auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

XAI Doge

DATED : 17 April 23'

AUDIT SUMMARY

Project name – X.AI Doge

Date: 17 April, 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	1	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 done on BSC Test network, each test has its transaction has 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 Link:
https://testnet.bscscan.com/token/0xb8a55a80ed7403e6da09d8b776398919df15894e

Token Information

Token Name : X.AI Doge

Token Symbol: XAIDoge

Decimals: 18

Token Supply: 1,000,000,000,000,000

Token Address:
0x66fB4C2320eA49f947eC465968bf0840c99D5152

Checksum:
7c55028dddcffdcd9680eb94b451f7f815ad68f1

Owner:
0x1DCDA9eB29f13B22D961b6Cb93bf02a0b651F6de
(at time of writing the audit)

TOKEN OVERVIEW

Fees:

Buy Fees: up to 25%

Sell Fees: up to 25%

Transfer Fees: up to 25%

Fees Privilege: Owner

Ownership: Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Priviliges: including and excluding form fee - changing distribution settings (min tokens to be eligible, cool down between claims etc)

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

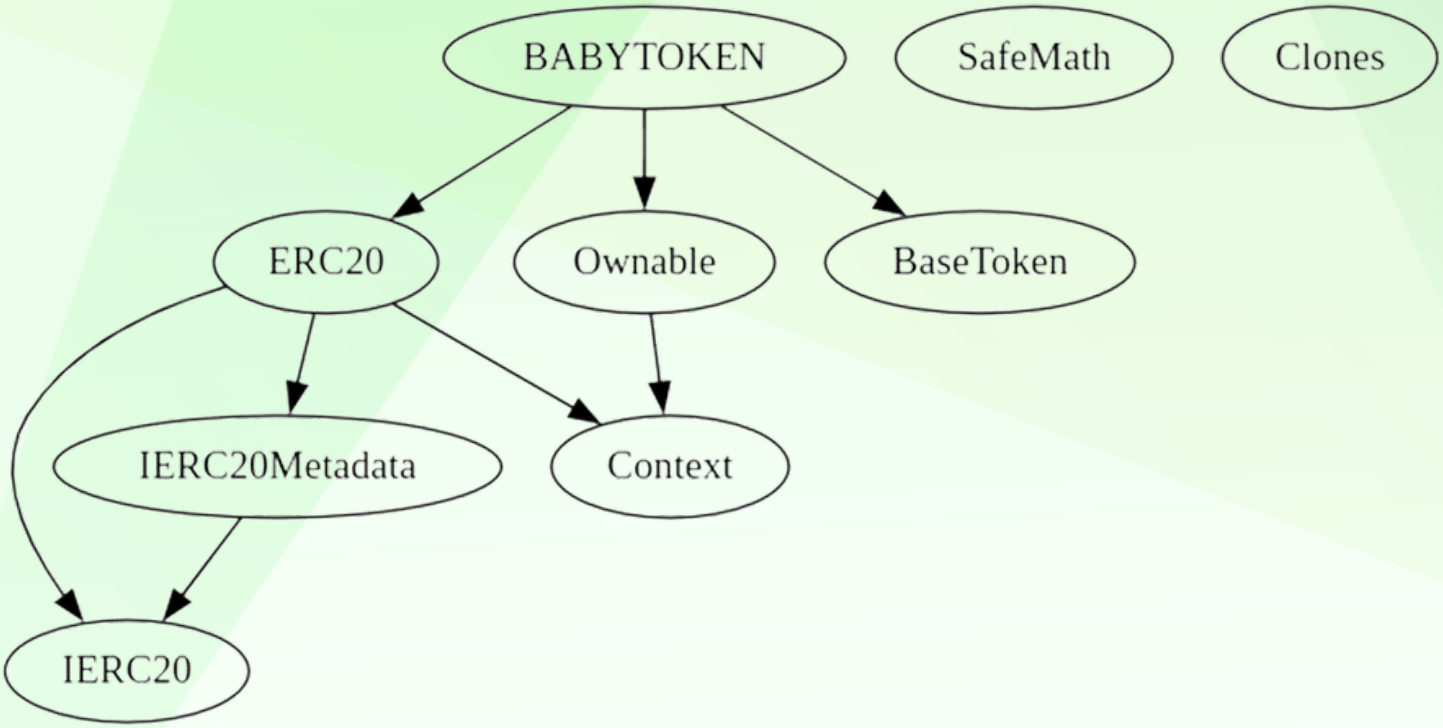
CLASSIFICATION OF RISK

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	1
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



POINTS TO NOTE

- Owner is able to change buy/sell/transfer fees but sum of fees can not exceed 25%
- Contract is recognized as proxy in bscscan, however this is because dividend distributor is minimal proxy contract which is not upgradeable currently
- Owner is not able to set max buy/sell/transfer/hold amount
- Owner is not able to blacklist an arbitrary wallet
- Owner is not able to disable trades
- Owner is not able to mint new tokens

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 ❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	decimals	External ❗		NO ❗
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	<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 ❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO ❗

CONTRACT ASSESMENT

└	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 🔒		
Clones	Library			
└	clone	Internal 🔒	🛑	
└	cloneDeterministic	Internal 🔒	🛑	
└	predictDeterministicAddress	Internal 🔒		
└	predictDeterministicAddress	Internal 🔒		
Address	Library			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionStaticCall	Internal 🔒		
└	functionStaticCall	Internal 🔒		
└	functionDelegateCall	Internal 🔒	🛑	
└	functionDelegateCall	Internal 🔒	🛑	
└	verifyCallResult	Internal 🔒		
IUniswapV2Factory	Interface			
└	feeTo	External ❗		NO ❗
└	feeToSetter	External ❗		NO ❗
└	getPair	External ❗		NO ❗

CONTRACT ASSESMENT

└	allPairs	External ❗			NO ❗
└	allPairsLength	External ❗			NO ❗
└	createPair	External ❗	🛑	NO ❗
└	setFeeTo	External ❗	🛑	NO ❗
└	setFeeToSetter	External ❗	🛑	NO ❗
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 ❗
IUniswapV2Router02	Interface	IUniswapV2Router01		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
IERC20Upgradeable	Interface			
└	totalSupply	External ❗			NO ❗
└	balanceOf	External ❗			NO ❗
└	transfer	External ❗	🛑	NO ❗
└	allowance	External ❗			NO ❗
└	approve	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
IERC20MetadataUpgradeable	Interface	IERC20Upgradeable		

CONTRACT ASSESMENT

└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	decimals	External ❗		NO ❗
Initializable	Implementation			
ContextUpgradeable	Implementation	Initializable		
└	__Context_init	Internal 🔒	🛑	initializer
└	__Context_init_unchained	Internal 🔒	🛑	initializer
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
ERC20Upgradeable	Implementation	Initializable, ContextUpgradeable, IERC20Upgradeable, IERC20MetadataUpgradeable		
└	__ERC20_init	Internal 🔒	🛑	initializer
└	__ERC20_init_unchained	Internal 🔒	🛑	initializer
└	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 ❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
└	__Ownable_init	Internal 🔒	🛑	initializer
└	__Ownable_init_unchained	Internal 🔒	🛑	initializer
└	owner	Public ❗		NO ❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_setOwner	Private 🔐	🛑	
IUniswapV2Pair	Interface			

CONTRACT ASSESMENT

└	name	External ❗			NO ❗	
└	symbol	External ❗			NO ❗	
└	decimals	External ❗			NO ❗	
└	totalSupply	External ❗			NO ❗	
└	balanceOf	External ❗			NO ❗	
└	allowance	External ❗			NO ❗	
└	approve	External ❗	🛑	NO ❗	
└	transfer	External ❗	🛑	NO ❗	
└	transferFrom	External ❗	🛑	NO ❗	
└	DOMAIN_SEPARATOR	External ❗			NO ❗	
└	PERMIT_TYPEHASH	External ❗			NO ❗	
└	nonces	External ❗			NO ❗	
└	permit	External ❗	🛑	NO ❗	
└	MINIMUM_LIQUIDITY	External ❗			NO ❗	
└	factory	External ❗			NO ❗	
└	token0	External ❗			NO ❗	
└	token1	External ❗			NO ❗	
└	getReserves	External ❗			NO ❗	
└	price0CumulativeLast	External ❗			NO ❗	
└	price1CumulativeLast	External ❗			NO ❗	
└	kLast	External ❗			NO ❗	
└	mint	External ❗	🛑	NO ❗	
└	burn	External ❗	🛑	NO ❗	
└	swap	External ❗	🛑	NO ❗	
└	skim	External ❗	🛑	NO ❗	
└	sync	External ❗	🛑	NO ❗	
└	initialize	External ❗	🛑	NO ❗	
SafeMathInt	Library				
└	mul	Internal 🔒			
└	div	Internal 🔒			
└	sub	Internal 🔒			
└	add	Internal 🔒			
└	abs	Internal 🔒			
└	toUint256Safe	Internal 🔒			
SafeMathUint	Library				
└	toInt256Safe	Internal 🔒			
IterableMapping	Library				
└	get	Internal 🔒			
└	getIndexOfKey	Internal 🔒			

CONTRACT ASSESMENT

└	getKeyAtIndex	Internal 🔒		
└	size	Internal 🔒		
└	set	Internal 🔒	🛑	
└	remove	Internal 🔒	🛑	
DividendPayingTokenInterface	Interface				
└	dividendOf	External ❗		NO ❗	
└	withdrawDividend	External ❗	🛑	NO ❗	
DividendPayingTokenOptionalInterface	Interface				
└	withdrawableDividendOf	External ❗		NO ❗	
└	withdrawnDividendOf	External ❗		NO ❗	
└	accumulativeDividendOf	External ❗		NO ❗	
DividendPayingToken	Implementation	ERC20Upgradeable, OwnableUpgradeable, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface			
└	__DividendPayingToken_init	Internal 🔒	🛑	initializer
└	distributeCAKEDividends	Public ❗	🛑	onlyOwner
└	withdrawDividend	Public ❗	🛑	NO ❗	
└	_withdrawDividendOfUser	Internal 🔒	🛑	
└	dividendOf	Public ❗		NO ❗	
└	withdrawableDividendOf	Public ❗		NO ❗	
└	withdrawnDividendOf	Public ❗		NO ❗	
└	accumulativeDividendOf	Public ❗		NO ❗	
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_setBalance	Internal 🔒	🛑	
BABYTOKENDividendTracker	Implementation	OwnableUpgradeable, DividendPayingToken			
└	initialize	External ❗	🛑	initializer
└	_transfer	Internal 🔒		
└	withdrawDividend	Public ❗		NO ❗	
└	excludeFromDividends	External ❗	🛑	onlyOwner
└	isExcludedFromDividends	Public ❗		NO ❗	
└	updateClaimWait	External ❗	🛑	onlyOwner
└	updateMinimumTokenBalanceForDividends	External ❗	🛑	onlyOwner
└	getLastProcessedIndex	External ❗		NO ❗	
└	getNumberOfTokenHolders	External ❗		NO ❗	
└	getAccount	Public ❗		NO ❗	
└	getAccountAtIndex	Public ❗		NO ❗	
└	canAutoClaim	Private 🔐		
└	setBalance	External ❗	🛑	onlyOwner

CONTRACT ASSESMENT

└	process	Public ❗	🛑	NO ❗
└	processAccount	Public ❗	🛑	onlyOwner
BaseToken	Implementation			
BABYTOKEN	Implementation	ERC20, Ownable, BaseToken		
└	<Constructor>	Public ❗	💵	ERC20
└	<Receive Ether>	External ❗	💵	NO ❗
└	setSwapTokensAtAmount	External ❗	🛑	onlyOwner
└	excludeFromFees	External ❗	🛑	onlyOwner
└	excludeMultipleAccountsFromFees	External ❗	🛑	onlyOwner
└	setMarketingWallet	External ❗	🛑	onlyOwner
└	setTokenRewardsFee	External ❗	🛑	onlyOwner
└	setLiquiditFee	External ❗	🛑	onlyOwner
└	setMarketingFee	External ❗	🛑	onlyOwner
└	_setAutomatedMarketMakerPair	Private 🔐	🛑	
└	updateGasForProcessing	Public ❗	🛑	onlyOwner
└	updateClaimWait	External ❗	🛑	onlyOwner
└	getClaimWait	External ❗		NO ❗
└	updateMinimumTokenBalanceForDividends	External ❗	🛑	onlyOwner
└	getMinimumTokenBalanceForDividends	External ❗		NO ❗
└	getTotalDividendsDistributed	External ❗		NO ❗
└	isExcludedFromFees	Public ❗		NO ❗
└	withdrawableDividendOf	Public ❗		NO ❗
└	dividendTokenBalanceOf	Public ❗		NO ❗
└	excludeFromDividends	External ❗	🛑	onlyOwner
└	isExcludedFromDividends	Public ❗		NO ❗
└	getAccountDividendsInfo	External ❗		NO ❗
└	getAccountDividendsInfoAtIndex	External ❗		NO ❗
└	processDividendTracker	External ❗	🛑	NO ❗
└	claim	External ❗	🛑	NO ❗
└	getLastProcessedIndex	External ❗		NO ❗
└	getNumberOfDividendTokenHolders	External ❗		NO ❗
└	_transfer	Internal 🔒	🛑	
└	swapAndSendToFee	Private 🔐	🛑	
└	swapAndLiquify	Private 🔐	🛑	
└	swapTokensForEth	Private 🔐	🛑	
└	swapTokensForCake	Private 🔐	🛑	
└	addLiquidity	Private 🔐	🛑	
└	swapAndSendDividends	Private 🔐	🛑	

Legend

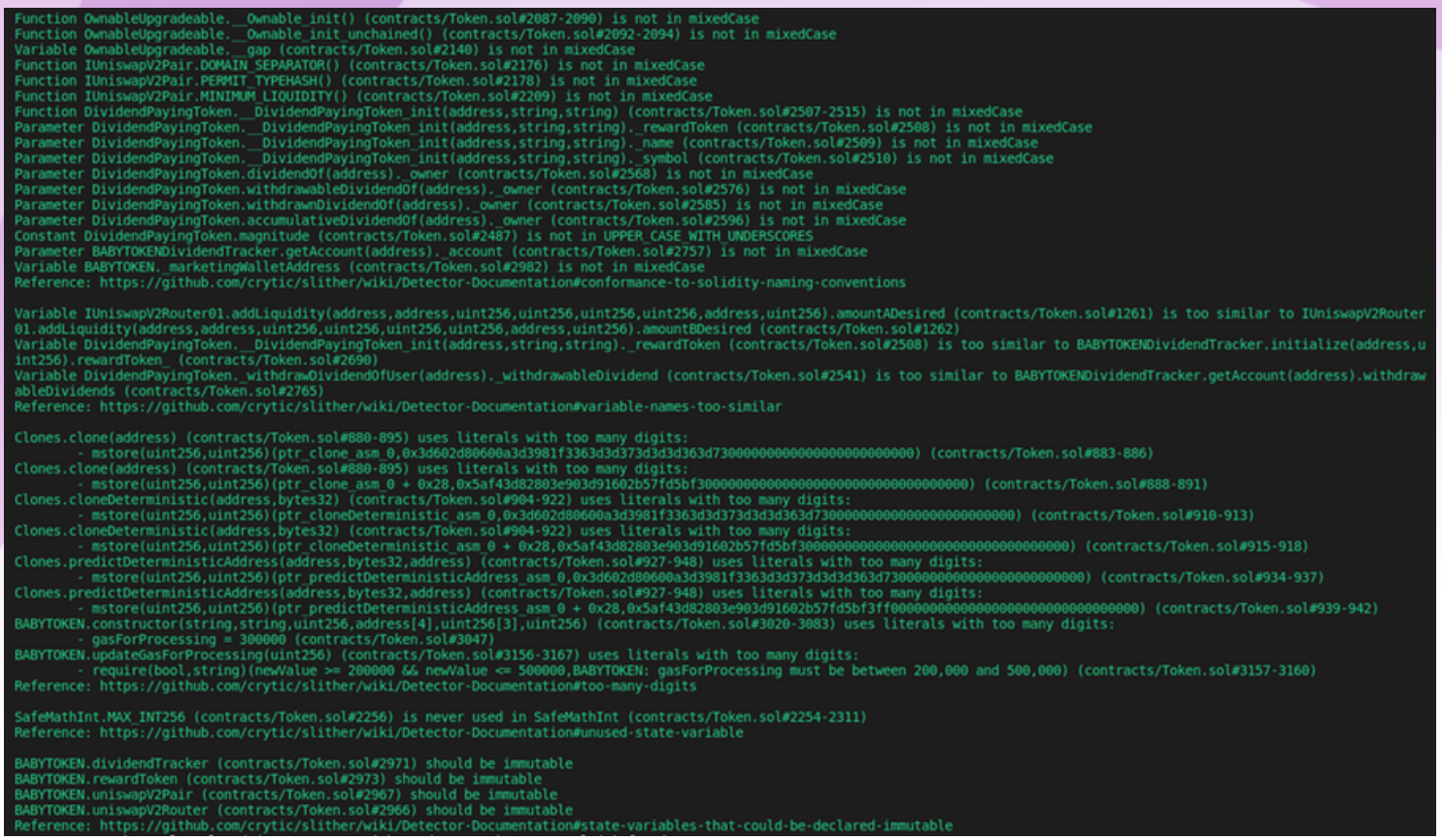
CONTRACT ASSESMENT

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Token distribution:

It should be noted that the owner currently holds 100% of the total supply. However, information about the distribution of these tokens is not available, and it is recommended that investors exercise caution when considering this aspect.

STATIC ANALYSIS



```
Function OwnableUpgradeable.__Ownable_init() (contracts/Token.sol#2087-2090) is not in mixedCase
Function OwnableUpgradeable.__Ownable_init_unchained() (contracts/Token.sol#2092-2094) is not in mixedCase
Variable OwnableUpgradeable.__gap (contracts/Token.sol#2140) is not in mixedCase
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#2176) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#2178) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#2209) is not in mixedCase
Function DividendPayingToken.__DividendPayingToken_init(address,string,string) (contracts/Token.sol#2507-2515) is not in mixedCase
Parameter DividendPayingToken.__DividendPayingToken_init(address,string,string)._rewardToken (contracts/Token.sol#2508) is not in mixedCase
Parameter DividendPayingToken.__DividendPayingToken_init(address,string,string)._name (contracts/Token.sol#2509) is not in mixedCase
Parameter DividendPayingToken.__DividendPayingToken_init(address,string,string)._symbol (contracts/Token.sol#2510) is not in mixedCase
Parameter DividendPayingToken.dividendOf(address)._owner (contracts/Token.sol#2568) is not in mixedCase
Parameter DividendPayingToken.withdrawableDividendOf(address)._owner (contracts/Token.sol#2576) is not in mixedCase
Parameter DividendPayingToken.withdrawnDividendOf(address)._owner (contracts/Token.sol#2585) is not in mixedCase
Parameter DividendPayingToken.accumulativeDividendOf(address)._owner (contracts/Token.sol#2596) is not in mixedCase
Constant DividendPayingToken.magnitude (contracts/Token.sol#2487) is not in UPPER_CASE_WITH_UNDERSCORES
Parameter BABYTOKENDividendTracker.getAccount(address)._account (contracts/Token.sol#2757) is not in mixedCase
Variable BABYTOKEN._marketingWalletAddress (contracts/Token.sol#2982) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#1261) is too similar to IUniswapV2Router
01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#1262)
Variable DividendPayingToken.__DividendPayingToken_init(address,string,string)._rewardToken (contracts/Token.sol#2508) is too similar to BABYTOKENDividendTracker.initialize(address,u
int256).rewardToken_ (contracts/Token.sol#2690)
Variable DividendPayingToken._withdrawDividendOfUser(address)._withdrawableDividend (contracts/Token.sol#2541) is too similar to BABYTOKENDividendTracker.getAccount(address).withdraw
ableDividends (contracts/Token.sol#2765)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

Clones.clone(address) (contracts/Token.sol#880-895) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_clone_asm_0,0x3d602d80600a3d3981f3363d3d373d3d3d363d730000000000000000000000000000) (contracts/Token.sol#883-886)
Clones.clone(address) (contracts/Token.sol#880-895) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_clone_asm_0 + 0x28,0x5af43d82803e903d91602b57fd5bf3000000000000000000000000000000000000) (contracts/Token.sol#888-891)
Clones.cloneDeterministic(address,bytes32) (contracts/Token.sol#904-922) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_cloneDeterministic_asm_0,0x3d602d80600a3d3981f3363d3d373d3d3d363d730000000000000000000000000000) (contracts/Token.sol#910-913)
Clones.cloneDeterministic(address,bytes32) (contracts/Token.sol#904-922) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_cloneDeterministic_asm_0 + 0x28,0x5af43d82803e903d91602b57fd5bf3000000000000000000000000000000000000) (contracts/Token.sol#915-918)
Clones.predictDeterministicAddress(address,bytes32,address) (contracts/Token.sol#927-948) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_predictDeterministicAddress_asm_0,0x3d602d80600a3d3981f3363d3d373d3d3d363d730000000000000000000000000000) (contracts/Token.sol#934-937)
Clones.predictDeterministicAddress(address,bytes32,address) (contracts/Token.sol#927-948) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_predictDeterministicAddress_asm_0 + 0x28,0x5af43d82803e903d91602b57fd5bf3ff0000000000000000000000000000000000000000) (contracts/Token.sol#939-942)
BABYTOKEN.constructor(string,string,uint256,address[4],uint256[3],uint256) (contracts/Token.sol#3020-3083) uses literals with too many digits:
        - gasForProcessing = 300000 (contracts/Token.sol#3047)
BABYTOKEN.updateGasForProcessing(uint256) (contracts/Token.sol#3156-3167) uses literals with too many digits:
        - require(bool,string)(newValue >= 200000 && newValue <= 500000,BABYTOKEN: gasForProcessing must be between 200,000 and 500,000) (contracts/Token.sol#3157-3160)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

SafeMathInt.MAX_INT256 (contracts/Token.sol#2256) is never used in SafeMathInt (contracts/Token.sol#2254-2311)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable

BABYTOKEN.dividendTracker (contracts/Token.sol#2971) should be immutable
BABYTOKEN.rewardToken (contracts/Token.sol#2973) should be immutable
BABYTOKEN.uniswapV2Pair (contracts/Token.sol#2967) should be immutable
BABYTOKEN.uniswapV2Router (contracts/Token.sol#2966) 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

FUNCTIONAL TESTING

Router (PCS V2):
0xD99D1c33F9fC3444f8101754aBC46c52416550D1

All the functionalities have been tested, no issues were found

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0x3d9da3528617d72b0501584abe75a9be7ed36e901432776698a92e82bd2fb558

2- Buying when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x3e96e85cf726815511b68de12c78b06b9e107541ea439eca08b9e7833475f3fd

3- Selling when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xa68cf98933a27a8827fd6a18dd7f6b9c9188b035566335ab50ead03eba5ba8a5

4- Transferring when excluded from fees (0% tax) (passed):
https://testnet.bscscan.com/tx/0x75f959d95742dc8701cedf52f13ab5b1534b8610af5f63aa322de3bdb85104be

5- Buying when not excluded from fees (up to 25% tax) (passed):
https://testnet.bscscan.com/tx/0x5f2423fb3ef17cd354450ef2cc4405843728d07dbe29cc88c4f261635fd5ffff

6- Selling when not excluded from fees (up to 25% tax) (passed):
https://testnet.bscscan.com/tx/0xee991777ab773c9f92c90f6007769a5f8a16aef70e0914d4e044cf048d985414

FUNCTIONAL TESTING

7- Transferring when not excluded from fees (up to 25% tax) (passed):
https://testnet.bscscan.com/tx/0xcd6e30990811b2cfdc80e502007b65cdf4dd0c70396d215ede68f18deb6480c0

8- Internal swap (passed):
marketing wallet received Rewards
https://testnet.bscscan.com/address/0xa2da001d772453f7a1d520148663462ebcbd79b4#tokentxns

9- Reflections (passed):
https://testnet.bscscan.com/tx/0xee991777ab773c9f92c90f6007769a5f8a16aef70e0914d4e044cf048d985414

8- Auto Liquidity (passed):
https://testnet.bscscan.com/token/0xc170359e0cc5f1e5c4a1d93f5afdae95ae70ba72?a=0x000000000000000000000000000000000000dead

MANUAL TESTING

Logical – Call to external ERC20 token

Severity: Medium
Status: Not Resolved
Overview:
The current implementation of the contract uses **DOGE** as its reward token **(0xbA2aE424d960c26247Dd6c32edC70B295c744C43). DOGE** is beyond the scope of this audit, and any exploits or issues found in the **DOGE** token can have an impact on the rewards system in **DOGE (considering that DOGE is an upgradeable contract)**. This may include consequences such as high gas usage or trade disablement.

Recommendation:

•Use a simpler token such as BUSD, USDC etc as reward token in order to reduce overall gas usage and mitigate other potential issues.
•Create a feature to be able to update reward token
•Give rewards in native token

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