Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	IoTeX Network
Website:	iotex.io
Platform:	Ethereum
Language:	Solidity
Date:	February 24th, 2024

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

As part of EtherAuthority's community smart contracts audit initiatives, the IoTeX Network smart contract from iotex.io was audited extensively. 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 February 24th, 2024.

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 IoTeXNetwork contract inherits from StandardToken and Pausable, implementing the IoTeX Network Token. It sets the token's parameters such as \`name\`, \`symbol\`, \`decimals\`, and \`totalSupply\`. The contract also overrides certain functions to add additional checks and behaviors specific to the IoTeX Network token.
- This code provides a complete implementation of an ERC20 token contract for the IoTeX Network Token, including functionality for transferring tokens, managing allowances, pausing and unpausing certain functions, and ensuring safety checks to prevent arithmetic overflows and underflows.
- The IoTeX Network is a smart contract that allows for the pause/unpause contracts and ownership transfers.

Audit scope

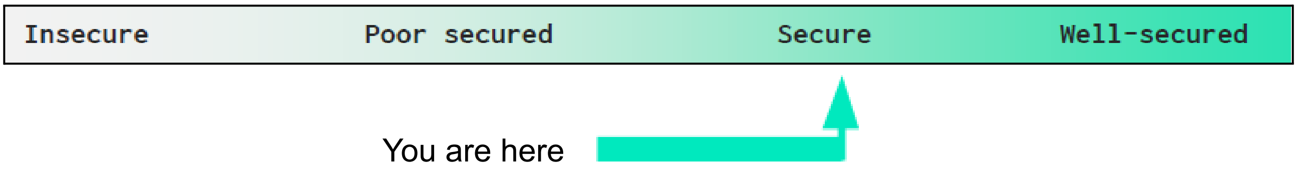
Name	Code Review and Security Analysis Report for IoTeX Network Smart Contract
Platform	**Ethereum**
Language	**Solidity**
File	IoTeXNetwork.sol
Smart Contract Code	0x6fb3e0a217407efff7ca062d46c26e5d60a14d69
Audit Date	February 24th, 2024

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: • Name: IoTeX Network • Symbol: IOTX • Decimals: 18	**YES, This is valid.**
Ownership Control: • Pause / Unpause contract. • The current owner can transfer the ownership.	**YES, This is valid.** **We suggest renouncing ownership once the ownership functions are not needed. This is to make the smart contract 100% decentralized.**

Audit Summary

According to the standard audit assessment, the Customer`s solidity-based smart contracts are **“Secured”.** Also, these contracts contain owner control, which does not make them fully decentralized.



We used various tools like Slither, Solhint, and Remix IDE. At the same time, this finding is based on a 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. A general overview is presented in the AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium, 0 low, and 3 very low level issues.

Investor Advice: A 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	The solidity version is not specified	Passed
	Solidity version is too old	Moderated
	Integer overflow/underflow	Passed
	Function input parameters lack check	Passed
	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	Moderated
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**

Business Risk Analysis

Category	Result
🟢 Buy Tax	0%
🟢 Sell Tax	0%
🟢 Cannot Buy	No
🟢 Cannot Sell	No
🟢 Max Tax	0%
🟢 Modify Tax	No
🟢 Fee Check	Not Detected
🟢 Is Honeypot	Not Detected
🟢 Trading Cooldown	Not Detected
🟢 Can Pause Trade?	Not Detected
🟢 Pause Transfer?	Yes
🟢 Max Tax?	No
🟢 Is it Anti-whale?	Not Detected
🟢 Is Anti-bot?	Not Detected
🟢 Is it a Blacklist?	No
🟢 Blacklist Check	No
🟢 Can Mint?	No
🟢 Is it a Proxy?	No
🟢 Can Take Ownership?	Yes
🟢 Hidden Owner?	Not Detected
🟢 Self Destruction?	Not Detected
🟢 Auditor Confidence	High

Overall Audit Result: **PASSED**

Code Quality

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

The libraries in the IoTeX Network 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 IoTeX Network.

The EtherAuthority team has no 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 in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given an IoTeX Network smart contract code in the form of an Etherscan web link.

As mentioned above, code parts are well commented on. and 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.

Use of Dependencies

As per our observation, the libraries used in this smart contract infrastructure 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	Function with the same name as the contract	Refer Audit Findings
2	validDestination	modifier	Passed	No Issue
3	IoTeXNetwork	write	No visibility specified	Refer Audit Findings
4	transfer	write	No visibility specified	Refer Audit Findings
5	transferFrom	write	No visibility specified	Refer Audit Findings
6	approve	write	Passed	No Issue
7	increaseApproval	write	Passed	No Issue
8	decreaseApproval	write	Passed	No Issue
9	transferFrom	write	Passed	No Issue
10	approve	write	Passed	No Issue
11	allowance	read	Passed	No Issue
12	increaseApproval	write	Passed	No Issue
13	decreaseApproval	write	Passed	No Issue
14	totalSupply	read	Passed	No Issue
15	transfer	write	Passed	No Issue
16	balanceOf	read	Passed	No Issue
17	allowance	read	Passed	No Issue
18	transferFrom	write	Passed	No Issue
19	approve	write	Passed	No Issue
20	totalSupply	write	Passed	No Issue
21	balanceOf	write	Passed	No Issue
22	transfer	write	Passed	No Issue
23	whenNotPaused	modifier	Passed	No Issue
24	whenPaused	modifier	Passed	No Issue
25	pause	write	access only Owner	No Issue
26	unpause	write	access only Owner	No Issue
27	Ownable	write	Passed	No Issue
28	onlyOwner	modifier	Passed	No Issue
29	transferOwnership	write	access only Owner	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 a 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 a 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

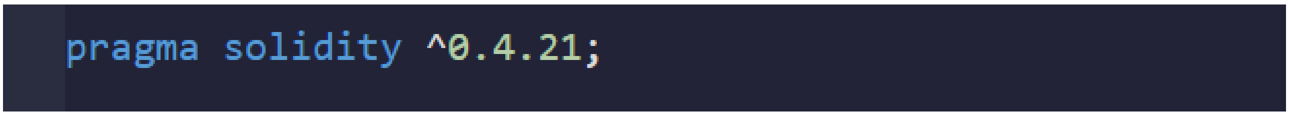
No Medium-severity vulnerabilities were found.

Low

No Low Severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Use the latest solidity version:



```
pragma solidity ^0.4.21;
```

Using the latest solidity will prevent any compiler-level bugs.

Resolution: We suggest using the latest solidity compiler version.

(2) Function with the same name as the contract:

Defining constructors as functions with the same name as the contract is deprecated.

Resolution: Use "constructor(...) { ... }" instead.

(3) No visibility specified:

No visibility was specified. Defaulting to "public".

- transferFrom
- transfer

- IoTeXNetwork

Resolution: Use public keywords as default.

Centralization

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

Pausable.sol

- pause: The owner can trigger a stopped state.
- unpause: The owner can return to a normal state.

Ownable.sol

- transferOwnership: Current owner can transfer ownership of the contract to a new account.

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 Etherscan web links. And we have used all possible tests based on given objects as files. We observed 3 Informational issues in the smart contracts. but those are not critical. So, **it's good to go for the 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 the 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 the 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 white box penetration testing. We look at the project's website 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, and 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).

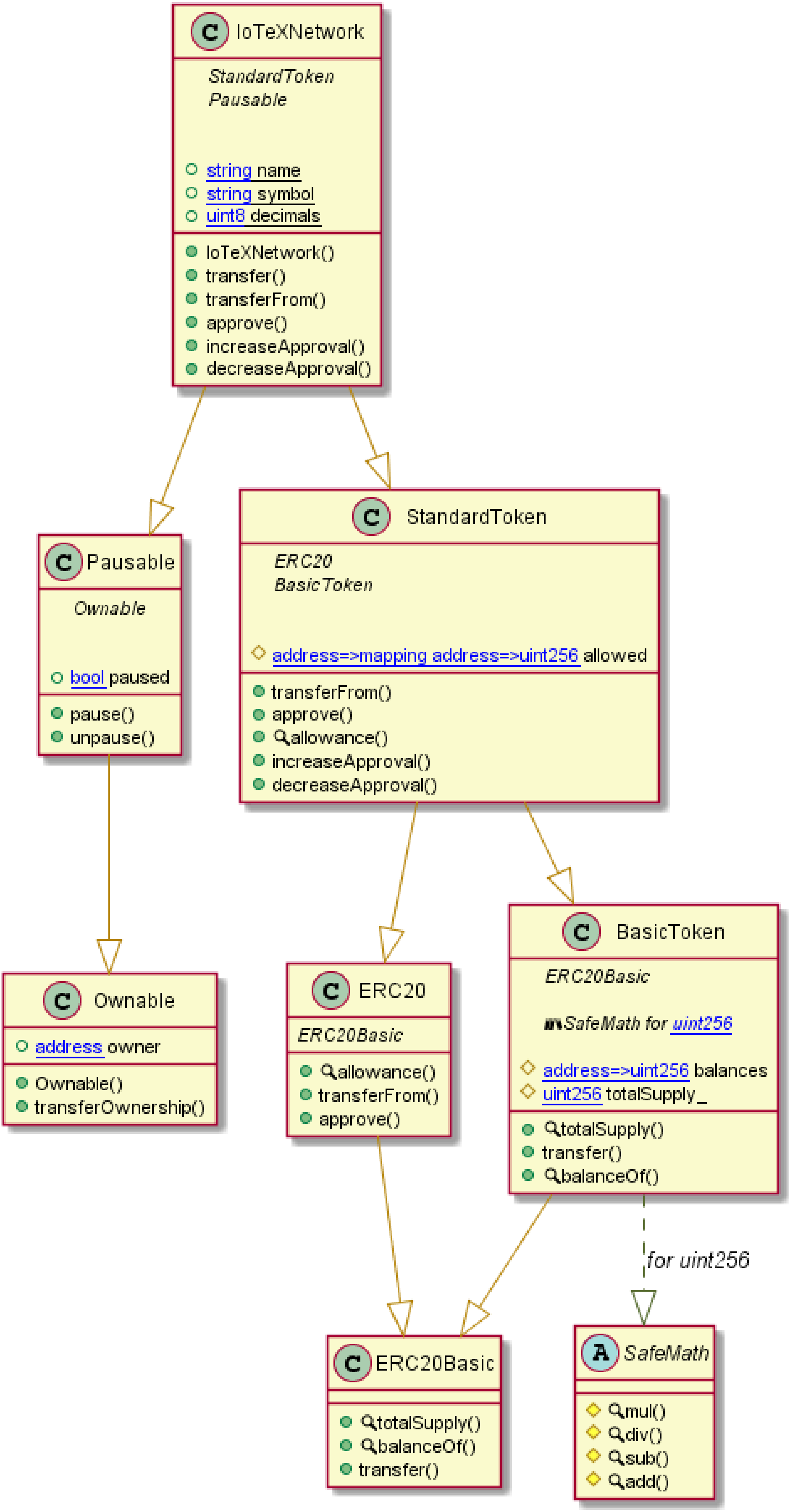
Due to the fact that the total number of test cases is unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While 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 the explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - IoTeX Network

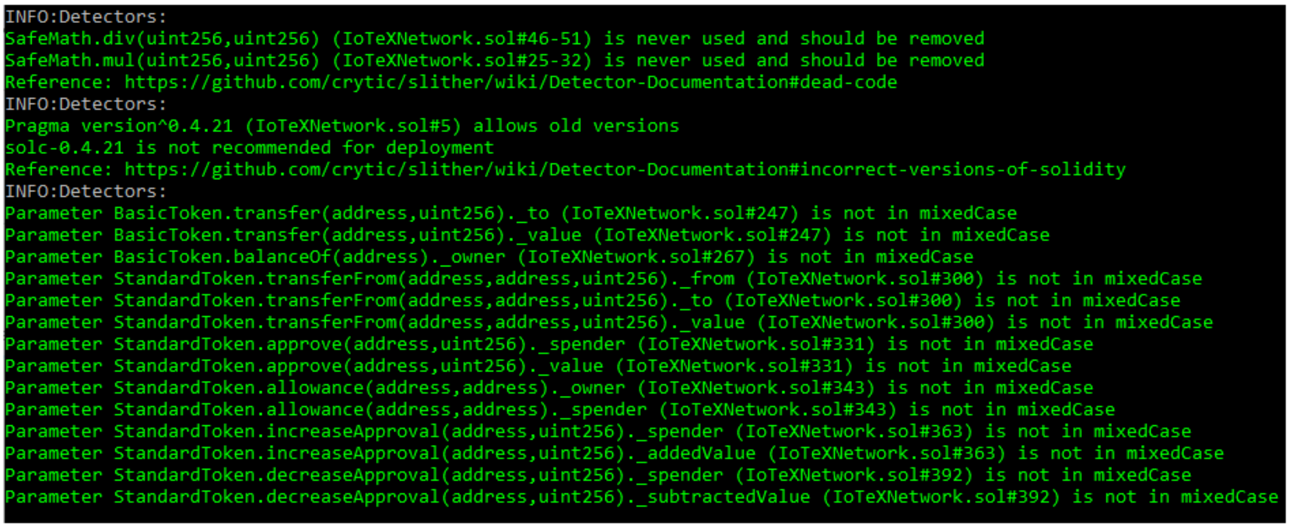


Slither Results Log

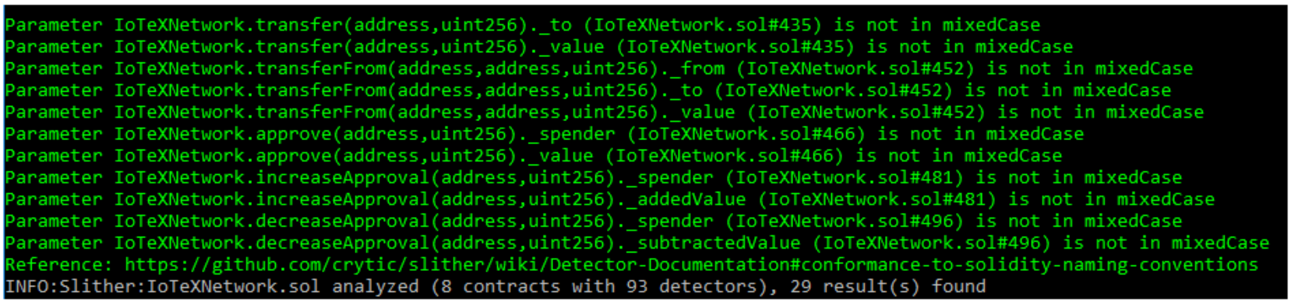
Slither is a Solidity static analysis framework that uses vulnerability detectors, displays contract details, and provides an API for writing custom analyses. It helps developers identify vulnerabilities, improve code comprehension, and prototype custom analyses quickly. The analysis includes a report with warnings and errors, allowing developers to quickly prototype and fix issues.

We did the analysis of the project altogether. Below are the results.

Slither Log >> IoTeXNetwork.sol



```
INFO:Detectors:
SafeMath.div(uint256,uint256) (IoTeXNetwork.sol#46-51) is never used and should be removed
SafeMath.mul(uint256,uint256) (IoTeXNetwork.sol#25-32) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.4.21 (IoTeXNetwork.sol#5) allows old versions
solc-0.4.21 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter BasicToken.transfer(address,uint256)._to (IoTeXNetwork.sol#247) is not in mixedCase
Parameter BasicToken.transfer(address,uint256)._value (IoTeXNetwork.sol#247) is not in mixedCase
Parameter BasicToken.balanceOf(address)._owner (IoTeXNetwork.sol#267) is not in mixedCase
Parameter StandardToken.transferFrom(address,address,uint256)._from (IoTeXNetwork.sol#300) is not in mixedCase
Parameter StandardToken.transferFrom(address,address,uint256)._to (IoTeXNetwork.sol#300) is not in mixedCase
Parameter StandardToken.transferFrom(address,address,uint256)._value (IoTeXNetwork.sol#300) is not in mixedCase
Parameter StandardToken.approve(address,uint256)._spender (IoTeXNetwork.sol#331) is not in mixedCase
Parameter StandardToken.approve(address,uint256)._value (IoTeXNetwork.sol#331) is not in mixedCase
Parameter StandardToken.allowance(address,address)._owner (IoTeXNetwork.sol#343) is not in mixedCase
Parameter StandardToken.allowance(address,address)._spender (IoTeXNetwork.sol#343) is not in mixedCase
Parameter StandardToken.increaseApproval(address,uint256)._spender (IoTeXNetwork.sol#363) is not in mixedCase
Parameter StandardToken.increaseApproval(address,uint256)._addedValue (IoTeXNetwork.sol#363) is not in mixedCase
Parameter StandardToken.decreaseApproval(address,uint256)._spender (IoTeXNetwork.sol#392) is not in mixedCase
Parameter StandardToken.decreaseApproval(address,uint256)._subtractedValue (IoTeXNetwork.sol#392) is not in mixedCase
```

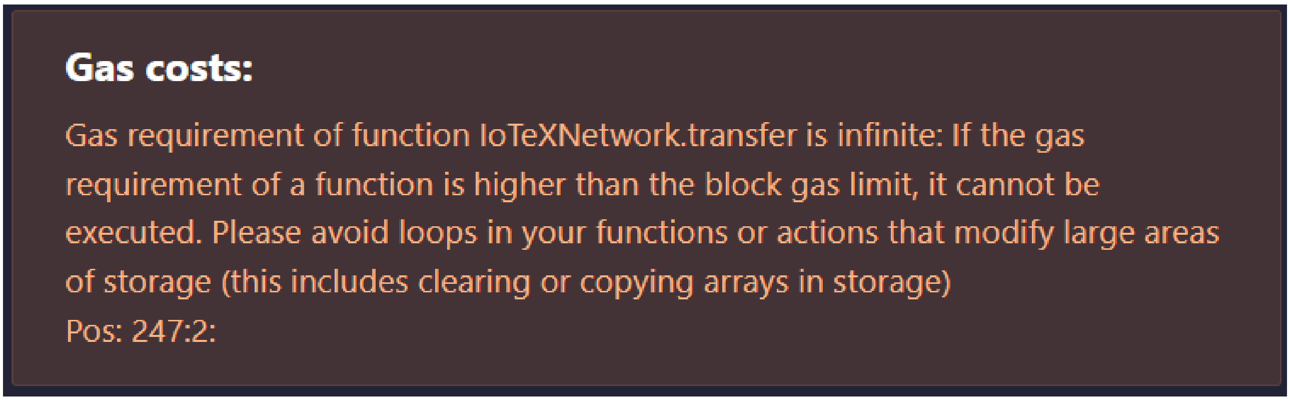


```
Parameter IoTeXNetwork.transfer(address,uint256)._to (IoTeXNetwork.sol#435) is not in mixedCase
Parameter IoTeXNetwork.transfer(address,uint256)._value (IoTeXNetwork.sol#435) is not in mixedCase
Parameter IoTeXNetwork.transferFrom(address,address,uint256)._from (IoTeXNetwork.sol#452) is not in mixedCase
Parameter IoTeXNetwork.transferFrom(address,address,uint256)._to (IoTeXNetwork.sol#452) is not in mixedCase
Parameter IoTeXNetwork.transferFrom(address,address,uint256)._value (IoTeXNetwork.sol#452) is not in mixedCase
Parameter IoTeXNetwork.approve(address,uint256)._spender (IoTeXNetwork.sol#466) is not in mixedCase
Parameter IoTeXNetwork.approve(address,uint256)._value (IoTeXNetwork.sol#466) is not in mixedCase
Parameter IoTeXNetwork.increaseApproval(address,uint256)._spender (IoTeXNetwork.sol#481) is not in mixedCase
Parameter IoTeXNetwork.increaseApproval(address,uint256)._addedValue (IoTeXNetwork.sol#481) is not in mixedCase
Parameter IoTeXNetwork.decreaseApproval(address,uint256)._spender (IoTeXNetwork.sol#496) is not in mixedCase
Parameter IoTeXNetwork.decreaseApproval(address,uint256)._subtractedValue (IoTeXNetwork.sol#496) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Slither:IoTeXNetwork.sol analyzed (8 contracts with 93 detectors), 29 result(s) found
```

Solidity Static Analysis

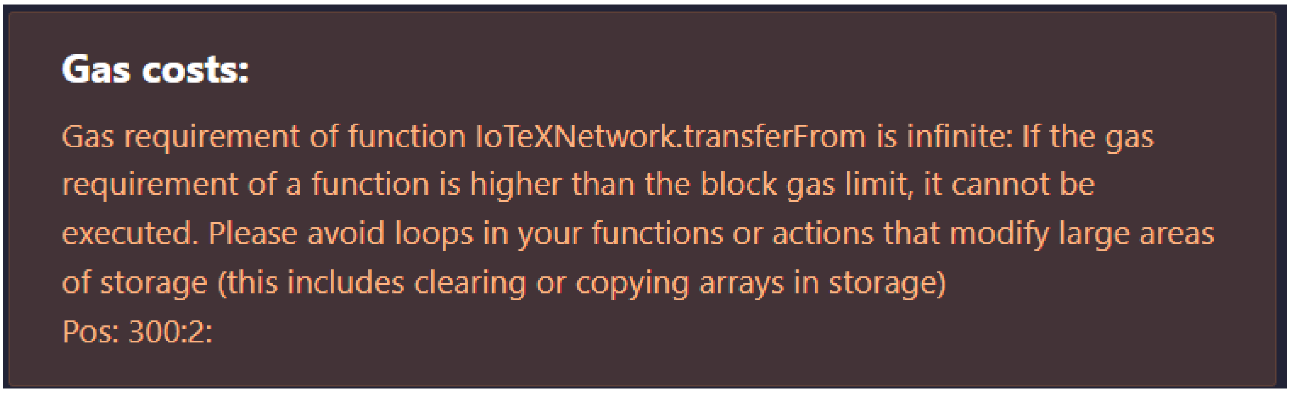
Static code analysis is used to identify many common coding problems before a program is released. It involves examining the code manually or using tools to automate the process. Static code analysis tools can automatically scan the code without executing it.

IoTeXNetwork.sol



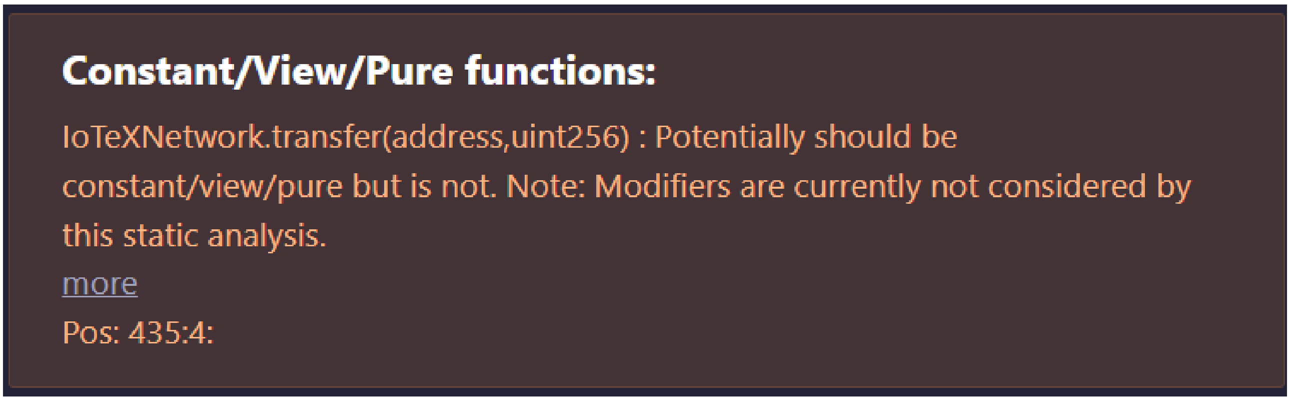
Gas costs:

Gas requirement of function IoTeXNetwork.transfer 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: 247:2:



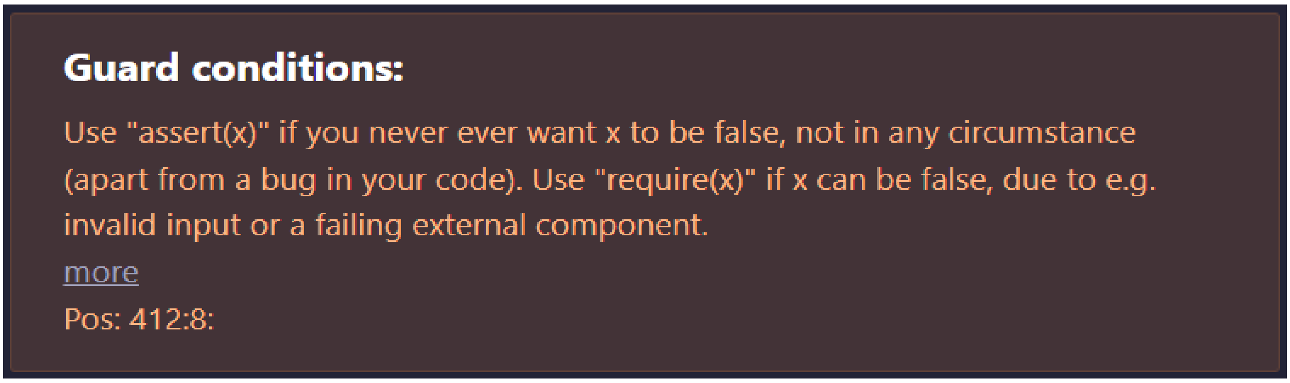
Gas costs:

Gas requirement of function IoTeXNetwork.transferFrom 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: 300:2:



Constant/View/Pure functions:

IoTeXNetwork.transfer(address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 435:4:



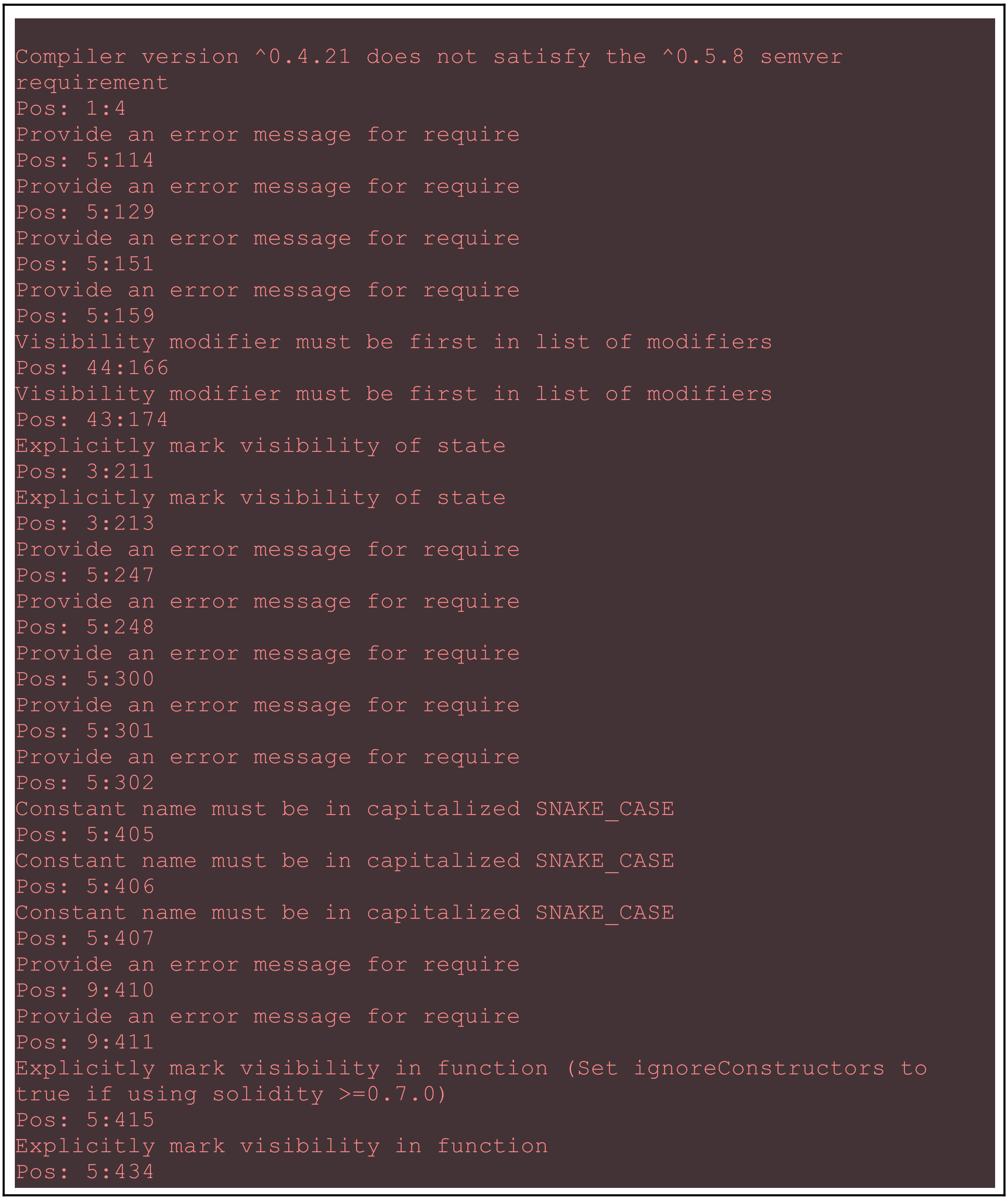
Guard conditions:

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: 412:8:

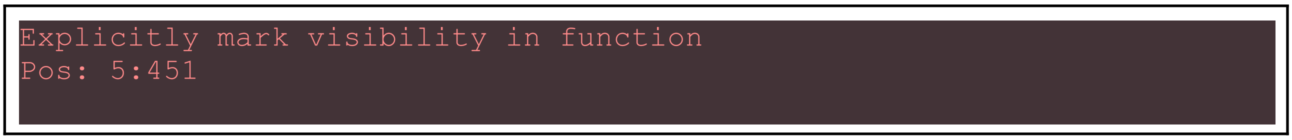
Solhint Linter

Linters are the utility tools that analyze the given source code and report programming errors, bugs, and stylistic errors. For the Solidity language, there are some linter tools available that a developer can use to improve the quality of their Solidity contracts.

IoTeXNetwork.sol



```
Compiler version ^0.4.21 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:4
Provide an error message for require
Pos: 5:114
Provide an error message for require
Pos: 5:129
Provide an error message for require
Pos: 5:151
Provide an error message for require
Pos: 5:159
Visibility modifier must be first in list of modifiers
Pos: 44:166
Visibility modifier must be first in list of modifiers
Pos: 43:174
Explicitly mark visibility of state
Pos: 3:211
Explicitly mark visibility of state
Pos: 3:213
Provide an error message for require
Pos: 5:247
Provide an error message for require
Pos: 5:248
Provide an error message for require
Pos: 5:300
Provide an error message for require
Pos: 5:301
Provide an error message for require
Pos: 5:302
Constant name must be in capitalized SNAKE_CASE
Pos: 5:405
Constant name must be in capitalized SNAKE_CASE
Pos: 5:406
Constant name must be in capitalized SNAKE_CASE
Pos: 5:407
Provide an error message for require
Pos: 9:410
Provide an error message for require
Pos: 9:411
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:415
Explicitly mark visibility in function
Pos: 5:434
```



```
Explicitly mark visibility in function
Pos: 5:451
```

Software analysis result:

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

EtherAuthority

Email: audit@EtherAuthority.io