SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

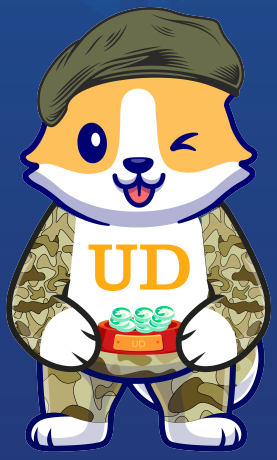
MADE IN GERMANY

Audit

Security Assessment

17. January, 2022

For



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	17. January 2022	• Layout project • Automated- /Manual-Security Testing • Summary

Network
Binance Smart Chain (BEP20)

Website
https://www.unidogearmy.io/

Telegram
https://t.me/unidogearmy

Twitter
https://twitter.com/UniDogebsc?t=f84rn3XPdfRddVr3CoEqWQ&s=08

Medium
http://unidogearmy.medium.com/

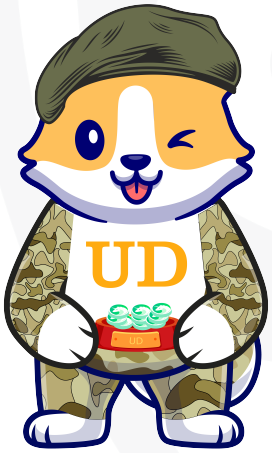
Description

WE LOVE DOGE AND UNICRYPT. UNIDOGE ARMY is the first decentralized autonomous
organization for social media industries on binance smart chain (BSC) and a community-centered
initiative that strives to promote the adoption of Unicrypt & Doge in general.

Project Engagement

During the 13th of January 2022, **UniDogeArmy 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/0xa524a6f203938dcf1eea2ccba813492c85a8ea85#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 aspossible.
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 there 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.

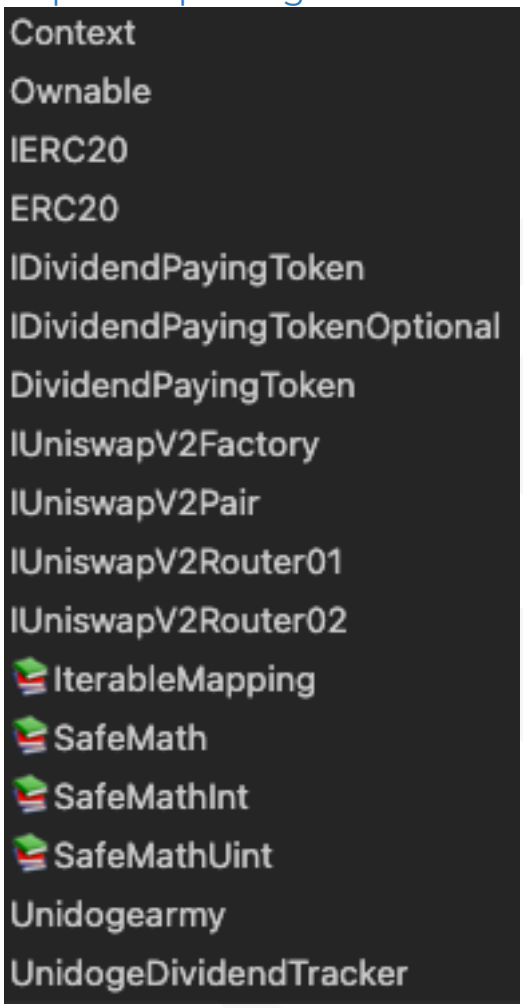
2. Testing and automated analysis that includes the following:
    i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
    ii) Symbolic execution, which is analysing a program 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:



Tested Contract Files

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

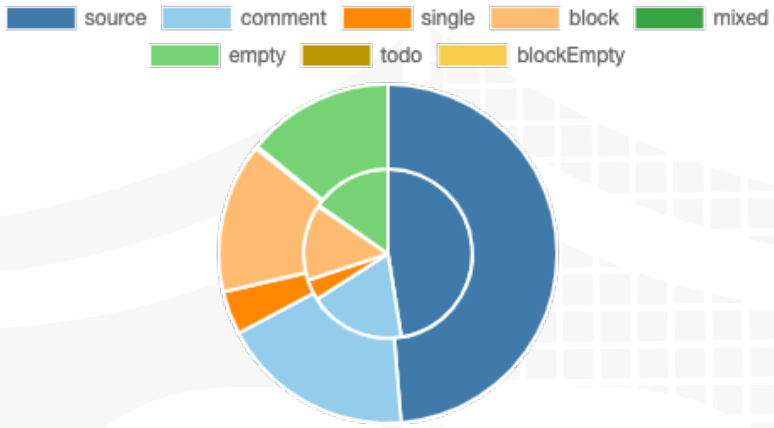
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

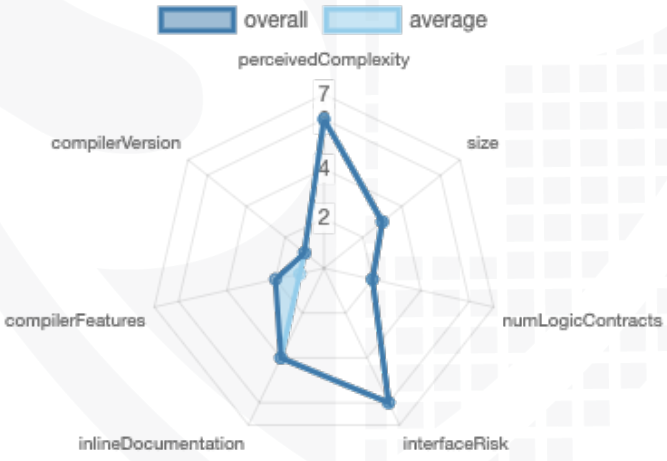
File Name	SHA-1 Hash
contracts/unidoge.sol	6eadf3d6a618a77f790717d6d5b30e31fe5a6b58

Metrics

Source Lines
v1.0



Risk Level
v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	5	4	7	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	184	8

Version	External	Internal	Private	Pure	View
1.0	142	159	11	33	73

State Variables

Version	Total	Public
1.0	69	51

Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	`^0.8.4`		`yes`	**** (0 asm blocks)	

Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	ECRecover	New/Create/Create2

1.0	yes			yes		yes → New Contract:UnidogeDividendTracker → New Contract:UNCLDividendTracker

Scope of Work

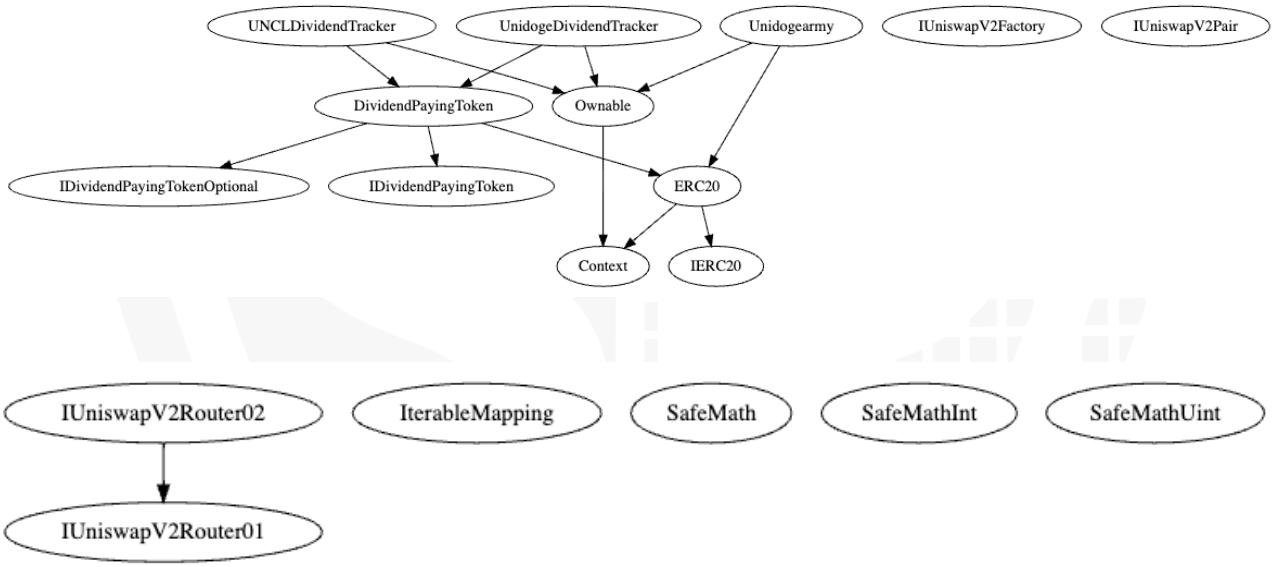
The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

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	✓	✓	✓

Write functions of contract

1. afterPreSale
2. approve
3. claim
4. decreaseAllowance
5. excludeFromDividend
6. excludeFromFees
7. excludeMultipleAccountsFromFees
8. increaseAllowance
9. lock
10. processDividendTracker
11. renounceOwnership
12. setAutomatedMarketMakerPair
13. setLiquifyEnabled
14. setMarketingEnabled
15. setMaxBuyTransaction
16. setMaxSellTransaction
17. setMaxWalletToken
18. setSellTransactionMultiplier
19. setSendUNCLInTx
20. setSendUnidogeInTx
21. setSwapTokensAtAmount
22. setTeamEnabled
23. setTradingIsEnabled
24. setUNCLDividendEnabled
25. setUnidogeDividendEnabled
26. setUnidogeDividendPriority
27. transfer
28. transferFrom
29. transferOwnership
30. updateClaimWait
31. updateGasForProcessing
32. updateLiquidityFee
33. updateLiquidityWallet
34. updateMarketingFee
35. updateMarketingWallet
36. updateMinUNCLBeforeSendDividend
37. updateMinUnidogeBeforeSendDividend
38. updateMinimumBalanceForDividends
39. updateTeamWallet
40. updateUNCLDividendRewardFee
41. updateUNCLDividendToken
42. updateUNCLDividendTracker
43. updateUnidogeDividendRewardFee
44. updateUnidogeDividendToken
45. updateUnidogeDividendTracker
46. updateUniswapV2Router

Deployer cannot mint any new tokens

Name	Exist	Tested	Verified
Deployer cannot mint	–	–	–

Max / Total Supply: 100.000.000.000

Comments:

v1.0

- Set Balance function is using mint/burn function in DividendPayingToken

Deployer cannot burn or lock user funds

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

Comments:

v1.0

- Set Balance function is using mint/burn function in DividendPayingToken
- Deployer can lock user funds by
  - Setting tradingIsEnabled to false
  - maxBuyTransactionAmount to 0
  - maxSellTransactionAmount to 0
  - maxWalletToken to 0

Deployer cannot pause the contract

Name	Exist	Tested	Verified
Deployer cannot pause	-	-	-

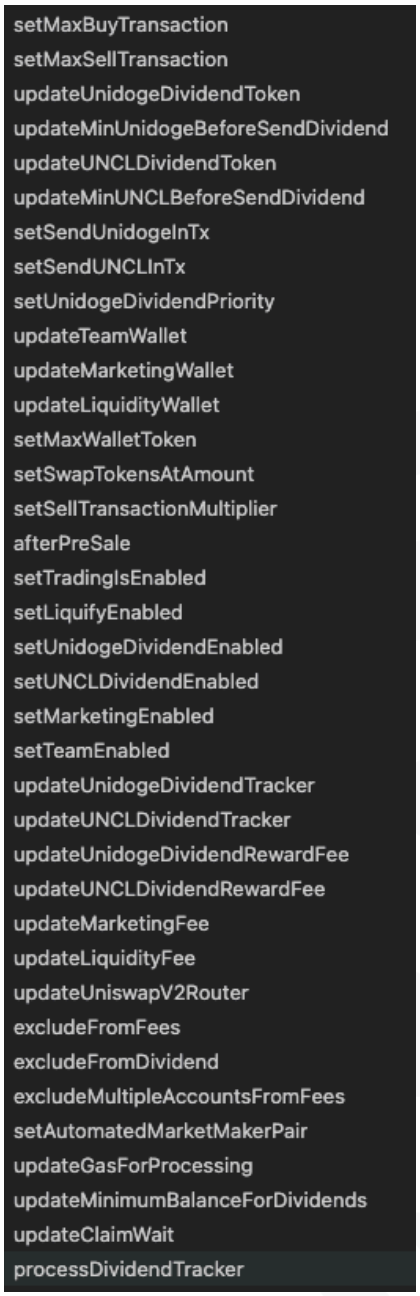
Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verfified / Checked	✓
Partly Verified	⚑
Unverified / Not checked	✗
Not available	–

Modifiers



Comments

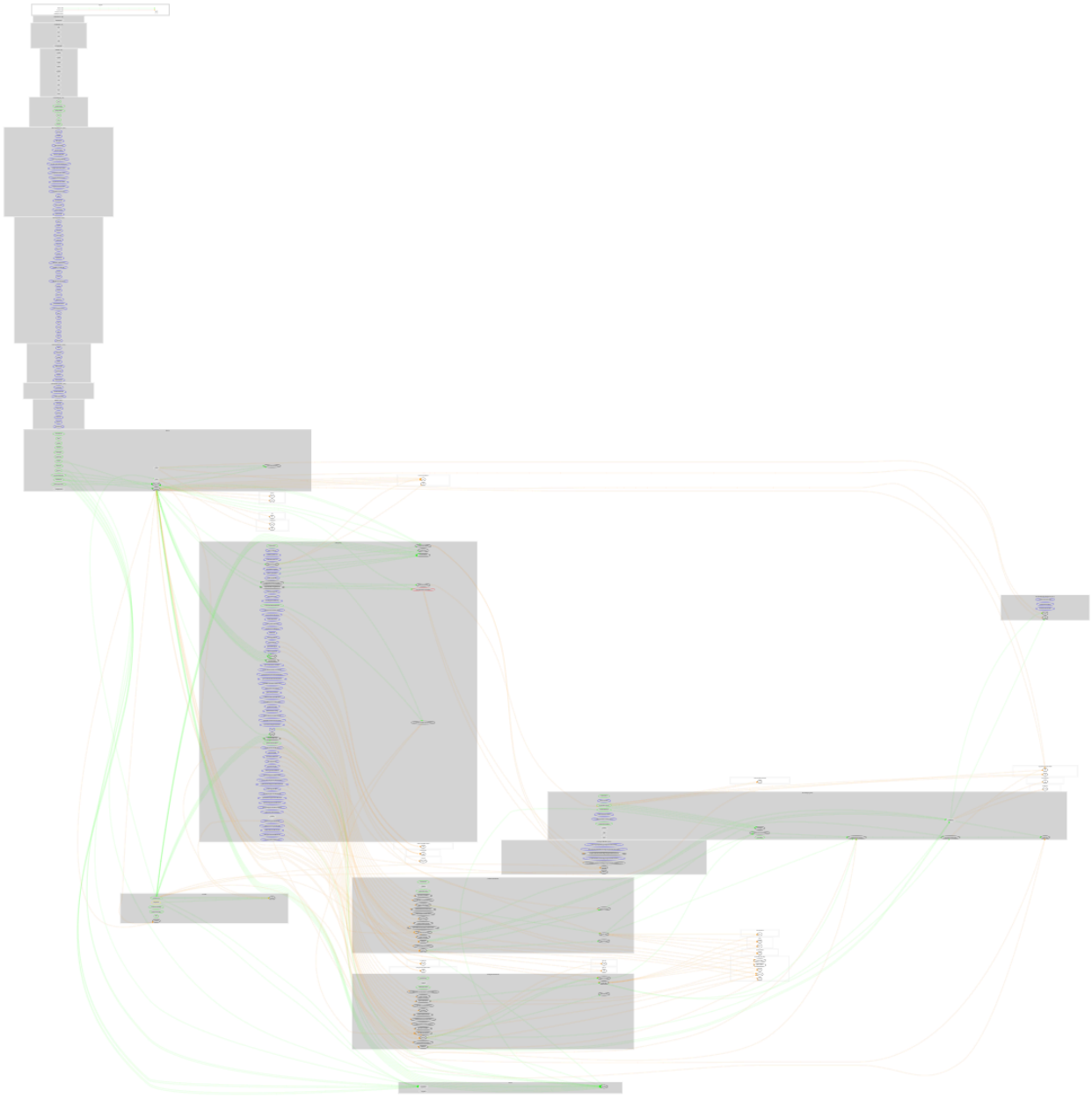
- Deployer can set following state variables without any limitations
  - maxBuyTransactionAmount
  - maxSellTransactionAmount
  - minTokenBeforeSendDividend
  - maxWalletToken
  - swapTokensAtAmount
  - sellFeeIncreaseFactor
  - gasForProcessing
  - minimumTokenBalanceForDividends

- Deployer can enable/disable following state variables

    - sendUnidogeInTx
    - sendUNCLInTx
    - isExcludedFromFees
    - tradingIsEnabled
    - LiquifyEnabled
    - unidogeDividendEnabled
    - unclDividendEnabled
    - marketingEnabled
    - teamEnabled
    - unidogeDividendTracker
    - excludedFromDividends

- Following state variables can be set maximal to 25
    - unidogeDividendRewardsFee
    - unclDividendRewardsFee
    - marketingFee
    - LiquidityFee
    -

CallGraph



Source Units in Scope
v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
📝📚🔍🎨	contracts/unidoge.sol	11	7	2533	2153	1262	577	1167	💰💠🧱🌀🌞♻️
📝📚🔍🎨	**Totals**	**11**	**7**	**2533**	**2153**	**1262**	**577**	**1167**	💰💠🧱🌀🌞♻️

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, ...)

Audit Results

AUDIT PASSED

Critical issues

No critical issues

High issues

No high issues

Medium issues

Issue	File	Type	Line	Description
#1	Main	Reentrancy vulnerabilities	1865	Apply the [`check-effects-interactions pattern`](http://solidity.readthedocs.io/en/v0.4.21/security-considerations.html#re-entrancy).or nonReentrant modifier from OpenZeppelin
#2	Main	Ownership cannot regained after using lock function	46	Owner cannot regain ownership if “lock” function was used because “unlock” function is missing If you implement unlock function ensure that ownership cannot regained by old owner if “_previousOwner” was set. Set _previousOwner to zero address after unlocking After owner renounced/ transfered ownership, avoid old owner can regaining ownership

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	7	The current pragma Solidity directive is „"^0.8.4"".
#3	Main	Missing Zero Address Validation (missing-zero-check)	2353, 2138, 1509, 1503, 1497, 1467, 1458	Check that the address is not zero
#4	Main	Local variables shadowing	584	Rename the local variables that shadow another component - _name - _symbol
#5	Main	Missing Events Arithmetic	1450, 1454, 1515, 1523, 1519, 1492, 1667, 1661, 1655, 1649	Emit an event for critical parameter changes

Informational issues

Issue	File	Type	Line	Description
#1	Main	State variables that could be declared constant (constable-states)	563, 1297	Add the `constant` attributes to state variables that never change
#2	Main	Unused return values	2030, 1845, 1846	Ensure that all the return values of the function calls are used and handle both success and failure cases if needed by the business logic

#3	Main	Functions that are not used	28, 458, 1201, 1163, 1221, 1071, 1081, 1056, 1046, 1244, 1234	Remove unused functions
#4	Main	Unused state variables	563	Remove unused state variables

#5	Main	Unnecessary code	702	Remove the following red part from source code because it is not reachable
				
				function _transfer(address from, address to, uint256 value) internal virtual override {
				require(false);
				
				int256 _magCorrection = magnifiedDividendPerShare.mul(value).toInt256Safe();
				
				magnifiedDividendCorrections[from] = magnifiedDividendCorrections[from].add(_magCorrection);
				
				magnifiedDividendCorrections[to] = magnifiedDividendCorrections[to].sub(_magCorrection);
				}

#6	Main	Misspelling	1372	Change tokensIntoLiqudity To tokensIntoLiquidity

Audit Comments

17. January 2022:

- Read whole report for more information

SWC Attacks

ID	Title	Relationships	Status
SWC-136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SWC-135	Code With No Effects	CWE-1164: Irrelevant Code	NOT PASSED
SWC-134	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SWC-133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SWC-132	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SWC-123	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SWC-122	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SWC-119	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	NOT PASSED
SWC-118	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SWC-117	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SWC-116	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-115	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SWC-114	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	NOT PASSED
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SWC-104	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SWC-103	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	NOT PASSED
SWC-102	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SWC-101	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SWC-100	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY