CFG NINJA AUDITS

Security Assessment

DogeReaperAI Token

September 26, 2023

Audit Status: Pass

Audit Edition: Pinksale

POWERED BY BLADE POOL

Project Overview

Token Summary

Parameter	Result
Address	0x9c7884Df791761847Df1E77f71400F3215a88A48
Name	DogeReaperAI
Token Tracker	DogeReaperAI (DRAI)
Decimals	18
Supply	1,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.4+commit.c7e474f2
Contract Name	BABYTOKEN
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x9c7884Df791761847Df1E77f71400F3215a88A48#code
Payment Tx	0x3cf3b8fc26ed7a374333bc0871f34e5162026cc52142c5b16958c07b8c971c6b

Main Contract Assessed
Contract Name

Name	Contract	Live
DogeReaperAI	0x9c7884Df791761847Df1E77f71400F3215a88A48	Yes

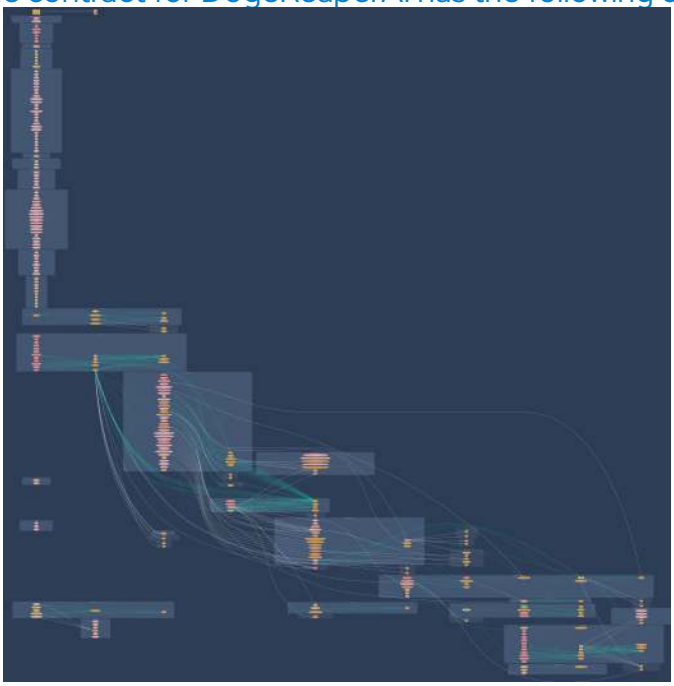
TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
DogeReaperAI	28485e40b4263b47c7504df29b8c08dd61f55535	DogeReaperAI.sol
DogeReaperAI		
DogeReaperAI		
DogeReaperAI		

Call Graph

The contract for DogeReaperAI has the following call graph structure.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	BabyToken.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	BabyToken.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	BabyToken.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	BabyToken.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	BabyToken.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	BabyToken.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	BabyToken.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	BabyToken.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	BabyToken.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	BabyToken.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	BabyToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	BabyToken.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	BabyToken.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	BabyToken.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	BabyToken.sol	L: 0 C: 0
SWC-115	low	Authorization through tx.origin.	BabyToken.sol	L: 3123 C: 12,L: 3223 C: 20
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	BabyToken.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	BabyToken.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	BabyToken.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	BabyToken.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	BabyToken.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	BabyToken.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	BabyToken.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	BabyToken.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	BabyToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-125	Pass	Incorrect Inheritance Order.	BabyToken.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	BabyToken.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	BabyToken.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	BabyToken.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	BabyToken.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	BabyToken.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	BabyToken.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	BabyToken.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	BabyToken.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	BabyToken.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	BabyToken.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	BabyToken.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Smart Contract Vulnerability Details

SWC-115 - Authorization through tx.origin

CWE-477: Use of Obsolete Function

Description:

tx.origin is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since tx.origin returns the original sender of the transaction which in this case is the authorized account.

Remediation:

tx.origin should not be used for authorization. Use msg.sender instead.

References:

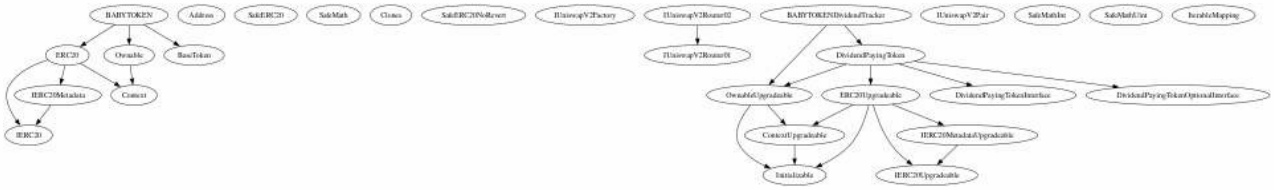
Solidity Documentation - tx.origin

Ethereum Smart Contract Best Practices - Avoid using tx.origin

SigmaPrime - Visibility.

Inheritance

The contract for DogeReaperAI has the following inheritance structure.



Social Media Checks

Social Media	URL	Result
Twitter	https://x.com/DogeReaperAI?s=20	Pass
Other	https://www.tiktok.com/@dogereaperai6?_t=8g0zXoTHc7E&_r=1, https://discord.gg/ykyb8jBD, https://youtube.com/@Dreaperai?si=c6AhI30uhzclYwB4, https://instagram.com/dogereaper_ai?igshid=MzMyNGUyNmU2YQ==	Pass
Website	Dreaperai.tech	Pass
Telegram	https://t.me/DogeReaperAI	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Audit Result

Final Audit Score

Review	Score
Security Score	85
Auditor Score	80

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- This is a BabyToken, please review the tax structure.
- Please DYOR on the project.

Auditor Score =80
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.