# SMART CONTRACT SECURITY AUDIT

WATCHTOWER

# DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or it's Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

**DISCLAIMER**: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and it's subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:
Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.
Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.
Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.
In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.

# OVERVIEW

**Watchtower was commissioned by DogeKongZilla to complete a Smart Contract audit.**
**The objective of the Audit is to achieve the following:**

- **Review the Project and experience and Development team**
- **Ensure that the Smart Contract functions are necessary and operate as intended.**
- **Identify any vulnerabilities in the Smart Contract code.**

**DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way, All investments are made at your own risk.**
**(https://www.cryptowatchtower.io/)**

# SMART CONTRACT REVIEW

## Contract Created on the 30th October 2021

| | |
|---|---|
| Contract name | DogeKongZilla |
| Contract address | 0x1B442512ED276e3e874149e4f4e51f06AEE8B58c |
| Total supply | 1,000,000,000,000,000 |
| Token ticker | DogeKongZilla |
| Decimals | 9 |
| Token holders | 2214 |
| Transactions count | 11368 |
| Top 5 holders dominance | 21.60% / 43.19% Burn Adjusted |
| Tax fee | 12% |
| Total fees | 12% ~ BUY / 16% ~ SELL |
| Contract deployer address | 0x319735C68D780928DF3C05D7c31C3c4D39D3b0A3 |
| Contract's current owner address | 0x319735C68D780928DF3C05D7c31C3c4D39D3b0A3 |

# Project Overview

## Project Details:

DogeKongZilla is a Rewards Meme Token offering rewards in BNB as a base with plans to complete a dashboard which allows you to choose your rewards.
The Tokenomics show that 8% of all purchase go towards rewards with a requirement of holding 10B DogeKongZilla tokens.
12% of sell transactions go to rewards with an additional 4% towards Liquidity
(The Tokenomics are fair and rewards holders over the developers).

## Tokenomics:

Starting Supply: 1,000,000,000,000,000 (1 Quadrillion)
12% Tax for Buys and 16% for Sells comprising of:
8% Rewards for Buy transactions and 12% rewards for Sells
4% Liquidity Fee

## Team Doxxed:

The DogeKongZilla Team is not doxxed at this point in time.

# CONTRACT FUNCTIONS DETAILS

## Functions (Public)

This contract has 39 available public functions which the owner can call.
These functions were reviewed and can be viewed on BSC Scan or through a DAPP.

**LINK**
https://www.bscscan.com/address/0x1b442512ed276e3e874149e4f4e51f06aee8b58c#writeContract
Function risks: No Scam Functions Identified!

- Tax fees can be increased to high levels making it harder to sell, which is quite normal with Rewards contracts.
- Watchtower believes the owners are operating with honesty as there are no alternate methods of scamming such as a mint function. (The price impact of the Top 5 holders however is a risk- Project wallets should be locked to provide more security to holders).

## Imported Libraries / Interfaces

- Context
- Ownable
- IERC20
- IERC20 Metadata
- DividendPayingTokenOptionalInterface
- DividendPayingTokenInterface
- SafeMathInt
- SafeMathUint
- SafeMath
- ERC20
- DividendPayingToken (https://github.com/roger-wu) + edits
- IUniswapV2Router01
- IUniswapV2Router02
- IUniswapV2Factory
- IUniswapV2Pair

## Overview

| | |
|---|---|
| 1. ADDITION OF COMMENTS: | 10 |
| 2. CALL STACK DEPTH ATTACK: | 10 |
| 3. TIME STAMP DEPENDENCY: | 10 |
| 4. PARTY MULTISIG BUG: | 10 |
| 5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES): | 10 |
| a. TRANSACTION-ORDERING DEPENDENCY: | 10 |
| 6. ACCESS CONTROL AND AUTHORIZATION: | 10 |
| 7. REENTRANCY ATTACKS: | 10 |
| 8. ERC/BEP STANDARD VIOLATIONS: | 10 |
| 9. USAGE OF VISIBILITY LEVELS: | 10 |

# ISSUES CHECKING STATUS

| Issue description | Checking status |
|---|---|
| 1. Compiler errors. | Passed |
| 2. Race conditions and Reentrancy. Cross-function race conditions. | Passed |
| 3. Possible delays in data delivery. | Passed |
| 4. Oracle calls. | Passed |
| 5. Front running. | Passed |
| 6. Timestamp dependence. | Passed |
| 7. Integer Overflow and Underflow. | Passed |
| 8. DoS with Revert. | Passed |
| 9. DoS with block gas limit. | Passed |
| 10. Methods execution permissions. | Passed |

| Issue description | Checking status |
|---|---|
| 11. Economy model of the contract. | Passed |
| 12. The impact of the exchange rate on the logic. | Passed |
| 13. Private user data leaks. | Passed |
| 14. Malicious Event log. | Passed |
| 15. Scoping and Declarations. | Passed |
| 16. Uninitialized storage pointers. | Passed |
| 17. Arithmetic accuracy. | Passed |
| 18. Design Logic. | Passed |
| 19. Cross-function race conditions. | Passed |
| 20. Safe Open Zeppelin contracts implementation and usage. | Passed |
| 21. Fallback function security. | Passed |

# SECURITY ISSUES

## High Severity Issues

- **NO HIGH SEVERITY ISSUES**

## Medium Severity Issues

- **Update Dividend Minimum can be Bypassed.**

If the owner decides to increase the minimumTokenBalanceForDividends the users must make a transaction to trigger setBalance() and let the contract check if the new limit is respected. So, if a user doesn't move their tokens after the function is called, and his balance is lower than minimum amount, he can still receive rewards.
In the Same way if the Minimum is reduced it will not take effect unless holders create an instance where the contract reviews their balance. The best way to do this is to buy or sell a small amount of tokens.

- **Include in Dividends does not update user dividend balance.**

It should be written as:

```
function includeInDividends(address account) external onlyOwner {
        require(excludedFromDividends[account]);
        excludedFromDividends[account] = false;
    _setBalance(account, balanceOf(account));
        tokenHoldersMap.set(account, balanceOf(account));
        emit IncludeInDividends(account);  }
```

# SECURITY ISSUES (CONT)

## Low Severity Issues

- **Coding Efficiency:**

Lines: 1514- 1519: liquidity, operations and buyback wallets are excluded from fees, so these lines could have been removed. Lines 1520-21 already includes them.

```
if(
canSwap &&
!swapping &&
!automatedMarketMakerPairs[from] &&
from != liquidityWallet &&
to != liquidityWallet &&
from != operationsWallet &&
to != operationsWallet &&
from != buyBackWallet &&
to != buyBackWallet &&
!_isExcludedFromFees[to] &&
!_isExcludedFromFees[from] &&
from != address(this) &&
from != address(dividendTracker)
) {
```

# CONCLUSION

**Watchtower reviewed DogeKongZillas' deployed and verified contract to conduct this audit.**
**Watchtower is satisfied that the team is operating with integrity however as noted above there are a low impact coding efficiency errors and the price impact of the Top 5 Holders is a risk.**

### *Watchtower Disclaimer:*

*Please check the disclaimer page and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do your own research. By reading this report you accept and agree to the disclaimer and understand investments are made at your own risk.* ***(https://www.cryptowatchtower.io/)***

## Contact Us

**@Watchtower_WTW**

**Watchtower-WTW**

**Watchtowercrypto**