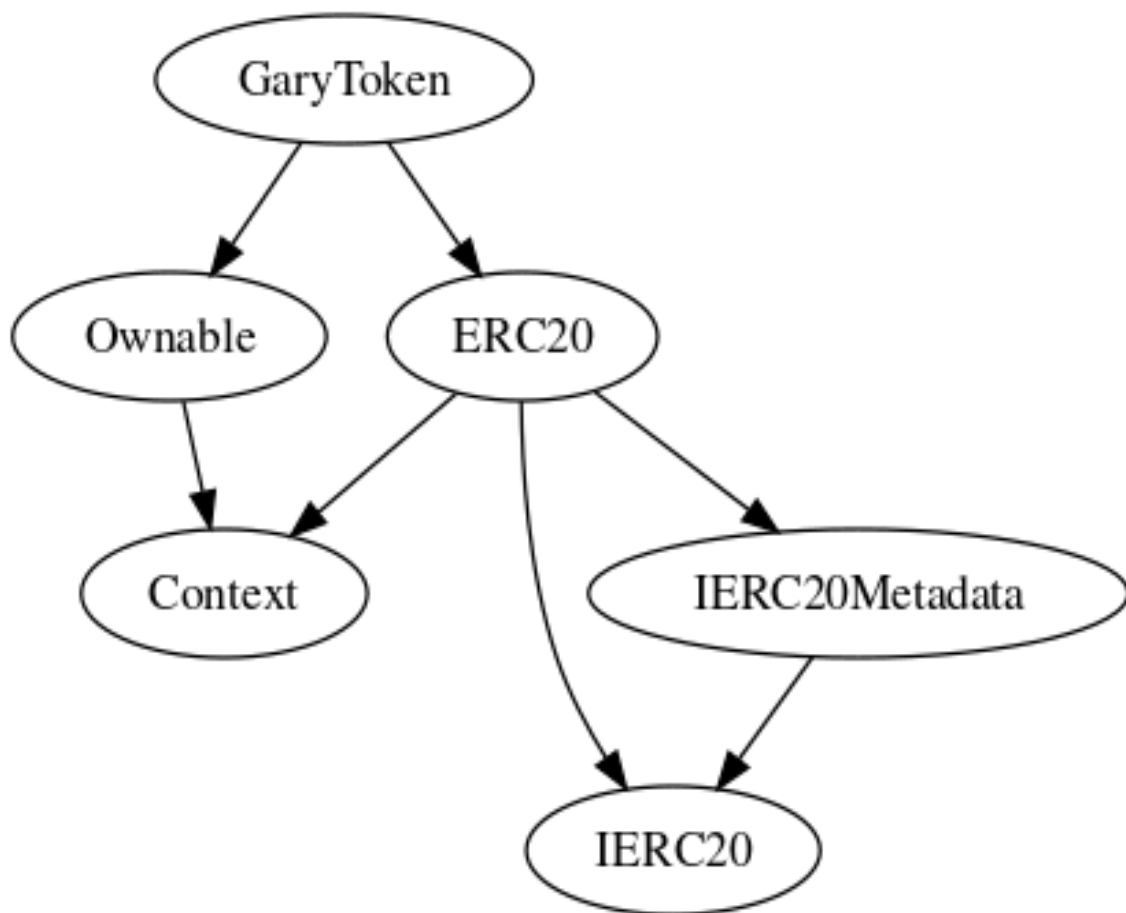
The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.



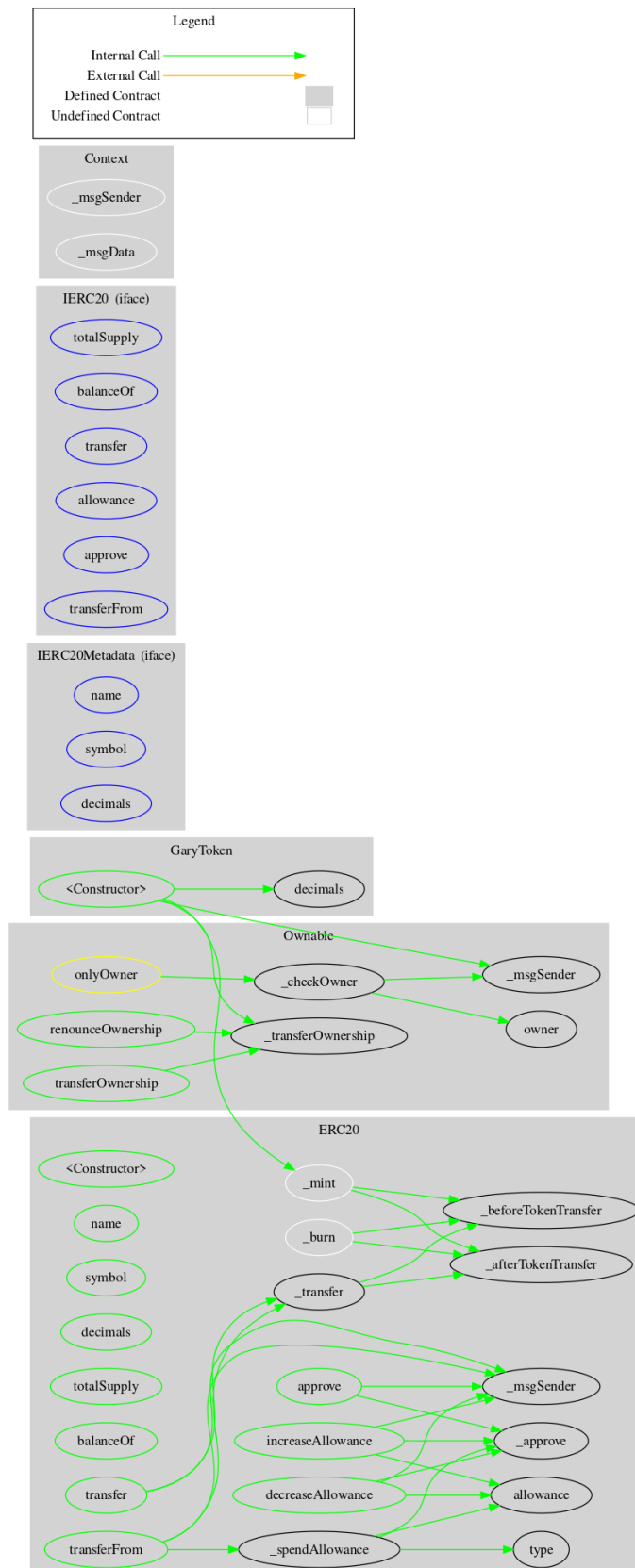
## Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
GaryToken	Implementation	ERC20, Ownable		
		Public	✓	ERC20

## Inheritance Graph



# Flow Graph



## Summary

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

## 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>