



Smart Contract Audit

FOR

Dogxim

DATED : 20 October 23'



AUDIT SUMMARY

Project name – Dogxim

Date: 20 October 2023

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **Passed**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:

A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :

The code has undergone static analysis using Slither.

Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/address/0x27dEFbfA39ec39E2d4bcC021C01c41e6A84b6833#code>



Token Information

Token Address :

0xc0F165Bf35BecACeFC871bBb93dD21d5597D102a

Name: Dogxim

Symbol: DOGXIM

Decimals: 9

Netowrk: BSC

Token Type: BEP20

Owner: 0xa6DCa99A12728007EA0Ac399b5b75bF9b15D36a3
(at time of writing the audit)

Deployer:

0xa6DCa99A12728007EA0Ac399b5b75bF9b15D36a3

Token Supply: 10,000,000,000,000

Checksum:

666e75b39d29acabb5178c89e9848d7b41227d93

Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:
<https://testnet.bscscan.com/address/0x27dEFbfA39ec39E2d4bcC021C01c41e6A84b6833#code>



TOKEN OVERVIEW

buy fee: 0-25%

Sell fee: 0-25%

transfer fee: 0-25%

Fee Privilege: Owner

Ownership: Owned

Minting: None

Max Tx: No

Blacklist: No

Other Privileges:

- Initial distribution of the tokens
 - Modifying fees
-



AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
 - Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
 - Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
 - Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
 - Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.
-



VULNERABILITY CHECKLIST

- | | |
|------------------------------------|-------------------------------|
| ✓ Return values of low-level calls | ✓ Gasless Send |
| ✓ Private modifier | ✓ Using block.timestamp |
| ✓ Multiple Sends | ✓ Re-entrancy |
| ✓ Using Suicide | ✓ Tautology or contradiction |
| ✓ Gas Limitand Loops | ✓ Timestamp Dependence |
| ✓ Address hardcoded | ✓ Revert/require functions |
| ✓ Exception Disorder | ✓ Use of tx.origin |
| ✓ Using inline assembly | ✓ Integer overflow/underflow |
| ✓ Divide before multiply | ✓ Dangerous strict equalities |
| ✓ Missing Zero Address Validation | ✓ Using SHA3 |
| ✓ Compiler version not fixed | ✓ Using throw |
-



CLASSIFICATION OF RISK

Severity

Description

◆ Critical

These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.

◆ High-Risk

A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.

◆ Medium-Risk

A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.

◆ Low-Risk

A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.

◆ Gas Optimization /Suggestion

A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity

Found

◆ Critical

0

◆ High-Risk

0

◆ Medium-Risk

0

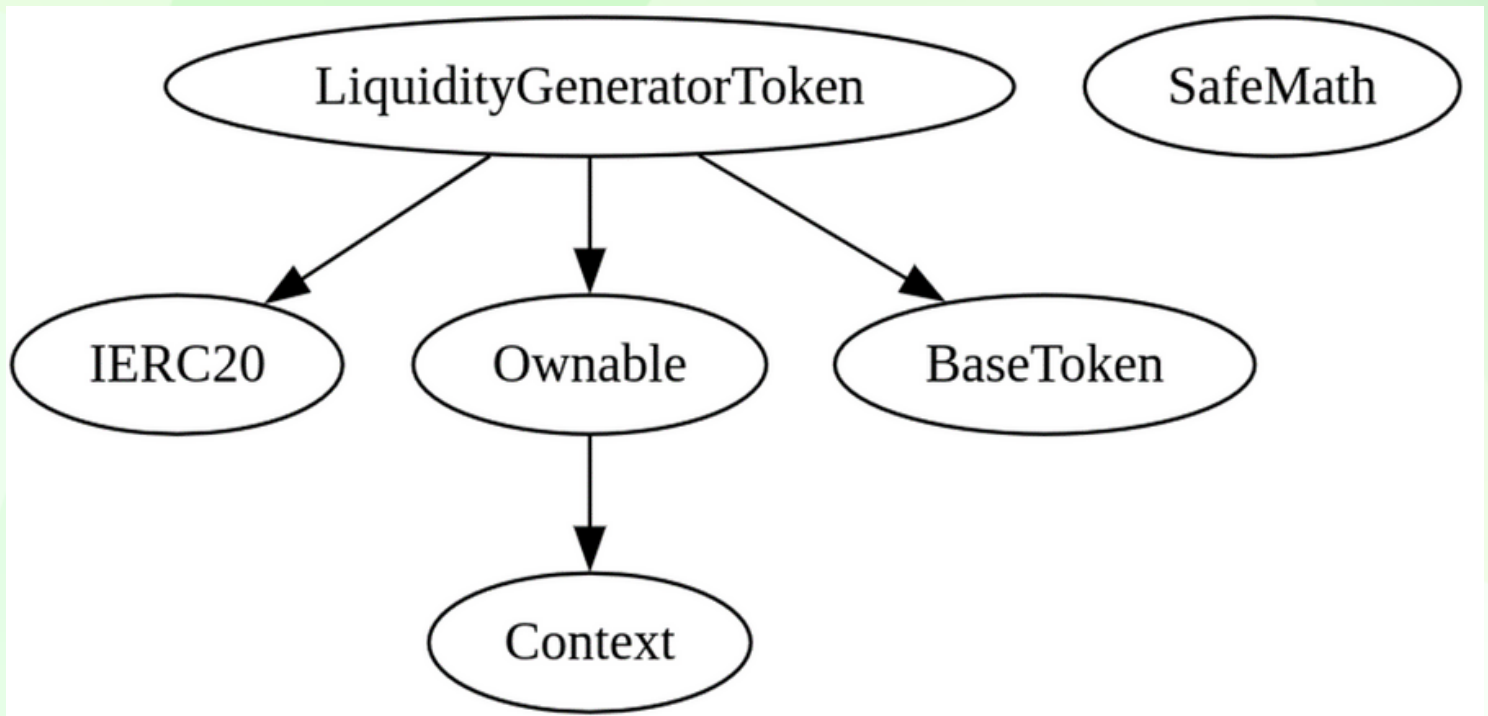
◆ Low-Risk

0

◆ Gas Optimization / Suggestions

0

INHERITANCE TREE



POINTS TO NOTE

- **Owner is able to change buy/sell/transfer fees in range 0-25%**
 - Owner is not able to blacklist an arbitrary address.
 - Owner is not able to disable trades
 - Owner is not able to set max buy/sell/transfer/hold amounts
 - Owner is not able to mint new tokens
-



STATIC ANALYSIS

```
Variable LiquidityGeneratorToken._getValues(uint256).rTransferAmount (contracts/Token.sol#1331) is too similar to LiquidityGeneratorToken._getValues(uint256).tTransferAmount (contracts/Token.sol#1326)
Variable LiquidityGeneratorToken.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1208) is too similar to LiquidityGeneratorToken._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1611)
Variable LiquidityGeneratorToken._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1372-1374) is too similar to LiquidityGeneratorToken._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1611)
Variable LiquidityGeneratorToken._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1609) is too similar to LiquidityGeneratorToken._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1256)
Variable LiquidityGeneratorToken._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1587) is too similar to LiquidityGeneratorToken._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1634)
Variable LiquidityGeneratorToken._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1609) is too similar to LiquidityGeneratorToken._getTValues(uint256).tTransferAmount (contracts/Token.sol#1355-1357)
Variable LiquidityGeneratorToken.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1208) is too similar to LiquidityGeneratorToken._getValues(uint256).tTransferAmount (contracts/Token.sol#1326)
Variable LiquidityGeneratorToken._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1609) is too similar to LiquidityGeneratorToken._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1589)
Variable LiquidityGeneratorToken._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1254) is too similar to LiquidityGeneratorToken._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1611)
Variable LiquidityGeneratorToken._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1587) is too similar to LiquidityGeneratorToken._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1611)
Variable LiquidityGeneratorToken._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1587) is too similar to LiquidityGeneratorToken._getValues(uint256).tTransferAmount (contracts/Token.sol#1326)
Variable LiquidityGeneratorToken._getValues(uint256).rTransferAmount (contracts/Token.sol#1331) is too similar to LiquidityGeneratorToken._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1256)
Variable LiquidityGeneratorToken._getValues(uint256).rTransferAmount (contracts/Token.sol#1331) is too similar to LiquidityGeneratorToken._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1634)
Variable LiquidityGeneratorToken._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1609) is too similar to LiquidityGeneratorToken._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1634)
Variable LiquidityGeneratorToken._getValues(uint256).rTransferAmount (contracts/Token.sol#1331) is too similar to LiquidityGeneratorToken._getTValues(uint256).tTransferAmount (contracts/Token.sol#1355-1357)
Variable LiquidityGeneratorToken._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1609) is too similar to LiquidityGeneratorToken._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1611)
Variable LiquidityGeneratorToken._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1632) is too similar to LiquidityGeneratorToken._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1611)
Variable LiquidityGeneratorToken.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1208) is too similar to LiquidityGeneratorToken._getTValues(uint256).tTransferAmount (contracts/Token.sol#1355-1357)
Variable LiquidityGeneratorToken.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1208) is too similar to LiquidityGeneratorToken._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1256)
Variable LiquidityGeneratorToken._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1372-1374) is too similar to LiquidityGeneratorToken._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1256)
Variable LiquidityGeneratorToken._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1609) is too similar to LiquidityGeneratorToken._getValues(uint256).tTransferAmount (contracts/Token.sol#1326)
Variable LiquidityGeneratorToken._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1587) is too similar to LiquidityGeneratorToken._getTValues(uint256).tTransferAmount (contracts/Token.sol#1355-1357)
Variable LiquidityGeneratorToken._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1587) is too similar to LiquidityGeneratorToken._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1256)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

LiquidityGeneratorToken.charityAddress (contracts/Token.sol#1003) should be immutable
LiquidityGeneratorToken.decimals (contracts/Token.sol#990) should be immutable
LiquidityGeneratorToken.name (contracts/Token.sol#988) should be immutable
LiquidityGeneratorToken.symbol (contracts/Token.sol#989) should be immutable
LiquidityGeneratorToken.tTotal (contracts/Token.sol#984) should be immutable
LiquidityGeneratorToken.swapAndLiquifyEnabled (contracts/Token.sol#1006) should be immutable
LiquidityGeneratorToken.uniswapV2Pair (contracts/Token.sol#1002) should be immutable
LiquidityGeneratorToken.uniswapV2Router (contracts/Token.sol#1001) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

Result => A static analysis of contract's source code has been performed using slither,

No major issues were found in the output



CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
⌞	**Function Name** **Visibility** **Mutability** **Modifiers**				
	IERC20 Interface				
⌞	totalSupply	External	!		NO !
⌞	balanceOf	External	!		NO !
⌞	transfer	External	!	●	NO !
⌞	allowance	External	!		NO !
⌞	approve	External	!	●	NO !
⌞	transferFrom	External	!	●	NO !
	Context Implementation				
⌞	_msgSender	Internal	🔒		
⌞	_msgData	Internal	🔒		
	Ownable Implementation Context				
⌞	<Constructor>	Public	!	●	NO !
⌞	owner	Public	!		NO !
⌞	renounceOwnership	Public	!	●	onlyOwner
⌞	transferOwnership	Public	!	●	onlyOwner
⌞	_setOwner	Private	🔒	●	
	SafeMath Library				
⌞	tryAdd	Internal	🔒		
⌞	trySub	Internal	🔒		
⌞	tryMul	Internal	🔒		
⌞	tryDiv	Internal	🔒		
⌞	tryMod	Internal	🔒		
⌞	add	Internal	🔒		
⌞	sub	Internal	🔒		
⌞	mul	Internal	🔒		
⌞	div	Internal	🔒		
⌞	mod	Internal	🔒		
⌞	sub	Internal	🔒		
⌞	div	Internal	🔒		
⌞	mod	Internal	🔒		



CONTRACT ASSESMENT

```
| **Address** | Library | |||
|  └ | isContract | Internal 🔒 | | |
|  └ | sendValue | Internal 🔒 | ● | |
|  └ | functionCall | Internal 🔒 | ● | |
|  └ | functionCall | Internal 🔒 | ● | |
|  └ | functionCallWithValue | Internal 🔒 | ● | |
|  └ | functionCallWithValue | Internal 🔒 | ● | |
|  └ | functionStaticCall | Internal 🔒 | | |
|  └ | functionStaticCall | Internal 🔒 | | |
|  └ | functionDelegateCall | Internal 🔒 | ● | |
|  └ | functionDelegateCall | Internal 🔒 | ● | |
|  └ | verifyCallResult | Internal 🔒 | | |
|||||

| **IUniswapV2Router01** | Interface | |||
|  └ | factory | External ! | | NO ! |
|  └ | WETH | External ! | | NO ! |
|  └ | addLiquidity | External ! | ● | NO ! |
|  └ | addLiquidityETH | External ! | 🏠 | NO ! |
|  └ | removeLiquidity | External ! | ● | NO ! |
|  └ | removeLiquidityETH | External ! | ● | NO ! |
|  └ | removeLiquidityWithPermit | External ! | ● | NO ! |
|  └ | removeLiquidityETHWithPermit | External ! | ● | NO ! |
|  └ | swapExactTokensForTokens | External ! | ● | NO ! |
|  └ | swapTokensForExactTokens | External ! | ● | NO ! |
|  └ | swapExactETHForTokens | External ! | 🏠 | NO ! |
|  └ | swapTokensForExactETH | External ! | ● | NO ! |
|  └ | swapExactTokensForETH | External ! | ● | NO ! |
|  └ | swapETHForExactTokens | External ! | 🏠 | NO ! |
|  └ | quote | External ! | | NO ! |
|  └ | getAmountOut | External ! | | NO ! |
|  └ | getAmountIn | External ! | | NO ! |
|  └ | getAmountsOut | External ! | | NO ! |
|  └ | getAmountsIn | External ! | | NO ! |
|||||
```



CONTRACT ASSESMENT

```
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 ||| |
|  └ | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● |NO ! |
|  └ | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● |NO ! |
|  └ | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● |NO ! |
|  └ | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🟢 |NO ! |
|  └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● |NO ! |
|||||
| **IUniswapV2Factory** | Interface | |||
|  └ | feeTo | External ! | |NO ! |
|  └ | feeToSetter | External ! | |NO ! |
|  └ | getPair | External ! | |NO ! |
|  └ | allPairs | External ! | |NO ! |
|  └ | allPairsLength | External ! | |NO ! |
|  └ | createPair | External ! | ● |NO ! |
|  └ | setFeeTo | External ! | ● |NO ! |
|  └ | setFeeToSetter | External ! | ● |NO ! |
|||||
| **BaseToken** | Implementation | |||
|||||
| **LiquidityGeneratorToken** | Implementation | IERC20, Ownable, BaseToken |||
|  └ | <Constructor> | Public ! | 🟢 |NO ! |
|  └ | name | Public ! | |NO ! |
|  └ | symbol | Public ! | |NO ! |
|  └ | decimals | Public ! | |NO ! |
|  └ | totalSupply | Public ! | |NO ! |
|  └ | balanceOf | Public ! | |NO ! |
|  └ | transfer | Public ! | ● |NO ! |
|  └ | allowance | Public ! | |NO ! |
|  └ | approve | Public ! | ● |NO ! |
|  └ | transferFrom | Public ! | ● |NO ! |
|  └ | increaseAllowance | Public ! | ● |NO ! |
|  └ | decreaseAllowance | Public ! | ● |NO ! |
|  └ | isExcludedFromReward | Public ! | |NO ! |
|  └ | totalFees | Public ! | |NO ! |
|  └ | deliver | Public ! | ● |NO ! |
|  └ | reflectionFromToken | Public ! | |NO ! |
|  └ | tokenFromReflection | Public ! | |NO ! |
|  └ | excludeFromReward | Public ! | ● |onlyOwner |
|  └ | includeInReward | External ! | ● |onlyOwner |
|  └ | _transferBothExcluded | Private 🟡 | ● |||
|  └ | excludeFromFee | Public ! | ● |onlyOwner |
```



CONTRACT ASSESMENT

	setTaxFeePercent	External !		onlyOwner
	setLiquidityFeePercent	External !		onlyOwner
	setCharityFeePercent	External !		onlyOwner
	setSwapBackSettings	External !		onlyOwner
	<Receive Ether>	External !		NO !
	_reflectFee	Private		
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private		
	_takeCharityFee	Private		
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		
	calculateCharityFee	Private		
	removeAllFee	Private		
	restoreAllFee	Private		
	isExcludedFromFee	Public !		NO !
	_approve	Private		
	_transfer	Private		
	swapAndLiquify	Private		lockTheSwap
	swapTokensForEth	Private		
	addLiquidity	Private		
	_tokenTransfer	Private		
	_transferStandard	Private		
	_transferToExcluded	Private		
	_transferFromExcluded	Private		

Legend

|Symbol | Meaning|

|:------:|------|

| | Function can modify state |

| | Function is payable |



FUNCTIONAL TESTING

1- Adding liquidity (**passed**):

<https://testnet.bscscan.com/tx/0xf214e06c2f8f56d968b06435fe01a75efa86f1bef093c97d7557a2aa24358155>

2- Buying when excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x9e70eff888f8ec6305a960ba48322b94bce92d59f6e02017d8c6c30935f804f6>

3- Selling when excluded (0% tax) from fees (**passed**):

<https://testnet.bscscan.com/tx/0xa6a0f356a946bf66f9a97b3f0c27abe287ad3463cf754ab5a0885f8b621a32e2>

4- Transferring when excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xe8ef0b38315aead5343b627d57ad13bf9c03aad3b4f850993fbd432dcbb8e9fe>

5- Buying from a regular wallet (0-25% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x97fdcf7421345ef9d3805fddaea45a75826721950e594ae44a65bf952778b3c0>

6- Selling from a regular wallet (0-25% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xe45823cfe4092311231561e84b9982fa2d8dae1d60eade139c01caa19bdc316>

7- Transferring from a regular wallet (0-25% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xc172717353ba6df30a3804eb9121eff80ea95e74702604dab1e7b748cd8ee74f>

8- Internal swap (marketing bnb + auto-liquidity) (**passed**):

<https://testnet.bscscan.com/tx/0xe45823cfe4092311231561e84b9982fa2d8dae1d60eade139c01caa19bdc316>



DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.



ABOUT AUDITACE

We specializes in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



<https://auditace.tech/>



https://t.me/Audit_Ace



https://twitter.com/auditace_



<https://github.com/Audit-Ace>
