



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

Audit

**Security Assessment
15. October, 2021**

For



Trillium

Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	10
Risk Level	10
Capabilities	11
Scope of Work	13
Inheritance Graph	13
Verify Claims	14
CallGraph	19
Source Units in Scope	20
OnlyOwner functions	21
Critical issues	22
High issues	22
Medium issues	22
Low issues	22
Informational issues	22
Audit Comments	23
SWC Attacks	24

Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	15. October 2021	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Binance Smart Chain (BEP20)

Website

<https://trilliumtoken.com>

Telegram

TBA

Twitter

TBA

Description

Trillium is an advanced multilayer payment technology Trillium (TT) is a decentralized finance (DeFi) protocol built to enable cross-border commercial transactions. The system enables traders and payees to send money using a decentralized network to their clients or investors in other territories.

Project Engagement

During the 11th of October 2021, **Trillium Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Link

v1.0

[https://bscscan.com/address/
0x2f8a4c0ca0b45a2fb240cba7010c34ba60ad9b6d#code](https://bscscan.com/address/0x2f8a4c0ca0b45a2fb240cba7010c34ba60ad9b6d#code)

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as they were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

- OpenZeppelin
 - Address
 - Ownable
 - SafeMath
 - Context
 - IERC20
- Uniswap
 - UniswapV2Factory
 - UniswapV2Pair
 - UniswapV2Router01
 - UniswapV2Router02

Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

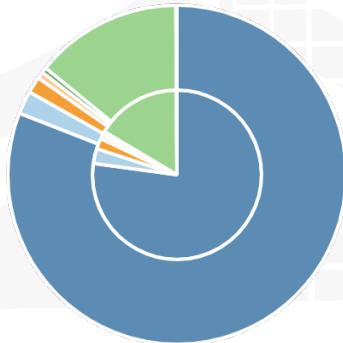
v1.0

File Name	SHA-1 Hash
contracts/trilium.sol	a6f29e1de5132eb64601d7a18abf99da45ff48ac

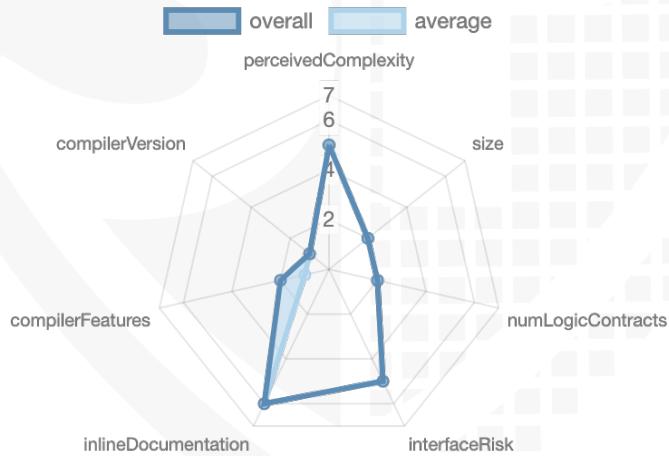
Metrics

Source Lines v1.0

source comment single block mixed
empty todo blockEmpty



Risk Level v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	1	2	5	2

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

Version	Public	Payable
1.0	101	6

Version	External	Internal	Private	Pure	View
1.0	72	99	24	25	46

State Variables

Version	Total	Public
1.0	29	11

Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	^0.8.4		yes	yes (2 asm blocks)	

Version	Transf ers ETH	Low- Level Calls	Delega teCall	Uses Hash Functi ons	ECRec over	New/ Create/ Create 2
1.0	yes		yes			

Scope of Work

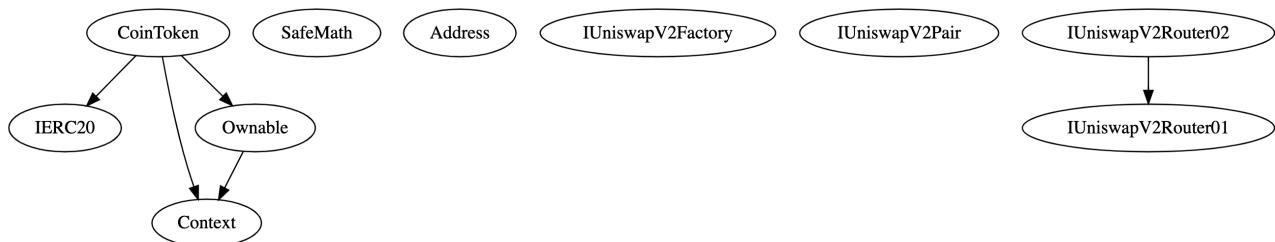
The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Correct implementation of Token standard
2. Deployer cannot mint any new tokens
3. Deployer cannot burn or lock user funds
4. Deployer cannot pause the contract
5. Overall checkup (Smart Contract Security)

Inheritance Graph

v1.0



Verify Claims

Correct implementation of Token standard

Tested	Verified
✓	✓

Function	Description	Exist	Tested	Verified
TotalSupply	provides information about the total token supply	✓	✓	✓
BalanceOf	provides account balance of the owner's account	✓	✓	✓
Transfer	executes transfers of a specified number of tokens to a specified address	✓	✓	✓
TransferFrom	executes transfers of a specified number of tokens from a specified address	✓	✓	✓
Approve	allow a spender to withdraw a set number of tokens from a specified account	✓	✓	✓
Allowance	returns a set number of tokens from a spender to the owner	✓	✓	✓

Optional implementations

Function	Description	Exist	Tested	Verified
renounceOwnership	Owner renounce ownership for more trust	✓	✓	✗

Deployer cannot mint any new tokens

Name	Exist	Tested	Verified	File
Deployer cannot mint	✓	✓	✓	Main
Comment	Line: -			

Max / Total Supply: 10.000.000.000

1. approve	→
2. decreaseAllowance	→
3. deliver	→
4. excludeFromFee	→
5. excludeFromReward	→
6. includeInFee	→
7. includeInReward	→
8. increaseAllowance	→
9. lock	→
10. renounceOwnership	→
11. setDevFeePercent	→
12. setDevWalletAddress	→
13. setLiquidityFeePercent	→
14. setMaxTxPercent	→
15. setNumTokensSellToAddToLiquidity	→
16. setRouterAddress	→
17. setSwapAndLiquifyEnabled	→
18. setTaxFeePercent	→
19. transfer	→
20. transferFrom	→
21. transferOwnership	→
22. unlock	→

Deployer cannot burn or lock user funds

Name	Exist	Tested	Verified
Deployer cannot lock	✓	✓	✗
Deployer cannot burn	✓	✓	✓

Comments:

v1.0

- Deployer can lock use funds
 - When maxTxAmount is set to 0, because amount must be higher than 0

```
require(from↑ != address(0), "ERC20: transfer from the zero address");
require(to↑ != address(0), "ERC20: transfer to the zero address");
require(amount↑ > 0, "Transfer amount must be greater than zero");
if(from↑ != owner() && to↑ != owner())
    require(amount↑ <= maxTxAmount, "Transfer amount exceeds the maxTxAmount.");
```

1. approve	→
2. decreaseAllowance	→
3. deliver	→
4. excludeFromFee	→
5. excludeFromReward	→
6. includeInFee	→
7. includeInReward	→
8. increaseAllowance	→
9. lock	→
10. renounceOwnership	→
11. setDevFeePercent	→
12. setDevWalletAddress	→
13. setLiquidityFeePercent	→
14. setMaxTxPercent	→
15. setNumTokensSellToAddToLiquidity	→
16. setRouterAddress	→
17. setSwapAndLiquifyEnabled	→
18. setTaxFeePercent	→
19. transfer	→
20. transferFrom	→
21. transferOwnership	→
22. unlock	→

Deployer cannot pause the contract

Name	Exist	Tested	Verified
Deployer cannot pause	✓	✓	✓

1. approve	→
2. decreaseAllowance	→
3. deliver	→
4. excludeFromFee	→
5. excludeFromReward	→
6. includeInFee	→
7. includeInReward	→
8. increaseAllowance	→
9. lock	→
10. renounceOwnership	→
11. setDevFeePercent	→
12. setDevWalletAddress	→
13. setLiquidityFeePercent	→
14. setMaxTxPercent	→
15. setNumTokensSellToAddToLiquidity	→
16. setRouterAddress	→
17. setSwapAndLiquifyEnabled	→
18. setTaxFeePercent	→
19. transfer	→
20. transferFrom	→
21. transferOwnership	→
22. unlock	→

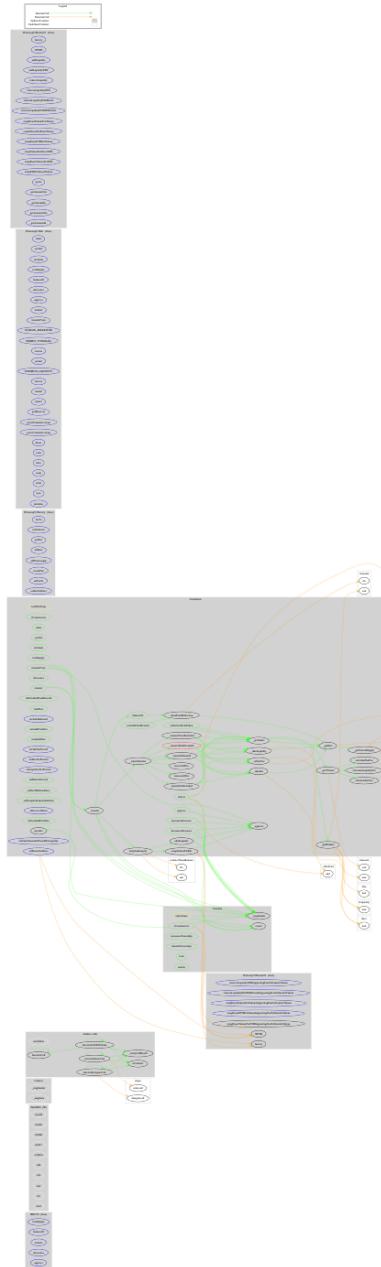
Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	🚩
Unverified / Not checked	✗
Not available	-

CallGraph



Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/trilium.sol	5	5	922	703	567	21	571	
	Totals	5	5	922	703	567	21	571	

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
nSLOC	normalized source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

OnlyOwner functions

- renounceOwnership
- transferOwnership
- lock
- excludeFromReward
- includeInReward
- setTaxFeePercent
- setDevFeePercent
- setLiquidityFeePercent
- setMaxTxPercent
- setDevWalletAddress
- setSwapAndLiquifyEnabled
- setRouterAddress
- setNumTokensSellToAddToLiquidity

Audit Results

AUDIT PASSED

Critical issues

- no critical issues found -

High issues

- no high issues found -

Medium issues

- no medium issues found -

Low issues

Issue	File	Type	Line	Description
#1	Main	Contract doesn't import npm packages from source (like OpenZeppelin etc.)		- We recommend to import all packages from npm directly without flatten the contract. Functions could be modified or can be susceptible to vulnerabilities
#2	Main	A floating pragma is set	11	The current pragma Solidity directive is „^0.8.4“.
#3	Main	Missing Zero Address Validation (missing-zero-check)	484, 664	Check that the address is not zero
#4	Main	State variable visibility is not set	466	It is best practice to set the visibility of state variables explicitly

Informational issues

- no informational issues found -

Audit Comments

15. October 2021:

- There is still an owner (Owner still has not renounced ownership)
- Developer can
 - set maxTxAmount to zero to lock transfer function (look at deployer cannot burn and lock user funds section)
- Deployer can
 - set route address variable while deployment
 - set total supply variable while deployment
 - Set fee to 100 percent

SWC Attacks

ID	Title	Relationships	Status
SW C-13_6	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-13_5	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-13_4	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-13_3	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-13_2	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-13_1	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SW C-13_0	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-12_9	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-12_8	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

<u>SW C-12 7</u>	Arbitrary Jump with Function Type Variable	<u>CWE-695: Use of Low-Level Functionality</u>	PASSED
<u>SW C-12 5</u>	Incorrect Inheritance Order	<u>CWE-696: Incorrect Behavior Order</u>	PASSED
<u>SW C-12 4</u>	Write to Arbitrary Storage Location	<u>CWE-123: Write-what-where Condition</u>	PASSED
<u>SW C-12 3</u>	Requirement Violation	<u>CWE-573: Improper Following of Specification by Caller</u>	PASSED
<u>SW C-12 2</u>	Lack of Proper Signature Verification	<u>CWE-345: Insufficient Verification of Data Authenticity</u>	PASSED
<u>SW C-12 1</u>	Missing Protection against Signature Replay Attacks	<u>CWE-347: Improper Verification of Cryptographic Signature</u>	PASSED
<u>SW C-12 0</u>	Weak Sources of Randomness from Chain Attributes	<u>CWE-330: Use of Insufficiently Random Values</u>	PASSED
<u>SW C-11 9</u>	Shadowing State Variables	<u>CWE-710: Improper Adherence to Coding Standards</u>	PASSED
<u>SW C-11 8</u>	Incorrect Constructor Name	<u>CWE-665: Improper Initialization</u>	PASSED
<u>SW C-11 7</u>	Signature Malleability	<u>CWE-347: Improper Verification of Cryptographic Signature</u>	PASSED

SW C-11 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SW C-11 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SW C-11 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SW C-11 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SW C-11 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SW C-10 9	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-10 8	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	NOT PASSED
SW C-10 7	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-10 6	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

Solid
Proofed

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

<u>SW C-10 5</u>	Unprotected Ether Withdrawal	<u>CWE-284: Improper Access Control</u>	PASSED
<u>SW C-10 4</u>	Unchecked Call Return Value	<u>CWE-252: Unchecked Return Value</u>	PASSED
<u>SW C-10 3</u>	Floating Pragma	<u>CWE-664: Improper Control of a Resource Through its Lifetime</u>	NOT PASSED
<u>SW C-10 2</u>	Outdated Compiler Version	<u>CWE-937: Using Components with Known Vulnerabilities</u>	PASSED
<u>SW C-10 1</u>	Integer Overflow and Underflow	<u>CWE-682: Incorrect Calculation</u>	PASSED
<u>SW C-10 0</u>	Function Default Visibility	<u>CWE-710: Improper Adherence to Coding Standards</u>	PASSED