Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: Bipgo Token
Platform: Binance Smart Chain
Language: Solidity
Date: January 25th, 2022

Table of contents

Introduction 4
Project Background 4
Audit Scope 4
Claimed Smart Contract Features 5
Audit Summary 6
Technical Quick Stats 7
Code Quality 8
Documentation 8
Use of Dependencies 8
AS-IS overview 9
Severity Definitions 11
Audit Findings 12
Conclusion 13
Our Methodology 14
Disclaimers 16
Appendix

- Code Flow Diagram 17
- Slither Results Log 18
- Solidity static analysis 20
- Solhint Linter 23

Email: audit@EtherAuthority.io

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

EtherAuthority was contracted by the Bipgo team to perform the Security audit of the Bipgo Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on January 25th, 2022.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

Bipgo is a standard BEP20 token smart contract having private and public sales. This audit only considers Bipgo token smart contracts, and does not cover any other smart contracts on the platform.

Audit scope

Name	**Code Review and Security Analysis Report for Bipgo Token Smart Contract**
Platform	**BSC / Solidity**
File	BGO.sol
File MD5 Hash	3D4F3BF9B3035FFD821D3752F0D8E0BE
Online code	0xea1f61C0B57F36DA3F6e7365898b1a63227455D5
Audit Date	January 25th, 2022

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Name: Bipgo ● Symbol: BGO ● Decimals: 18 ● Total Supply: 400 Million ● Private pre sale amount cap: 10% ● Public pre sale amount cap: 4%	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **"Secured"**. This token contract does contain owner control, which does not make it fully decentralized.

We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 1 low and some very low level issues. These issues are not critical ones.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderated
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Code Quality

This audit scope has 1 smart contract file. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in Bipgo Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Bipgo Token.

The Bipgo Token team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **well** commented on smart contracts.

Documentation

We were given a Bipgo Token smart contracts code in the form of a BSCScan web link.The hash of that code is mentioned above in the table.

As mentioned above, code parts are **well** commented. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	_setDefaultValues	write	Passed	No Issue
3	_setCoinDistribution	write	Passed	No Issue
4	onlyAdmin	modifier	Passed	No Issue
5	hasPrivatePreSaleContract NotYetSet	modifier	Passed	No Issue
6	hasPublicPreSaleContractN otYetSet	modifier	Passed	No Issue
7	isPrivatePreSaleContract	modifier	Passed	No Issue
8	isPublicPreSaleContract	modifier	Passed	No Issue
9	whenPaused	modifier	Passed	No Issue
10	whenNotPaused	modifier	Passed	No Issue
11	transferOwnership	external	Critical operation lacks event log	Refer Audit Findings
12	setPrivatePreSaleContractN otYetSet	external	Access only admin	No Issue
13	setPublicPreSaleContractN otYetSet	external	Access only admin	No Issue
14	totalSupply	read	Passed	No Issue
15	balanceOf	external	Passed	No Issue
16	transfer	external	Passed	No Issue
17	allowance	external	Passed	No Issue
18	approve	external	Passed	No Issue
19	transferFrom	external	Passed	No Issue
20	increaseAllowance	write	Passed	No Issue
21	decreaseAllowance	write	Passed	No Issue
22	_transfer	internal	Passed	No Issue
23	_approve	internal	Passed	No Issue
24	transferPrivatePresale	external	Passed	No Issue
25	transferPublicPresale	external	Passed	No Issue
26	transferLocalCategories	external	Critical operation lacks event log	Refer Audit Findings
27	_categoriesTransfer	write	Passed	No Issue
28	pause	external	Access only admin	No Issue
29	unpause	external	Access only admin	No Issue
30	pausedAddress	external	Access only admin	No Issue
31	unPausedAddress	external	Access only admin	No Issue
32	receive	external	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Email: audit@EtherAuthority.io

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

(1) Critical operation lacks event log:
Missing event log for:

- transferOwnership()
- transferLocalCategories()

Resolution: We suggest writing an event log for listed events.

Very Low / Informational / Best practices:

(1) SafeMath Library:
SafeMath Library is used in this contract code, but the compiler version is greater than or equal to 0.8.0, Then it will not be required to use it, solidity automatically handles overflow / underflow.

Resolution: We suggest removing the SafeMath library and use normal math operators, It will improve code size, and less gas consumption.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- transferOwnership: The Admin can access the change of the contract administrator.
- setPrivatePreSaleContractNotYetSet: The Admin can set the address of the private sale contract.
- setPublicPreSaleContractNotYetSet: The Admin can set the address of the public sale contract.
- pause: The Admin can deactivate the contract.
- unpause:The Admin can allow you to reactivate the contract.
- pausedAddress: The Admin can deactivate an address.
- unPausedAddress: The Admin can activate an address.

Conclusion

We were given a contract code. And we have used all possible tests based on given objects as files. We have not observed any major issues in the smart contracts. So, **it's good to go to production**.

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is **"Secured"**.

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

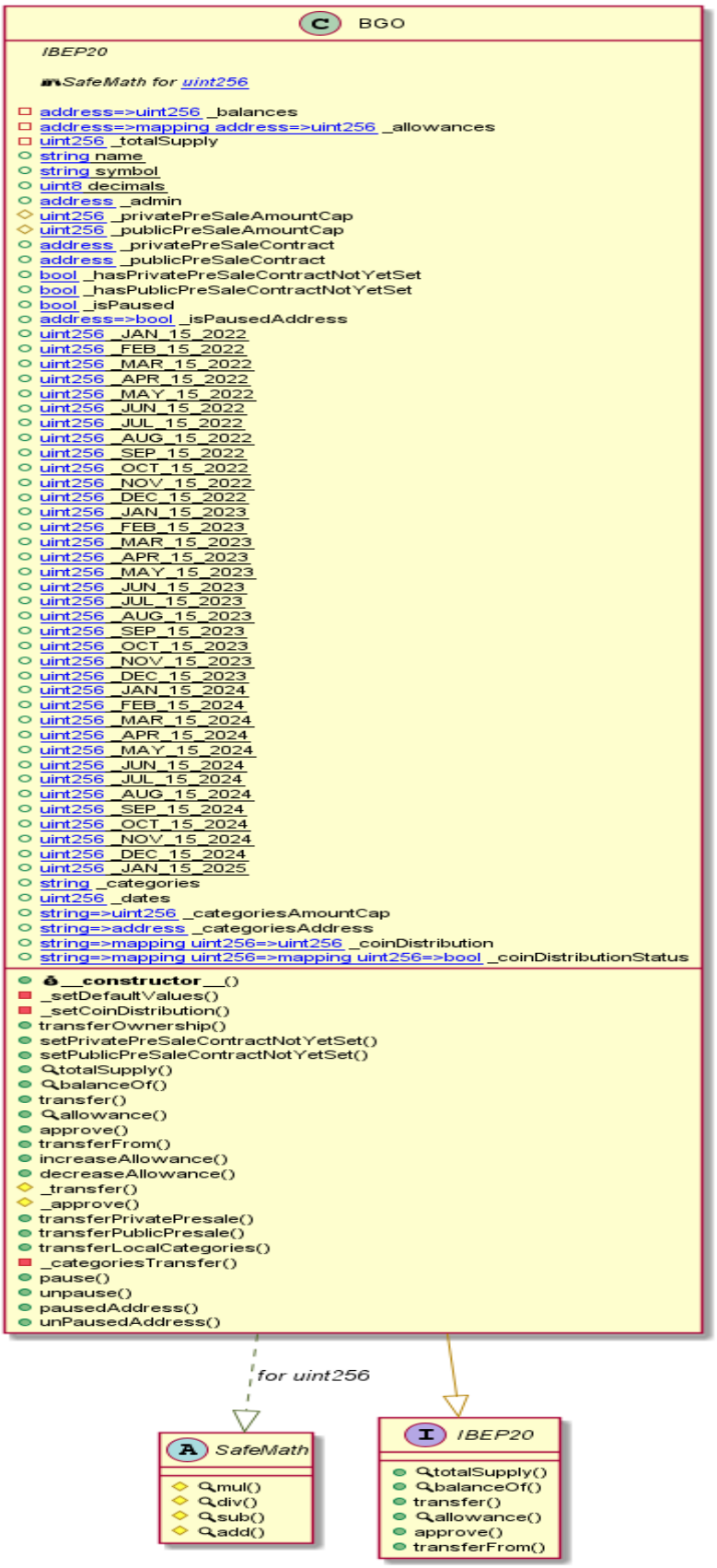
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Bipgo Token



Slither Results Log

Slither log >> BGO.sol

```
INFO:Detectors:
Contract locking ether found:
        Contract BGO (BGO.sol#126-1133) has payable functions:
         - BGO.receive() (BGO.sol#1129-1131)
        But does not have a function to withdraw the ether
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#contracts-that-lock-ether
INFO:Detectors:
BGO.transferPrivatePresale(address,uint256) (BGO.sol#1004-1016) contains a tautology or contradiction:
        - require(bool,string)(_privatePreSaleAmountCap.sub(amount) >= 0,The quantity is greater than available) (BGO.sol#1009
012)
BGO.transferPublicPresale(address,uint256) (BGO.sol#1025-1037) contains a tautology or contradiction:
        - require(bool,string)(_publicPreSaleAmountCap.sub(amount) >= 0,The quantity is greater than available) (BGO.sol#1030-
33)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#tautology-or-contradiction
INFO:Detectors:
BGO.transferOwnership(address) (BGO.sol#771-774) should emit an event for:
        - _admin = admin (BGO.sol#773)
BGO.setPrivatePreSaleContractNotYetSet(address) (BGO.sol#781-792) should emit an event for:
        - _privatePreSaleContract = privatePreSaleContract (BGO.sol#790)
BGO.setPublicPreSaleContractNotYetSet(address) (BGO.sol#799-810) should emit an event for:
        - _publicPreSaleContract = publicPreSaleContract (BGO.sol#808)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-access-control
INFO:Detectors:
BGO.transferLocalCategories() (BGO.sol#1043-1066) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp >= _dates[y] (BGO.sol#1048)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
SafeMath.div(uint256,uint256) (BGO.sol#30-35) is never used and should be removed
SafeMath.mul(uint256,uint256) (BGO.sol#18-25) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version0.8.4 (BGO.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Variable BGO._admin (BGO.sol#138) is not in mixedCase
```

```
Variable BGO._privatePreSaleAmountCap (BGO.sol#141) is not in mixedCase
Variable BGO._publicPreSaleAmountCap (BGO.sol#142) is not in mixedCase
Variable BGO._privatePreSaleContract (BGO.sol#143) is not in mixedCase
Variable BGO._publicPreSaleContract (BGO.sol#144) is not in mixedCase
Variable BGO._hasPrivatePreSaleContractNotYetSet (BGO.sol#145) is not in mixedCase
Variable BGO._hasPublicPreSaleContractNotYetSet (BGO.sol#146) is not in mixedCase
Variable BGO._isPaused (BGO.sol#149) is not in mixedCase
Variable BGO._isPausedAddress (BGO.sol#150) is not in mixedCase
Variable BGO._categories (BGO.sol#191) is not in mixedCase
Variable BGO._dates (BGO.sol#192) is not in mixedCase
Variable BGO._categoriesAmountCap (BGO.sol#193-194) is not in mixedCase
Variable BGO._categoriesAddress (BGO.sol#195) is not in mixedCase
Variable BGO._coinDistribution (BGO.sol#196-197) is not in mixedCase
Variable BGO._coinDistributionStatus (BGO.sol#198-199) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable BGO._APR_15_2022 (BGO.sol#156) is too similar to BGO._APR_15_2023 (BGO.sol#168)
Variable BGO._APR_15_2022 (BGO.sol#156) is too similar to BGO._APR_15_2024 (BGO.sol#180)
Variable BGO._APR_15_2022 (BGO.sol#156) is too similar to BGO._MAR_15_2022 (BGO.sol#155)
Variable BGO._APR_15_2023 (BGO.sol#168) is too similar to BGO._APR_15_2024 (BGO.sol#180)
Variable BGO._AUG_15_2022 (BGO.sol#160) is too similar to BGO._AUG_15_2023 (BGO.sol#172)
Variable BGO._AUG_15_2022 (BGO.sol#160) is too similar to BGO._AUG_15_2024 (BGO.sol#184)
Variable BGO._AUG_15_2023 (BGO.sol#172) is too similar to BGO._AUG_15_2024 (BGO.sol#184)
Variable BGO._DEC_15_2022 (BGO.sol#164) is too similar to BGO._DEC_15_2023 (BGO.sol#176)
Variable BGO._DEC_15_2022 (BGO.sol#164) is too similar to BGO._DEC_15_2024 (BGO.sol#188)
Variable BGO._DEC_15_2023 (BGO.sol#176) is too similar to BGO._DEC_15_2024 (BGO.sol#188)
Variable BGO._FEB_15_2022 (BGO.sol#154) is too similar to BGO._FEB_15_2023 (BGO.sol#166)
Variable BGO._FEB_15_2023 (BGO.sol#166) is too similar to BGO._FEB_15_2024 (BGO.sol#178)
Variable BGO._FEB_15_2022 (BGO.sol#154) is too similar to BGO._FEB_15_2024 (BGO.sol#178)
Variable BGO._JAN_15_2022 (BGO.sol#153) is too similar to BGO._JAN_15_2023 (BGO.sol#165)
Variable BGO._JAN_15_2023 (BGO.sol#165) is too similar to BGO._JAN_15_2024 (BGO.sol#177)
Variable BGO._JAN_15_2023 (BGO.sol#165) is too similar to BGO._JAN_15_2025 (BGO.sol#189)
Variable BGO._JAN_15_2023 (BGO.sol#165) is too similar to BGO._JUN_15_2023 (BGO.sol#170)
Variable BGO._JAN_15_2022 (BGO.sol#153) is too similar to BGO._JAN_15_2024 (BGO.sol#177)
Variable BGO._JAN_15_2024 (BGO.sol#177) is too similar to BGO._JAN_15_2025 (BGO.sol#189)
Variable BGO._JAN_15_2024 (BGO.sol#177) is too similar to BGO._JUN_15_2024 (BGO.sol#182)
Variable BGO._JAN_15_2022 (BGO.sol#153) is too similar to BGO._JAN_15_2025 (BGO.sol#189)
```

```
Variable BGO._JAN_15_2023 (BGO.sol#165) is too similar to BGO._JUN_15_2023 (BGO.sol#170)
Variable BGO._JAN_15_2022 (BGO.sol#153) is too similar to BGO._JAN_15_2024 (BGO.sol#177)
Variable BGO._JAN_15_2024 (BGO.sol#177) is too similar to BGO._JAN_15_2025 (BGO.sol#189)
Variable BGO._JAN_15_2024 (BGO.sol#177) is too similar to BGO._JUN_15_2024 (BGO.sol#182)
Variable BGO._JAN_15_2022 (BGO.sol#153) is too similar to BGO._JAN_15_2025 (BGO.sol#189)
Variable BGO._JUL_15_2022 (BGO.sol#159) is too similar to BGO._JUL_15_2023 (BGO.sol#171)
Variable BGO._JUL_15_2022 (BGO.sol#159) is too similar to BGO._JUL_15_2024 (BGO.sol#183)
Variable BGO._JUL_15_2023 (BGO.sol#171) is too similar to BGO._JUL_15_2024 (BGO.sol#183)
Variable BGO._JAN_15_2022 (BGO.sol#153) is too similar to BGO._JUN_15_2022 (BGO.sol#158)
Variable BGO._JUL_15_2022 (BGO.sol#159) is too similar to BGO._JUN_15_2022 (BGO.sol#158)
Variable BGO._JUN_15_2022 (BGO.sol#158) is too similar to BGO._JUN_15_2023 (BGO.sol#170)
Variable BGO._JUN_15_2022 (BGO.sol#158) is too similar to BGO._JUN_15_2024 (BGO.sol#182)
Variable BGO._JUL_15_2023 (BGO.sol#171) is too similar to BGO._JUN_15_2023 (BGO.sol#170)
Variable BGO._JUN_15_2023 (BGO.sol#170) is too similar to BGO._JUN_15_2024 (BGO.sol#182)
Variable BGO._JUL_15_2024 (BGO.sol#183) is too similar to BGO._JUN_15_2024 (BGO.sol#182)
Variable BGO._MAR_15_2022 (BGO.sol#155) is too similar to BGO._MAR_15_2023 (BGO.sol#167)
Variable BGO._MAR_15_2022 (BGO.sol#155) is too similar to BGO._MAR_15_2024 (BGO.sol#179)
```

```
Variable BGO._MAR_15_2022 (BGO.sol#155) is too similar to BGO._MAR_15_2024 (BGO.sol#179)
Variable BGO._MAR_15_2022 (BGO.sol#155) is too similar to BGO._MAY_15_2022 (BGO.sol#157)
Variable BGO._APR_15_2023 (BGO.sol#168) is too similar to BGO._MAR_15_2023 (BGO.sol#167)
Variable BGO._MAR_15_2023 (BGO.sol#167) is too similar to BGO._MAR_15_2024 (BGO.sol#179)
Variable BGO._MAR_15_2023 (BGO.sol#167) is too similar to BGO._MAY_15_2023 (BGO.sol#169)
Variable BGO._APR_15_2024 (BGO.sol#180) is too similar to BGO._MAR_15_2024 (BGO.sol#179)
Variable BGO._MAR_15_2024 (BGO.sol#179) is too similar to BGO._MAY_15_2024 (BGO.sol#181)
Variable BGO._MAY_15_2022 (BGO.sol#157) is too similar to BGO._MAY_15_2023 (BGO.sol#169)
Variable BGO._MAY_15_2022 (BGO.sol#157) is too similar to BGO._MAY_15_2024 (BGO.sol#181)
Variable BGO._MAY_15_2023 (BGO.sol#169) is too similar to BGO._MAY_15_2024 (BGO.sol#181)
Variable BGO._NOV_15_2022 (BGO.sol#163) is too similar to BGO._NOV_15_2023 (BGO.sol#175)
Variable BGO._NOV_15_2022 (BGO.sol#163) is too similar to BGO._NOV_15_2024 (BGO.sol#187)
Variable BGO._NOV_15_2023 (BGO.sol#175) is too similar to BGO._NOV_15_2024 (BGO.sol#187)
Variable BGO._OCT_15_2022 (BGO.sol#162) is too similar to BGO._OCT_15_2023 (BGO.sol#174)
Variable BGO._OCT_15_2022 (BGO.sol#162) is too similar to BGO._OCT_15_2024 (BGO.sol#186)
Variable BGO._OCT_15_2023 (BGO.sol#174) is too similar to BGO._OCT_15_2024 (BGO.sol#186)
Variable BGO._SEP_15_2022 (BGO.sol#161) is too similar to BGO._SEP_15_2023 (BGO.sol#173)
Variable BGO._SEP_15_2022 (BGO.sol#161) is too similar to BGO._SEP_15_2024 (BGO.sol#185)
Variable BGO._SEP_15_2023 (BGO.sol#173) is too similar to BGO._SEP_15_2024 (BGO.sol#185)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
INFO:Detectors:
BGO.slitherConstructorConstantVariables() (BGO.sol#126-1133) uses literals with too many digits:
        - _SEP_15_2022 = 1663200000 (BGO.sol#161)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
totalSupply() should be declared external:
        - BGO.totalSupply() (BGO.sol#817-819)
increaseAllowance(address,uint256) should be declared external:
        - BGO.increaseAllowance(address,uint256) (BGO.sol#916-926)
decreaseAllowance(address,uint256) should be declared external:
        - BGO.decreaseAllowance(address,uint256) (BGO.sol#935-945)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:BGO.sol analyzed (3 contracts with 75 detectors), 81 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

BGO.sol

Security

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

more

Pos: 1048:20:

Gas & Economy

Gas costs:

Gas requirement of function BGO.name is infinite:
If the gas requirement of a function is higher than the block gas limit, it cannot be executed.
Please avoid loops in your functions or actions that modify large areas of storage
(this includes clearing or copying arrays in storage)
Pos: 135:4:

Gas costs:

Gas requirement of function BGO.increaseAllowance is infinite:
If the gas requirement of a function is higher than the block gas limit, it cannot be executed.
Please avoid loops in your functions or actions that modify large areas of storage
(this includes clearing or copying arrays in storage)
Pos: 916:4:

Gas costs:

Gas requirement of function BGO.decreaseAllowance is infinite:
If the gas requirement of a function is higher than the block gas limit, it cannot be executed.
Please avoid loops in your functions or actions that modify large areas of storage
(this includes clearing or copying arrays in storage)
Pos: 935:4:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point.
Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.

more

Pos: 1046:12:

Email: audit@EtherAuthority.io

Miscellaneous

Constant/View/Pure functions:

IBEP20.transfer(address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 74:4:

Similar variable names:

BGO._setDefaultValues() : Variables have very similar names "_JAN_15_2022" and "_MAR_15_2022". Note: Modifiers are currently not considered by this static analysis.

Pos: 248:20:

Similar variable names:

BGO._setDefaultValues() : Variables have very similar names "_JAN_15_2022" and "_MAR_15_2022". Note: Modifiers are currently not considered by this static analysis.

Pos: 250:20:

Similar variable names:

BGO._setCoinDistribution() : Variables have very similar names "_JAN_15_2024" and "_MAR_15_2024". Note: Modifiers are currently not considered by this static analysis.

Pos: 494:38:

Similar variable names:

BGO._setCoinDistribution() : Variables have very similar names "_JAN_15_2024" and "_MAR_15_2024". Note: Modifiers are currently not considered by this static analysis.

Pos: 600:39:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 969:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 991:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 992:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 211:34:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 287:44:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 288:39:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 689:12:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 692:12:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 695:12:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 698:12:

Solhint Linter

BGO.sol

```
BGO.sol:3:1: Error: Compiler version 0.8.10 does not satisfy the r
semver requirement
BGO.sol:126:1: Error: Contract has 18 states declarations but allowed
no more than 15
BGO.sol:135:28: Error: Constant name must be in capitalized
SNAKE_CASE
BGO.sol:136:28: Error: Constant name must be in capitalized
SNAKE_CASE
BGO.sol:137:27: Error: Constant name must be in capitalized
SNAKE_CASE
BGO.sol:207:5: Error: Explicitly mark visibility in function (Set
ignoreConstructors to true if using solidity >=0.7.0)
BGO.sol:1048:21: Error: Avoid to make time-based decisions in your
business logic
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

Email: audit@EtherAuthority.io