EtherAuthority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	Deflationary Token
Website:	deflationarytoken.com
Platform:	Binance Smart Chain
Language:	Solidity
Date:	March 11th, 2023

Table of contents

`

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.

Introduction

EtherAuthority was contracted by the Deflationary Token team to perform the Security audit of the Deflationary 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 March 11th, 2023.

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

- The Deflationary is a DEF token smart contract in Binance Smart Chain.
- DEF is the native utility token for the DEFswap Finance platform.
- DEF is a true deflationary token with a use case and a goal of creating financial literacy.
- DEF tokens can also be used to purchase DEF NFTs directly from the NFT store.
- Converting DEF token into fiat is not required before making online purchases at most retail platforms like Shopify and more.
- Inflation is a lifetime problem and $DEF has a lifetime deflationary solution.

Audit scope

Name	**Code Review and Security Analysis Report for Deflationary Token Smart Contract**
Platform	**BSC / Solidity**
File	Deflationary.sol
File MD5 Hash	91D93A6F2E9BC7027D92B39E4B97F037
Audit Date	March 11th, 2023

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Name: Deflationary ● Symbol: DEF ● Decimals: 9 ● Total Supply: 1 Quadrillion ● The automatic 3% BURN on every transaction will continue even after manual burn is complete.	**YES, This is valid.**
<u>Owner Specifications:</u> ● The owner can check if the account is excluded or not and set the account status to true. ● The owner can check if the account is excluded or not and set the account status to false. ● The address for the fee can be set by the owner.	**YES, This is valid.**

Audit Summary

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

Insecure
Poor secured
Secure
Well-secured
You are here

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, 1 medium and 0 low and some very low level issues.

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	Moderate
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	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. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in the Deflationary 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 Deflationary Token.

The Deflationary 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 not well commented on in the smart contracts. Ethereum's NatSpec commenting style is used, which is a good thing.

Documentation

We were given a Deflationary Token smart contract 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 **not well** commented. But the logic is straightforward. 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.

Another source of information was its official website: https://deflationarytoken.com which provided rich information about the project architecture and tokenomics.

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 not used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	name	write	Passed	No Issue
7	symbol	write	Passed	No Issue
8	decimals	write	Passed	No Issue
9	totalSupply	read	Passed	No Issue
10	balanceOf	read	Passed	No Issue
11	transfer	write	Passed	No Issue
12	allowance	read	Passed	No Issue
13	approve	write	Passed	No Issue
14	transferFrom	write	Passed	No Issue
15	increaseAllowance	write	Passed	No Issue
16	decreaseAllowance	write	Passed	No Issue
17	isExcludedFromReward	read	Passed	No Issue
18	totalRfiFees	read	Passed	No Issue
19	totalBurnFees	read	Passed	No Issue
20	reflectionFromToken	read	Passed	No Issue
21	tokenFromReflection	read	Passed	No Issue
22	excludeFromReward	write	access only Owner	No Issue
23	includeInReward	external	access only Owner	No Issue
24	excludeFromFee	write	access only Owner	No Issue
25	includeInFee	write	access only Owner	No Issue
26	isExcludedFromFee	read	Passed	No Issue
27	setFeeRates	write	Function input parameters lack of check	Refer to audit findings
28	_reflectRfi	write	Passed	No Issue
29	_takeBurn	write	Passed	No Issue
30	_getValues	read	Passed	No Issue
31	_getTValues	read	Passed	No Issue
32	_getRValues	write	Passed	No Issue
33	_getRate	read	Passed	No Issue
34	_getCurrentSupply	read	Passed	No Issue
35	_approve	write	Passed	No Issue
36	_transfer	write	Passed	No Issue
37	_tokenTransfer	write	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.

Audit Findings

Critical Severity

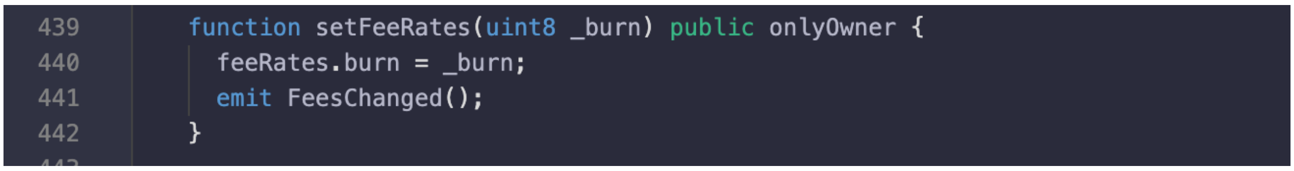
No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

(1) Function input parameters lack of check:



```
    function setFeeRates(uint8 _burn) public onlyOwner {
      feeRates.burn = _burn;
      emit FeesChanged();
    }
```

By this, the owner can set any number for the burn fee.

Resolution: We suggest validating the input and set some range for burn fee. In case the owner's private key is compromised, then an attacker can misuse this function to harm the token holders.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Consider using the latest solidity compiler while deploying:

Although this does not create major security vulnerabilities, the latest solidity version has lots of improvements, so it's recommended to use the latest solidity version, which is 0.8.19 at the time of this audit.

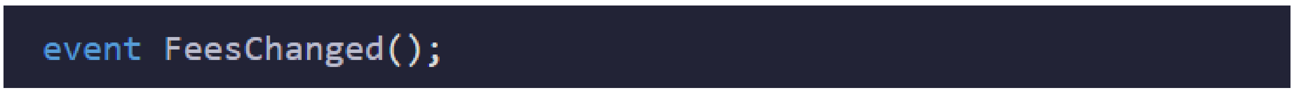
Resolution: We suggest using the latest solidity version.

(2) No need to use SafeMath library for solidity version over 0.8.0:

The solidity version over 0.8.0 has an in-built overflow/underflow prevention mechanism. And thus, the explicit use of SathMath library is not necessary. It saves some gas as well.

Resolution: We suggest removing the SafeMath library.

(3) An event with no parameters:



```
event FeesChanged();
```

An event is defined and emitted without parameters.

Resolution: We suggest having an event with proper parameters to store the arguments passed in transaction logs.

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:

- excludeFromReward: The owner can check if the account is excluded or not and set the account status to true.
- includeInReward: The owner can check if the account is excluded or not and set the account status to false.
- excludeFromFee: The owner can set excluded account fees status true.
- includeInFee: The owner can set excluded account fees status false.
- setFeeRates: The owner can set fee rates.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code in the form of a bscscan.com link and we have used all possible tests based on given objects as files. We have observed 1 medium and some informational severity issues in the token smart contract. But those issues are not critical. So, **it's good to go for the mainnet deployment**.

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.

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

The security state of the reviewed smart 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).

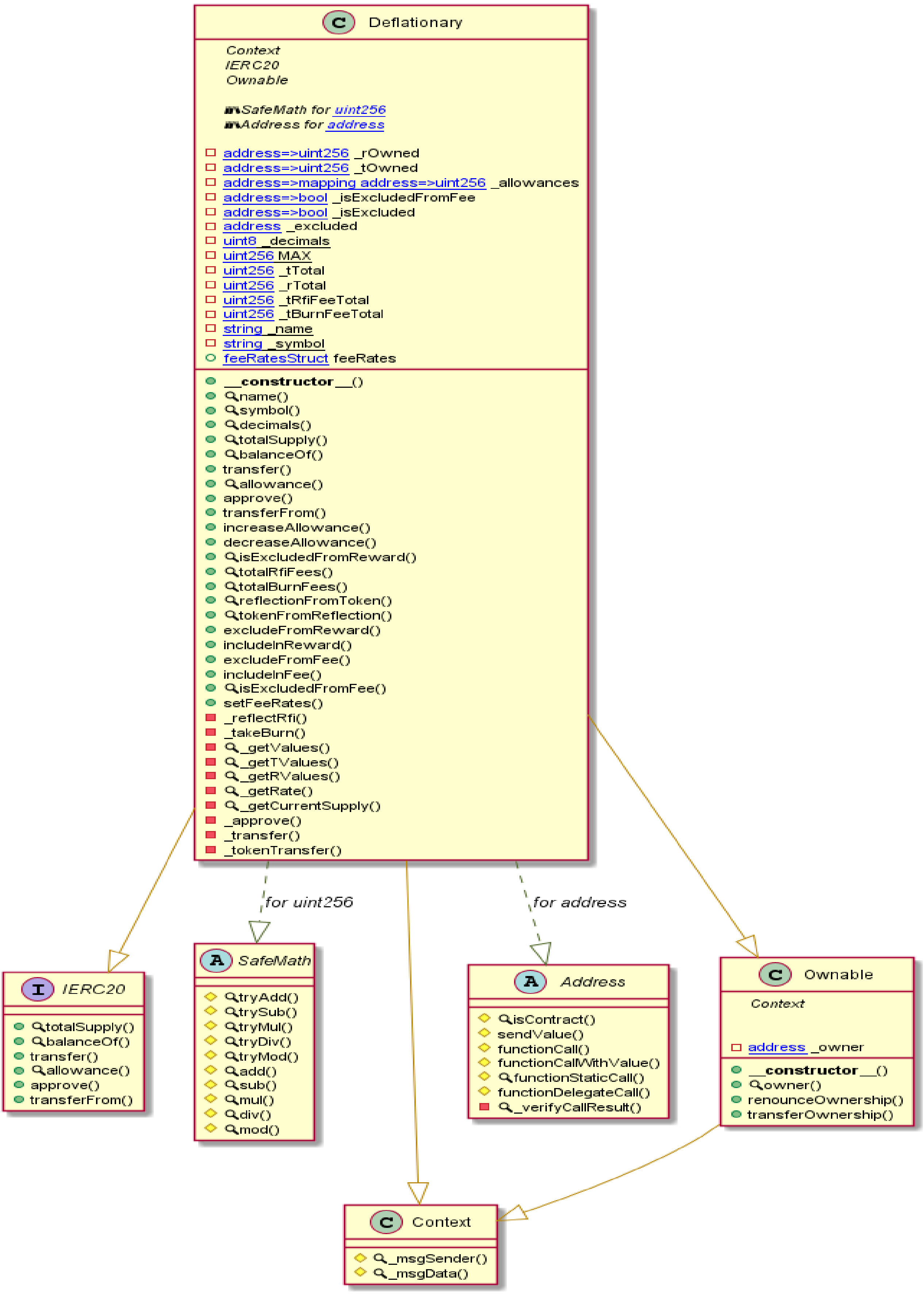
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we 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.

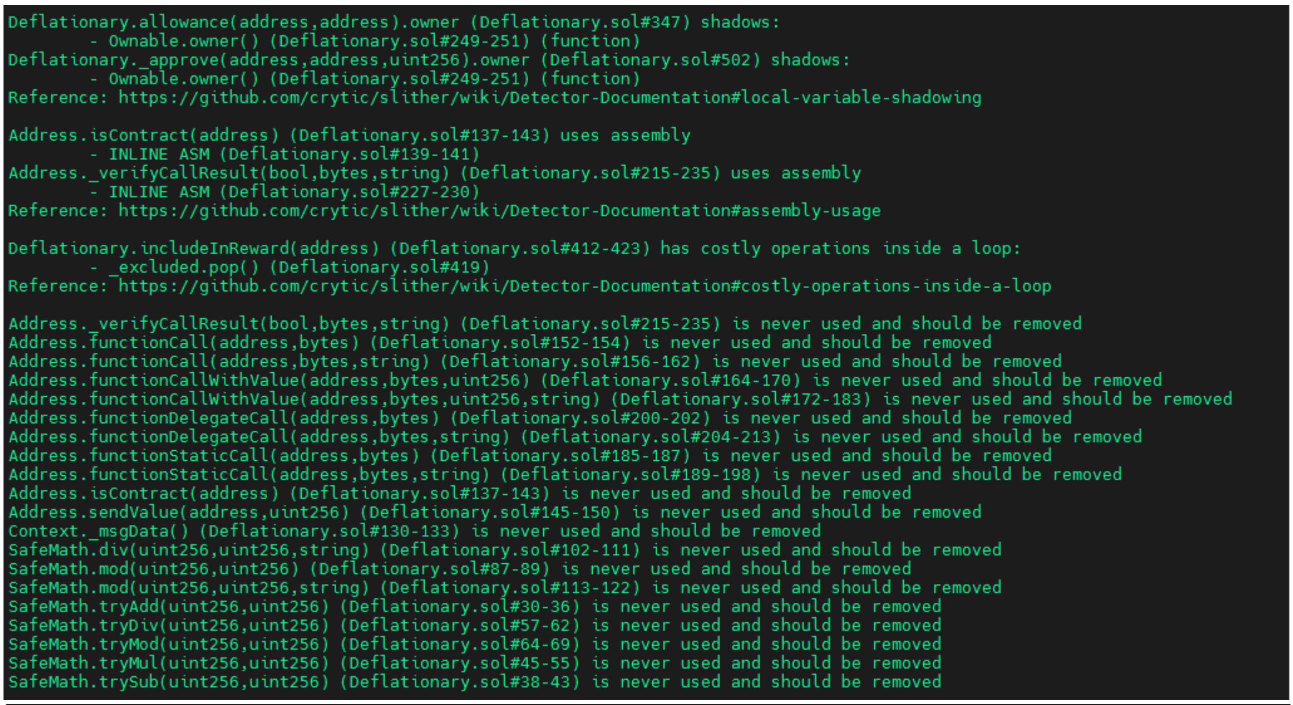
Appendix

Code Flow Diagram - Deflationary Token

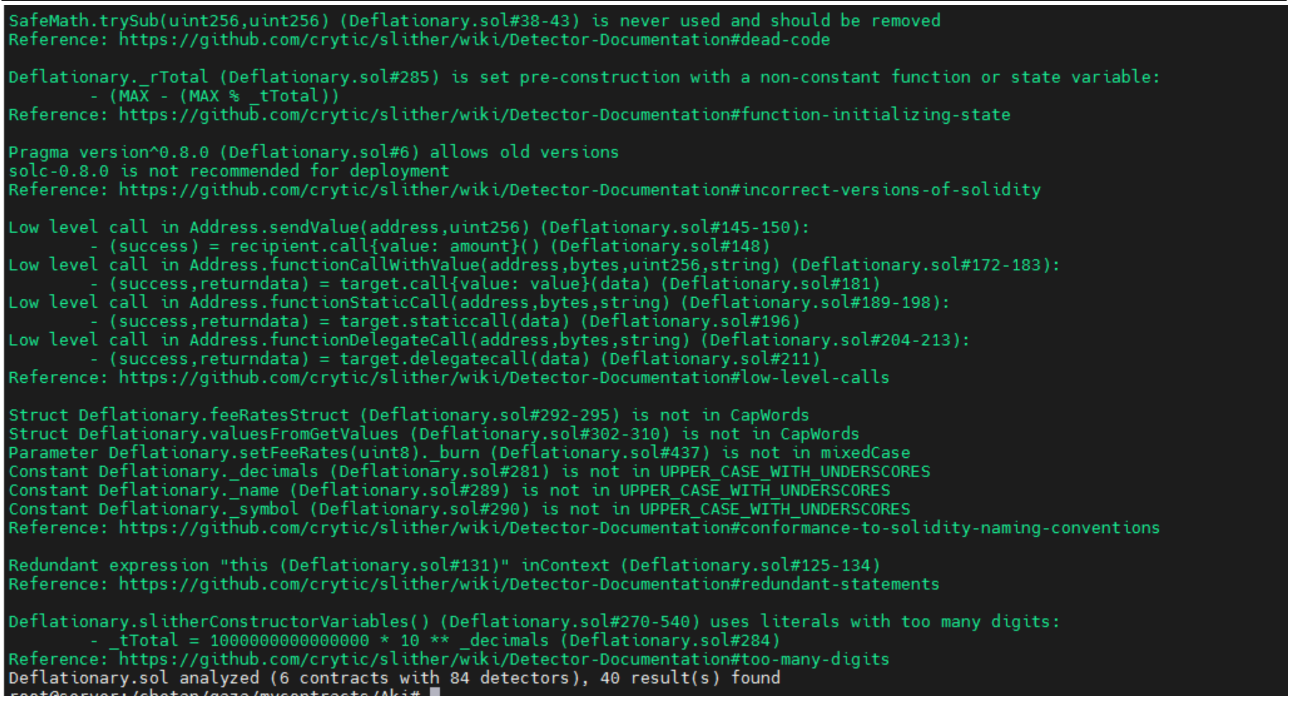


Slither Results Log

Slither Log >> Deflationary.sol



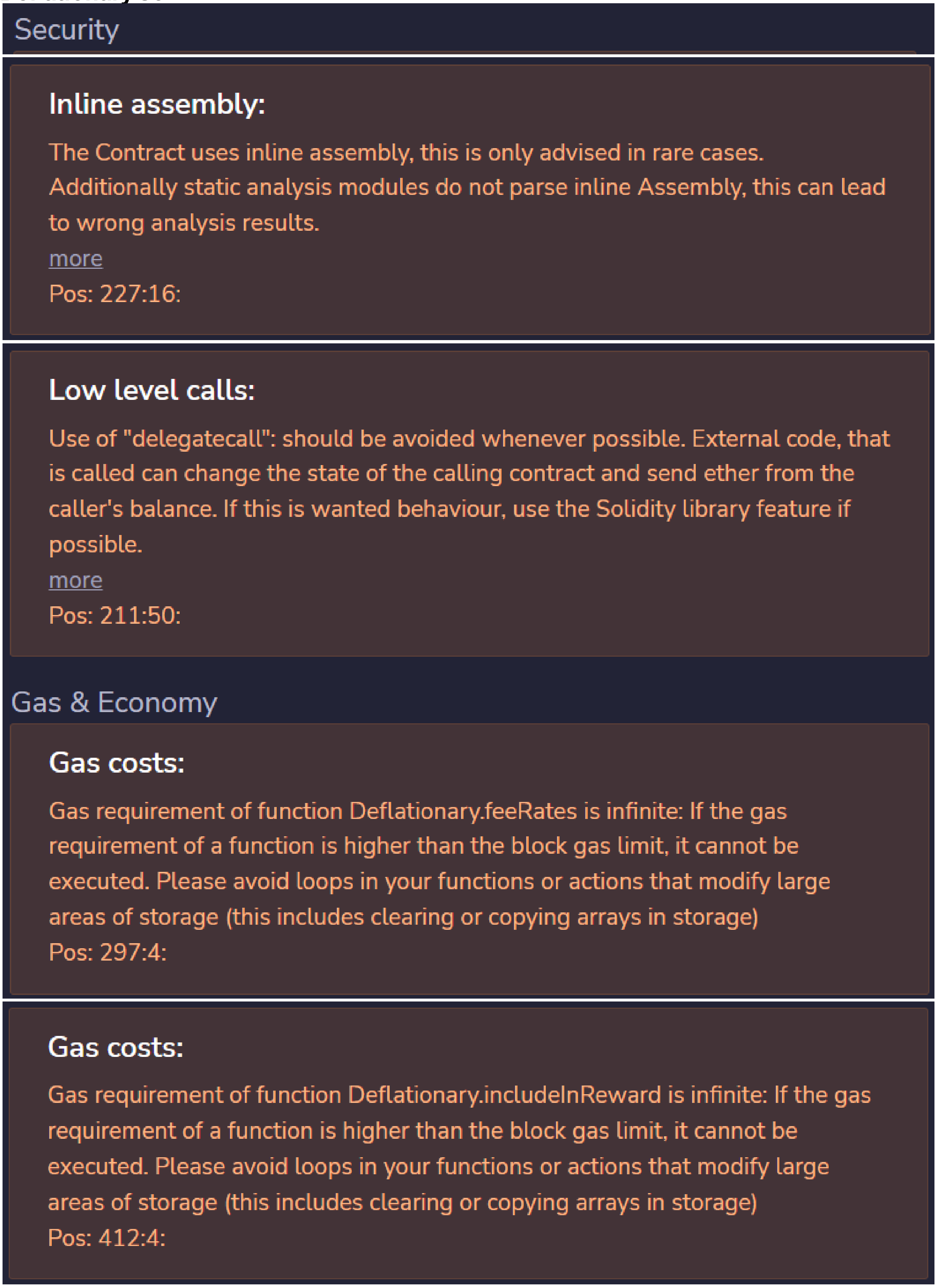
```
Deflationary.allowance(address,address).owner (Deflationary.sol#347) shadows:
        - Ownable.owner() (Deflationary.sol#249-251) (function)
Deflationary._approve(address,address,uint256).owner (Deflationary.sol#502) shadows:
        - Ownable.owner() (Deflationary.sol#249-251) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing

Address.isContract(address) (Deflationary.sol#137-143) uses assembly
        - INLINE ASM (Deflationary.sol#139-141)
Address._verifyCallResult(bool,bytes,string) (Deflationary.sol#215-235) uses assembly
        - INLINE ASM (Deflationary.sol#227-230)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage

Deflationary.includeInReward(address) (Deflationary.sol#412-423) has costly operations inside a loop:
        - _excluded.pop() (Deflationary.sol#419)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop

Address._verifyCallResult(bool,bytes,string) (Deflationary.sol#215-235) is never used and should be removed
Address.functionCall(address,bytes) (Deflationary.sol#152-154) is never used and should be removed
Address.functionCall(address,bytes,string) (Deflationary.sol#156-162) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (Deflationary.sol#164-170) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (Deflationary.sol#172-183) is never used and should be removed
Address.functionDelegateCall(address,bytes) (Deflationary.sol#200-202) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (Deflationary.sol#204-213) is never used and should be removed
Address.functionStaticCall(address,bytes) (Deflationary.sol#185-187) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (Deflationary.sol#189-198) is never used and should be removed
Address.isContract(address) (Deflationary.sol#137-143) is never used and should be removed
Address.sendValue(address,uint256) (Deflationary.sol#145-150) is never used and should be removed
Context._msgData() (Deflationary.sol#130-133) is never used and should be removed
SafeMath.div(uint256,uint256,string) (Deflationary.sol#102-111) is never used and should be removed
SafeMath.mod(uint256,uint256) (Deflationary.sol#87-89) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Deflationary.sol#113-122) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (Deflationary.sol#30-36) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (Deflationary.sol#57-62) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (Deflationary.sol#64-69) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (Deflationary.sol#45-55) is never used and should be removed
SafeMath.trySub(uint256,uint256) (Deflationary.sol#38-43) is never used and should be removed
```



```
SafeMath.trySub(uint256,uint256) (Deflationary.sol#38-43) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Deflationary._rTotal (Deflationary.sol#285) is set pre-construction with a non-constant function or state variable:
        - (MAX - (MAX % _tTotal))
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state

Pragma version^0.8.0 (Deflationary.sol#6) allows old versions
solc-0.8.0 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (Deflationary.sol#145-150):
        - (success) = recipient.call{value: amount}() (Deflationary.sol#148)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (Deflationary.sol#172-183):
        - (success,returndata) = target.call{value: value}(data) (Deflationary.sol#181)
Low level call in Address.functionStaticCall(address,bytes,string) (Deflationary.sol#189-198):
        - (success,returndata) = target.staticcall(data) (Deflationary.sol#196)
Low level call in Address.functionDelegateCall(address,bytes,string) (Deflationary.sol#204-213):
        - (success,returndata) = target.delegatecall(data) (Deflationary.sol#211)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Struct Deflationary.feeRatesStruct (Deflationary.sol#292-295) is not in CapWords
Struct Deflationary.valuesFromGetValues (Deflationary.sol#302-310) is not in CapWords
Parameter Deflationary.setFeeRates(uint8)._burn (Deflationary.sol#437) is not in mixedCase
Constant Deflationary._decimals (Deflationary.sol#281) is not in UPPER_CASE_WITH_UNDERSCORES
Constant Deflationary._name (Deflationary.sol#289) is not in UPPER_CASE_WITH_UNDERSCORES
Constant Deflationary._symbol (Deflationary.sol#290) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (Deflationary.sol#131)" inContext (Deflationary.sol#125-134)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

Deflationary.slitherConstructorVariables() (Deflationary.sol#270-540) uses literals with too many digits:
        - _tTotal = 1000000000000000 * 10 ** _decimals (Deflationary.sol#284)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
Deflationary.sol analyzed (6 contracts with 84 detectors), 40 result(s) found
```

Solidity Static Analysis

Deflationary.sol



Security

Inline assembly:

The Contract uses inline assembly, this is only advised in rare cases. Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.

more

Pos: 227:16:

Low level calls:

Use of "delegatecall": should be avoided whenever possible. External code, that is called can change the state of the calling contract and send ether from the caller's balance. If this is wanted behaviour, use the Solidity library feature if possible.

more

Pos: 211:50:

Gas & Economy

Gas costs:

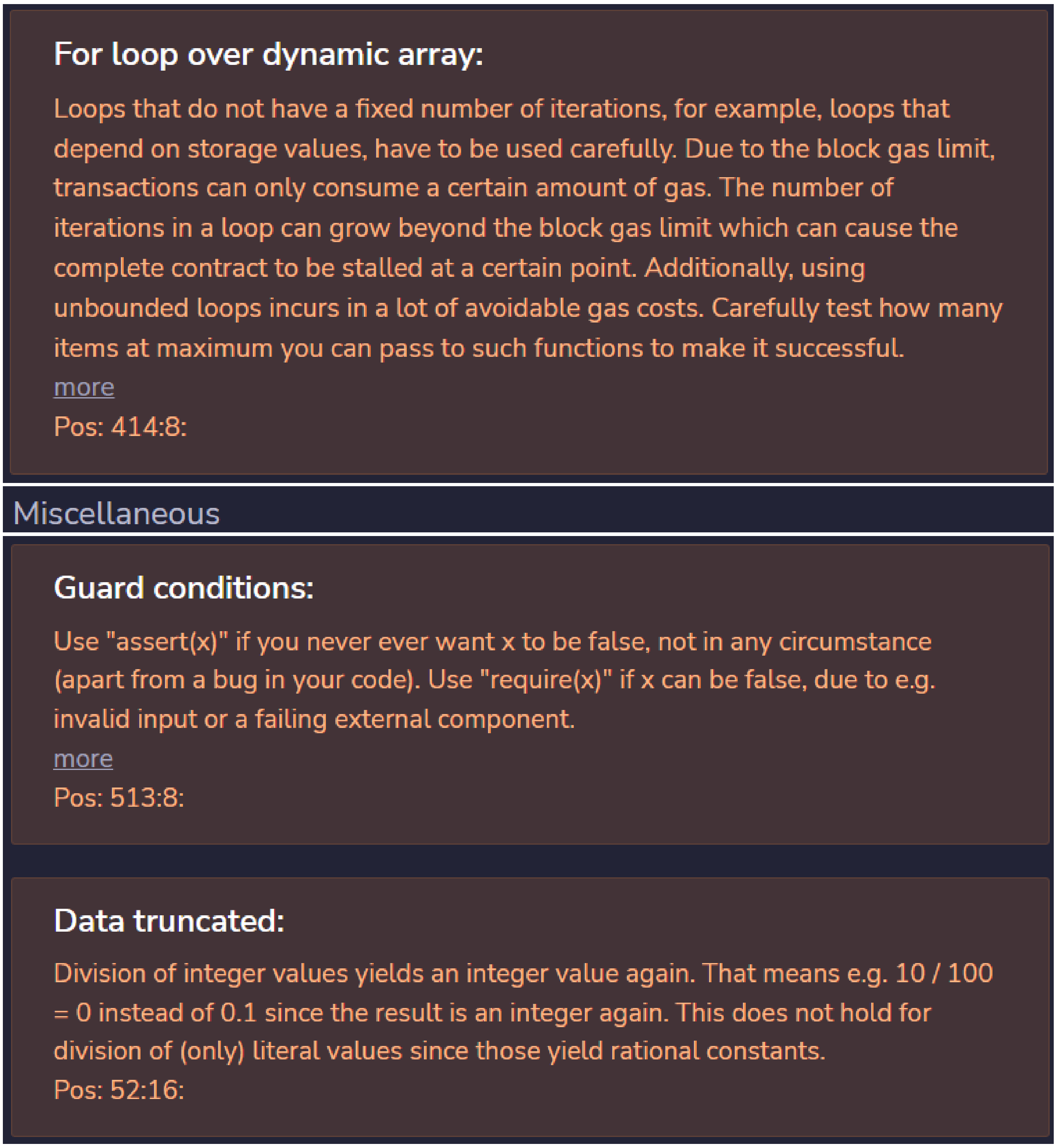
Gas requirement of function Deflationary.feeRates is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 297:4:

Gas costs:

Gas requirement of function Deflationary.includeInReward 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: 412:4:



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: 414:8:

Miscellaneous

Guard conditions:

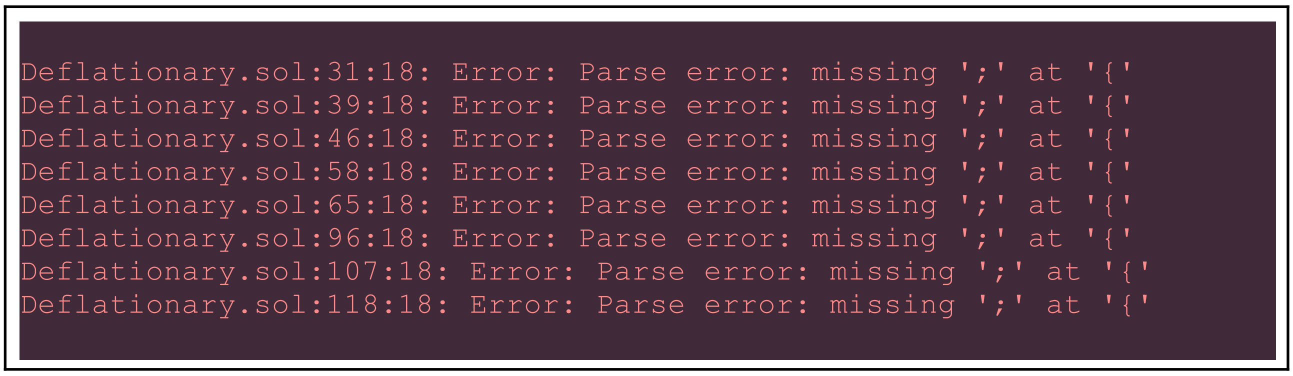
Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 513:8:

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: 52:16:

Solhint Linter

Deflationary.sol



```
Deflationary.sol:31:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:39:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:46:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:58:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:65:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:96:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:107:18: Error: Parse error: missing ';' at '{'
Deflationary.sol:118:18: Error: Parse error: missing ';' at '{'
```

Software analysis result:

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

EtherAuthority