



DogePal

\$DOGEPAL

BSC

meme

Contract:

0x9833.....584e88

Issues	Found	Fixed
Critical	3	0
Medium	1	0
Minor	0	0
Informational	3	0

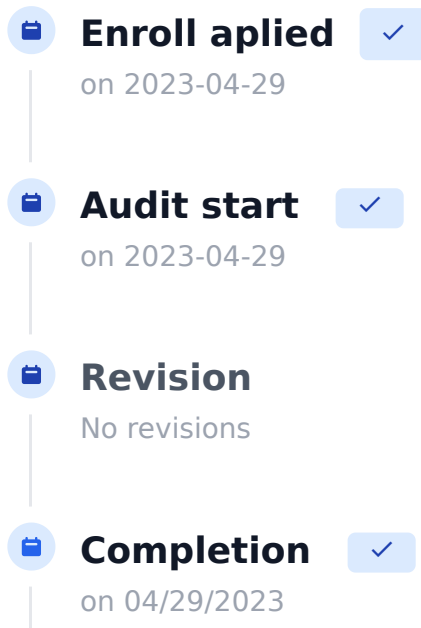
7.6/10

AUDIT FAILED

Project Description

Introducing the ultimate fusion of two iconic brands in the world of finance and cryptocurrency - Dogecoin and PayPal This innovative project brings together the fun and friendly spirit of Dogecoin with the secure and trusted payment platform of PayPal. Whether you're a seasoned crypto enthusiast or a first-time user, our seamless integration allows for easy transactions and quick access to your funds. Join DogePal revolution and experience the future of finance today!

Project details



Language: **Solidity**

Contract address: **0x98...4e88**

Owner: **0xcc...fbc9**

SHA-256:
995...fd8

Supply: **1,000,000,000,000**

Decimals: **9**

Deployer: **0x68...6049**

Chain: **Binance Smart Chain**

Compiler: **v0.7.6+commit.7338295f**

Optimization: **Yes with 200 runs**

License: **MIT**

Verified: **Yes**

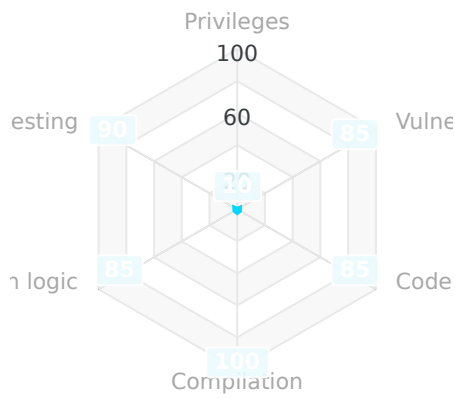
Contract type: **bep-20**

Contract Name: **DogePal**

Deploy date: **2023-04-02**

Overview

Enroll



Minting[?]

The contract owner has the authority to modify the balance of tokens at other addresses

Blacklist[?]

Can blacklist multiple wallets at once

Ownership

Owned, high risk considering the nature of functions

Honeypot

Honeypot risk

Buy fees[?]

Can set up to 33%

Sell fees[?]

Can set up to 33%

Proxy[?]

No proxy contract detected

Max tx amount[?]

Can set maxTx without limits

Trading Cooldown

No limits

Anti Bot

No antibot

Pause[?]

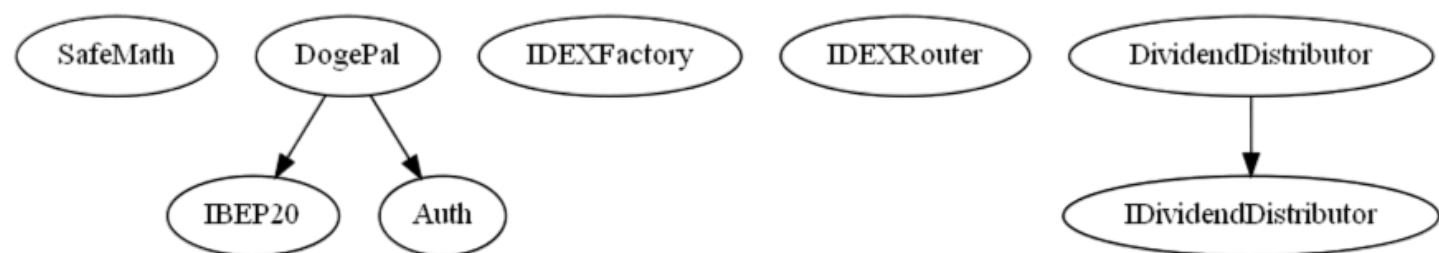
Can pause trading

Hidden Owner

No

- Safe
- Caution advised
- Be careful
- Extreme caution

Inheritance



Contract details [0x98...4e88](#)

Contracts and libraries collapse

```
| **SafeMath** | Library |   |||
| **IBEP20** | Interface |   |||
| **Auth** | Implementation |   |||
| **IDEXFactory** | Interface |   |||
| **IDEXRouter** | Interface |   |||
| **IDividendDistributor** | Interface |   |||
| **DividendDistributor** | Implementation | IDividendDistributor |||
| **DogePal** | Implementation | IBEP20, Auth |||
```

Modifiers collapse

Enroll

Contract SafeMath

+-----+-----+		
Function	Modifiers	
+-----+-----+		
add	[]	
sub	[]	
sub	[]	
mul	[]	
div	[]	
div	[]	
+-----+-----+		

Contract IDEXFactory

+-----+-----+		
Function	Modifiers	

▼ Constructor calls collapse

```
#####
##### DividendDistributor #####
#####

## Constructor Call Sequence
    - DividendDistributor

## Constructor Definitions

### DividendDistributor

    constructor (address _router) {
        router = _router != address(0)
            ? IDEXRouter(_router)
            : IDEXRouter(0x10ED43C718714eb63d5aA57B78B54704E256024E);
    }
```

▼ Requires collapse

Contract SafeMath

+-----+-----+		
Function	require or assert	
+-----+-----+		
add	require(bool,string)(c >= a, SafeMath: addition overflow)	
sub	require(bool,string)(b <= a, errorMessage)	
sub	require(bool,string)(b <= a, errorMessage)	
mul	require(bool,string)(c / a == b, SafeMath: multiplication overf	
div	require(bool,string)(b > 0, errorMessage)	

```
|   div   |   require(bool,string)(b > 0,errorMessage)
```

```
+-----+
```

Contract IDEXFactory

```
+-----+
```

```
|   Function   |   require or assert   |
```

Findings

High Severity

✓ Centralization - Owner can modify balance of addresses

Lines: #735

Description: The contract owner has the authority to modify the balance of tokens at other addresses through multiTransfer functions

Possible remediation: Delete functions

✓ Centralization - blacklist

Lines: #636-644

Description: The owner can blacklist multiple addresses at once. By blacklisting wallets, the owner can prevent certain individuals or groups from trading

Possible remediation: Delete function or create limits

✓ Centralization - pause function

Lines: #567-569

Description: The owner can pause the trading any time, when this function is activated the transfers don't work. function tradingStatus(bool _status) public onlyOwner { tradingOpen = _status; }

Possible remediation: Remove function

Medium Severity

✓ Centralization - High fees

Lines: #659-667

Description: Owners can set buy and sell fees to a max of 33% each, meaning 66% in total.

Possible remediation: Decrease the limits

Low Severity

No low severity issues found

Informational

✓ A floating pragma is set

Lines: #7

Description: The current pragma Solidity directive is ^0.7.6

Possible remediation: It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds

SWC Vulnerabilities

✓ 35/37 tests passed [collapse](#)

Code #	Name	Result	Severity
SWC-100	Function Default Visibility	Passed	n/a
SWC-101	Integer Overflow and Underflow	Passed	n/a
SWC-102	Outdated Compiler Version	Passed	n/a
SWC-103	Floating Pragma	Failed	Informational
SWC-104	Unchecked Call Return Value	Passed	n/a
SWC-105	Unprotected Ether Withdrawal	Passed	n/a
SWC-106	Unprotected SELF-DESTRUCT Instruction	Passed	n/a
SWC-107	Reentrancy	Passed	n/a
SWC-108	State Variable Default Visibility	Failed	Informational
SWC-109	Uninitialized Storage Pointer	Passed	n/a
SWC-110	Assert Violation	Passed	n/a
SWC-111	Use of Deprecated Solidity Functions	Passed	n/a
SWC-112	Delegatecall to Untrusted Callee	Passed	n/a
SWC-113	DoS with Failed Call	Passed	n/a
SWC-114	Transaction Order Dependence	Passed	n/a

Code #	Name	Result	Severity
SWC-115	Authorization through tx.origin	Passed	n/a
SWC-116	Block values as a proxy for time	Passed	n/a
SWC-117	Signature Malleability	Passed	n/a
SWC-118	Incorrect Constructor Name		Passed n/a
SWC-119	Shadowing State Variables		Passed n/a
SWC-120	Weak Sources of Randomness from Chain Attributes		Passed n/a
SWC-121	Missing Protection against Signature Replay Attacks		Passed n/a
SWC-122	Lack of Proper Signature Verification		Passed n/a
SWC-123	Requirement Violation		Passed n/a
SWC-124	Write to Arbitrary Storage Location		Passed n/a
SWC-125	Incorrect Inheritance Order		Passed n/a
SWC-126	Insufficient Gas Griefing		Passed n/a
SWC-127	Arbitrary Jump with Function Type Variable		Passed n/a
SWC-128	DoS With Block Gas Limit		Passed n/a
SWC-129	Typographical Error		Passed n/a
SWC-130	Right-To-Left-Override control character (U+202E)		Passed n/a
SWC-131	Presence of unused variables		Passed n/a
SWC-132	Unexpected Ether balance		Passed n/a
SWC-133	Hash Collisions With Multiple Variable Length Arguments		Passed n/a
SWC-134	Message call with the hardcoded gas amount		Passed n/a
SWC-135	Code With No Effects		Passed n/a
SWC-136	Unencrypted Private Data On-Chain		Passed n/a

Other findings

✓ Ignored returned value

DividendDistributor.distributeDividend(address) (token.sol#287-298) ignores return value by RWRD.transfer(shareholder,amount) (token.sol#293)

- Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

Additional information: [↗link](#)

✓ Costly gas operations

DividendDistributor.process(uint256) (token.sol#256-280) has costly operations inside a loop

- Use a local variable to hold the loop computation result.

Additional information: [link](#)

Holders stats (top 10)

0xcc...fbc9	95.00%
0x68...6049	5.00%
0x00...0000 locked	0.00%

KYC & DOXX

- KYC
- ✕

 No information
- DOXX
- ✕

 No information

Website audit <https://dogepal.io/>

- Domain Registry
- GoDaddy
- Domain Expiry Date
- 2024-04-26
- Response Code
- 400

- **SSL Check and HTTPS test**

fail

- **HTTP2**

fail

- **Safe Browsing Test**

fail

Disclaimer

GuardGate is not a financial institution and the information provided on this website does not constitute investment advice, financial advice, trading advice, or any other sort of advice. You should not treat any of the website's content as such. Investing in crypto assets carries a high level of risk and does not hold guarantees for not sustaining financial loss due to their volatility. Accuracy of Information GuardGate will strive to ensure the accuracy of the information listed on this website although it will not hold any responsibility for any missing or wrong information. GuardGate provides all information as is. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion. The purpose of the audit is to analyze the on-chain smart contract source code and to provide a basic overview of the project. While we have used all the information available to us for this straightforward investigation, you should not rely on this report only - we recommend proceeding with several independent audits Be aware that smart contracts deployed on a blockchain aren't secured enough against external vulnerability or a hack. Be aware that active smart contract owner privileges constitute an elevated impact on the smart contract safety and security. Therefore, GuardGate does not guarantee the explicit security of the audited smart contract. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.



GuardGate

PRODUCTS

Audit

Scanner

AMA *coming soon

COMPANY

Pricing

About us

How it works

Enroll

Airdrop *coming soon

Enroll

Disclaimer

STAY IN TOUCH



© 2023 GuardGate Co. All rights reserved.

Enroll