Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	Matic Token
Website:	polygon.technology
Platform:	Ethereum
Language:	Solidity
Date:	April 15th, 2024

Table of contents

Introduction 4

Project Background 4

Audit Scope 5

Claimed Smart Contract Features 6

Audit Summary 7

Technical Quick Stats 8

Business Risk Analysis 9

Code Quality 10

Documentation 10

Use of Dependencies 10

AS-IS overview 11

Severity Definitions 12

Audit Findings 13

Conclusion 18

Our Methodology 19

Disclaimers 21

Appendix

- Code Flow Diagram 22
- Slither Results Log 23
- Solidity static analysis 24
- Solhint Linter 26

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

As part of EtherAuthority's community smart contracts audit initiatives, the Matic token smart contract from polygon.technology 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 April 15th, 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

- These Solidity codes are for implementing an ERC20 token along with functionalities like pausing/unpausing transfers. Let's break down the provided code:
    - **ERC20 Interface:** The `IERC20` interface defines the standard functions and events for an ERC20 token.
    - **SafeMath Library:** This library contains functions for safe arithmetic operations to prevent overflow and underflow vulnerabilities.
    - **ERC20 Contract:** The main ERC20 contract implements the token functionality according to the ERC20 standard. It includes functions for transferring tokens, approving spending, and allowance management.
    - **Roles Library and PauserRole Contract:** These define a role-based access control system. The `PauserRole` contract allows certain accounts to pause and unpause token transfers.
    - **Pausable Contract:** This contract adds pausing functionality to the token. When paused, transfers are halted.
    - **ERC20Pausable Contract:** This contract combines ERC20 functionality with pausing capabilities.
    - **ERC20Detailed Contract:** This contract provides additional information about the token, such as its name, symbol, and decimals.

    - **MaticToken Contract:** This is the main token contract that inherits from `ERC20Pausable` and `ERC20Detailed`. It initializes the token with an initial supply and mints tokens to the contract deployer.
- This code creates a token with ERC20 functionality along with the ability to pause/unpause token transfers.

Audit scope

Name	**Code Review and Security Analysis Report for Matic Token Smart Contract**
Platform	**Ethereum**
File	MaticToken.sol
Smart Contract Code	0x7d1afa7b718fb893db30a3abc0cfc608aacfebb0
Audit Date	April 15th, 2024

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: • Name: Matic Token • Symbol: MATIC • Decimals: 18 • Total Supply: 10 billion	**YES, This is valid.**
Controller of the owner control: • Pause / Unpause state. • Add pauser address.	**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 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. The 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 2 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	The solidity version is not specified	Passed
	The 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**

Email: audit@EtherAuthority.io

Business Risk Analysis

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

Overall Audit Result: **PASSED**

Email: audit@EtherAuthority.io

Code Quality

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

The libraries in Matic 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 Matic Token.

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 not well commented on in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given a Matic Token smart contract code in the form of an Etherscan web link.

As mentioned above, code parts are not well commented on. 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.

Use of Dependencies

As per our observation, the libraries 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	name	read	Passed	No Issue
3	symbol	read	Passed	No Issue
4	decimals	read	Passed	No Issue
5	transfer	write	Passed	No Issue
6	transferFrom	write	Passed	No Issue
7	approve	write	Passed	No Issue
8	increaseAllowance	write	Passed	No Issue
9	decreaseAllowance	write	Passed	No Issue
10	paused	read	Passed	No Issue
11	whenNotPaused	modifier	Passed	No Issue
12	whenPaused	modifier	Passed	No Issue
13	pause	write	access only Pauser	No Issue
14	unpause	write	access only Pauser	No Issue
15	onlyPauser	modifier	Passed	No Issue
16	isPauser	read	Passed	No Issue
17	addPauser	write	access only Pauser	No Issue
18	renouncePauser	write	Passed	No Issue
19	_addPauser	internal	Passed	No Issue
20	_removePauser	internal	Passed	No Issue
21	totalSupply	read	Passed	No Issue
22	balanceOf	read	Passed	No Issue
23	allowance	read	Passed	No Issue
24	transfer	write	Passed	No Issue
25	approve	write	Passed	No Issue
26	transferFrom	write	Passed	No Issue
27	increaseAllowance	write	Passed	No Issue
28	decreaseAllowance	write	Passed	No Issue
29	_transfer	internal	Passed	No Issue
30	_mint	internal	Passed	No Issue
31	_burn	internal	Passed	No Issue
32	_burnFrom	internal	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

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Use the latest solidity version:

```
pragma solidity 0.5.2;
```

Use the latest solidity version while contract deployment to prevent any compiler version-level bugs.

Resolution: Please use versions greater than 0.8.7.

(2) Explicit Visibility for State Variables Warning:

```
library Roles {
    struct Role {
        mapping (address => bool) bearer;
    }
```

The warning is related to the visibility of state variables in your Solidity code.

Resolution: We recommend updating the code to explicitly mark the visibility of state variables using the internal or public keyword, depending on the intended visibility.

Centralization

This smart contract has some functions that 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:

Pausable.sol

- pause: The stopped state can be triggered by the owner to pause.
- unpause: The normal state can be returned by the owner to unpause.

PauserRole.sol

- addPauser: Pauser address can be added by the owner.

To make the smart contract 100% decentralized, we suggest renouncing ownership of 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 2 informational issues in the smart contracts. And those issues 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.

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

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

Email: audit@EtherAuthority.io

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).

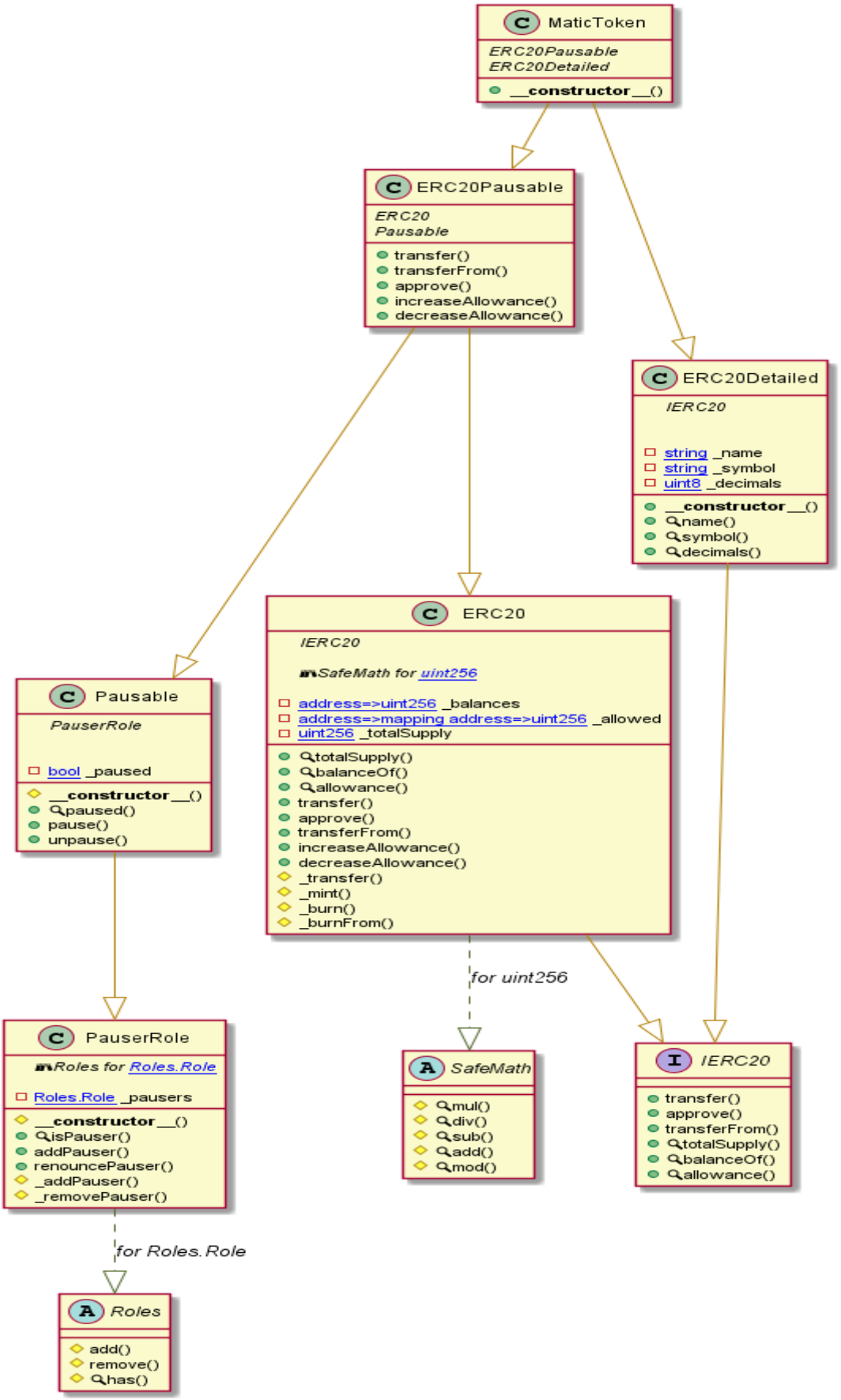
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we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



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 >> MaticToken.sol

```
ERC20Detailed.constructor(string,string,uint8).name (MaticToken.sol#462) shadows:
        - ERC20Detailed.name() (MaticToken.sol#471-473) (function)
ERC20Detailed.constructor(string,string,uint8).symbol (MaticToken.sol#462) shadows:
        - ERC20Detailed.symbol() (MaticToken.sol#478-480) (function)
ERC20Detailed.constructor(string,string,uint8).decimals (MaticToken.sol#462) shadows:
        - ERC20Detailed.decimals() (MaticToken.sol#485-487) (function)
MaticToken.constructor(string,string,uint8,uint256).name (MaticToken.sol#493) shadows:
        - ERC20Detailed.name() (MaticToken.sol#471-473) (function)
MaticToken.constructor(string,string,uint8,uint256).symbol (MaticToken.sol#493) shadows:
        - ERC20Detailed.symbol() (MaticToken.sol#478-480) (function)
MaticToken.constructor(string,string,uint8,uint256).decimals (MaticToken.sol#493) shadows:
        - ERC20Detailed.decimals() (MaticToken.sol#485-487) (function)
MaticToken.constructor(string,string,uint8,uint256).totalSupply (MaticToken.sol#493) shadows:
        - ERC20.totalSupply() (MaticToken.sol#123-125) (function)
        - IERC20.totalSupply() (MaticToken.sol#20) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing

ERC20._burn(address,uint256) (MaticToken.sol#259-265) is never used and should be removed
ERC20._burnFrom(address,uint256) (MaticToken.sol#275-279) is never used and should be removed
SafeMath.div(uint256,uint256) (MaticToken.sol#58-65) is never used and should be removed
SafeMath.mod(uint256,uint256) (MaticToken.sol#91-94) is never used and should be removed
SafeMath.mul(uint256,uint256) (MaticToken.sol#41-53) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version0.5.2 (MaticToken.sol#5) allows old versions
solc-0.5.2 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
MaticToken.sol analyzed (9 contracts with 84 detectors), 14 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.

MaticToken.sol

Gas costs:

Gas requirement of function MaticToken.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: 151:4:

Gas costs:

Gas requirement of function MaticToken.isPauser 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: 342:4:

Gas costs:

Gas requirement of function MaticToken.pause 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: 407:4:

Gas costs:

Gas requirement of function MaticToken.unpause 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: 415:4:

Constant/View/Pure functions:

ERC20Pausable.decreaseAllowance(address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 444:4:

Similar variable names:

Pausable.() : Variables have very similar names "_paused" and "_pausers". Note: Modifiers are currently not considered by this static analysis.

Pos: 378:8:

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: 392:8:

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: 400:8:

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: 61:20:

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.

MaticToken.sol

```
Compiler version 0.5.2 does not satisfy the ^0.5.8 semver requirement
Pos: 1:4
Provide an error message for require
Pos: 9:49
Provide an error message for require
Pos: 9:59
Provide an error message for require
Pos: 9:70
Provide an error message for require
Pos: 9:81
Provide an error message for require
Pos: 9:91
Provide an error message for require
Pos: 9:165
Provide an error message for require
Pos: 9:198
Provide an error message for require
Pos: 9:216
Provide an error message for require
Pos: 9:230
Provide an error message for require
Pos: 9:245
Provide an error message for require
Pos: 9:259
Provide an error message for require
Pos: 9:296
Provide an error message for require
Pos: 9:297
Provide an error message for require
Pos: 9:306
Provide an error message for require
Pos: 9:307
Provide an error message for require
Pos: 9:391
Provide an error message for require
Pos: 9:399
```

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