



Rodeo Solutions
Develop – Audit – Coach

JAILDOGE Token Smart Contract Audit

Rodeo Studios
July 2021

<https://github.com/RodeoSolutions>



Contents

Commission	3
Disclaimer	4
\$JAILDOGE Properties	5
Token Analytics	6
Contract Functions	8
Public	8
View.....	8
Virtual.....	8
Executables.....	8
Owner Executables	8
Checklist	9
Potential Issues	10
Zero Address Owner – Low severity issue.....	10
No logic issues found.....	10
Owner privileges	11
Conclusions	13



Commission

Audited Project	JAILDOGE Token
Project website	https://jaildoge.net/
Contract Owner	0x00
Smart Contract Address	0xBe4628d7E02e9257875149FA4981C400a01A49A3
Blockchain	Binance Main Smart Chain

Rodeo Solutions was commissioned by WOLFY Token owners to perform an audit of their main smart contract. The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.



Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Rodeo Solutions and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rodeo Solutions) owe no duty of care towards you or any other person, nor does Rodeo Solutions make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Rodeo Solutions hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Rodeo Solutions hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rodeo Solutions, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. 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.



\$JAILDOGE Properties

Contract name	JAILDOGE Token
Contract address	0xBe4628d7E02e9257875149FA4981C400a01A49A3
Total supply	1Q
Token ticker	\$JAILDOGE
Decimals	9
Token holders	865
Transactions count	5021
Top 100 holder's dominance	96.90%
Liquidity fee	6
Tax fee	3
Total fees	9
Mintable	No
Burnable	Yes
Uniswap V2 pair	0x43e628cfe34c501f84d62e7dbf77c43d052a09b9
Contract deployer address	0xd2D732d604E873A09dE33f34790485E213d64287
Contract's current owner address	0x00
Marketing Address	0x67896231Ec57D45BA883931940A8CCe995b6d4f1

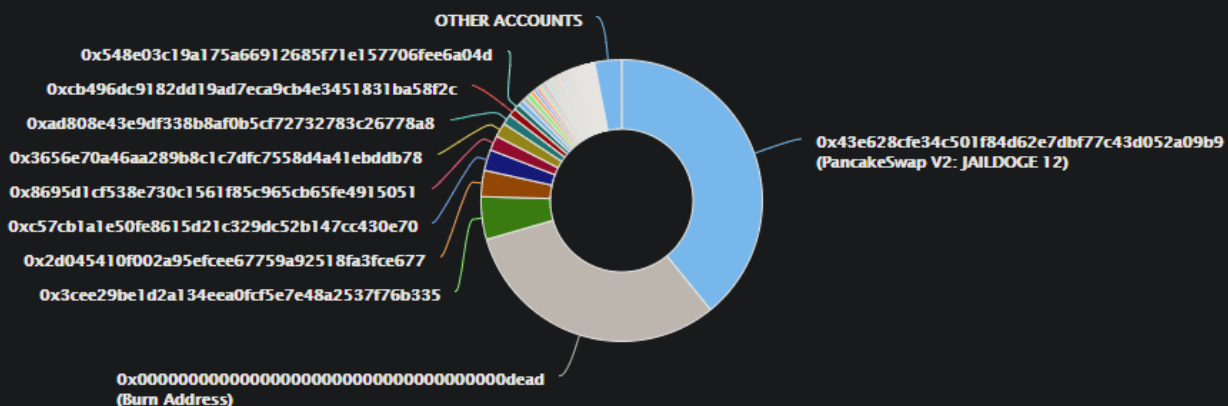
As of 07/23/2021



Token Analytics

Jail Doge Top 100 Token Holders

Source: BscScan.com

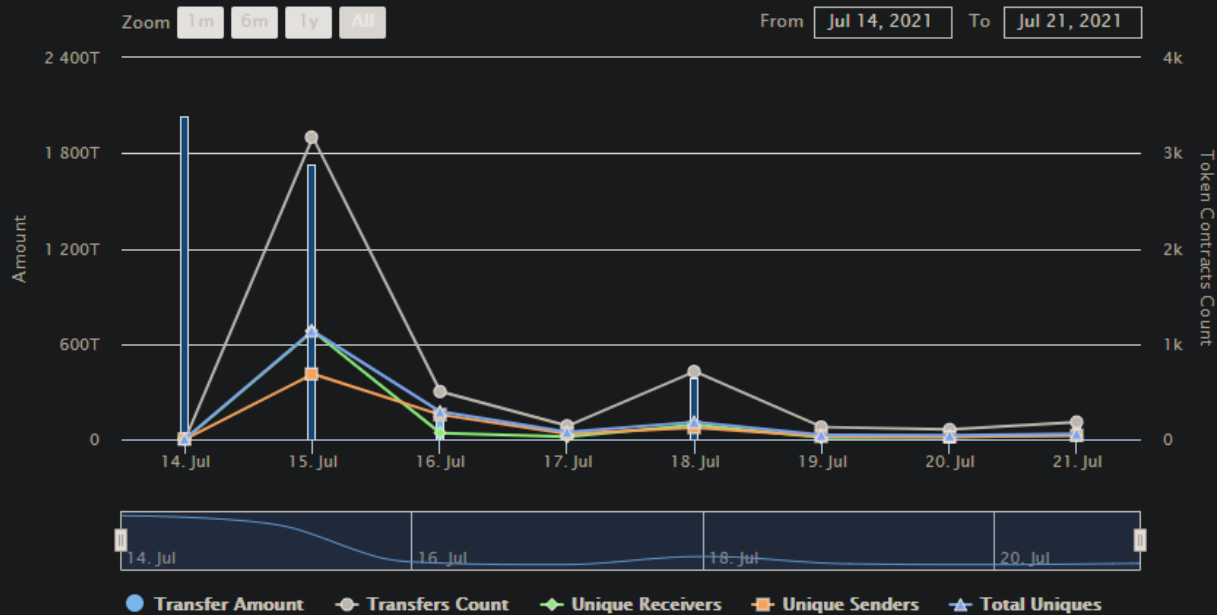


Time Series: Token Contract Overview

Tue 13, Jul 2021 - Tue 20, Jul 2021

Token Contract 0xbe4628d7e02e9257875149fa4981c400a01a49a3 (Jail Doge)

Source: BscScan.com





Time Series: BNB Balance

Tue 13, Jul 2021 - Tue 20, Jul 2021

● **BNB Highest Balance**

On Tue 13, Jul 2021

0.2 BNB

● **BNB Lowest Balance**

On Sat 17, Jul 2021

0.19999999999999184 BNB

■ **USD Highest Value**

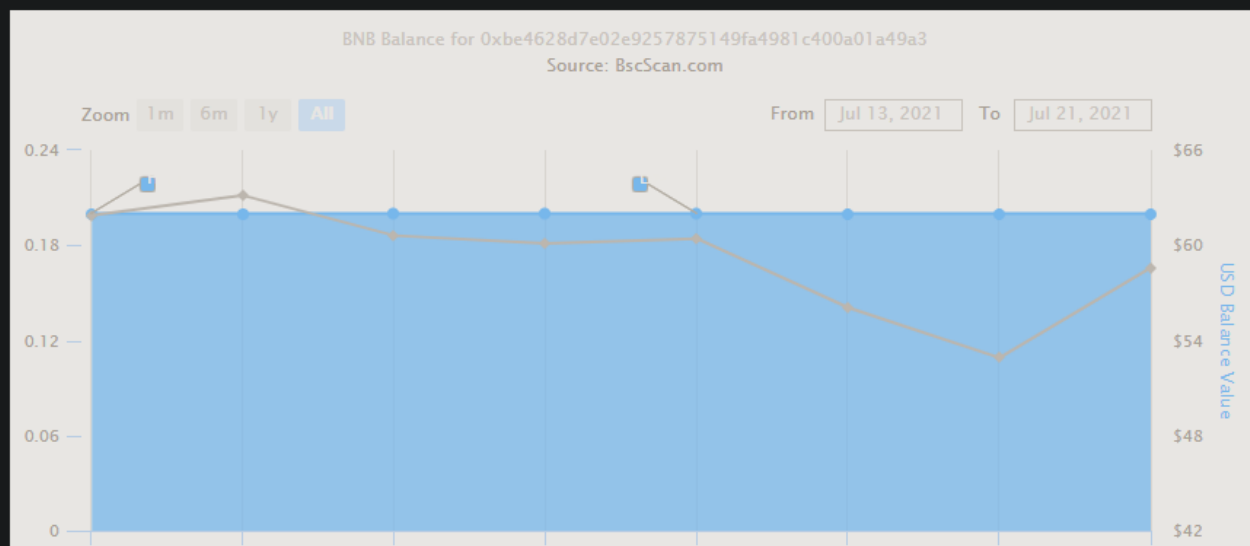
On Wed 14, Jul 2021

USD 63.14

■ **USD Lowest Value**

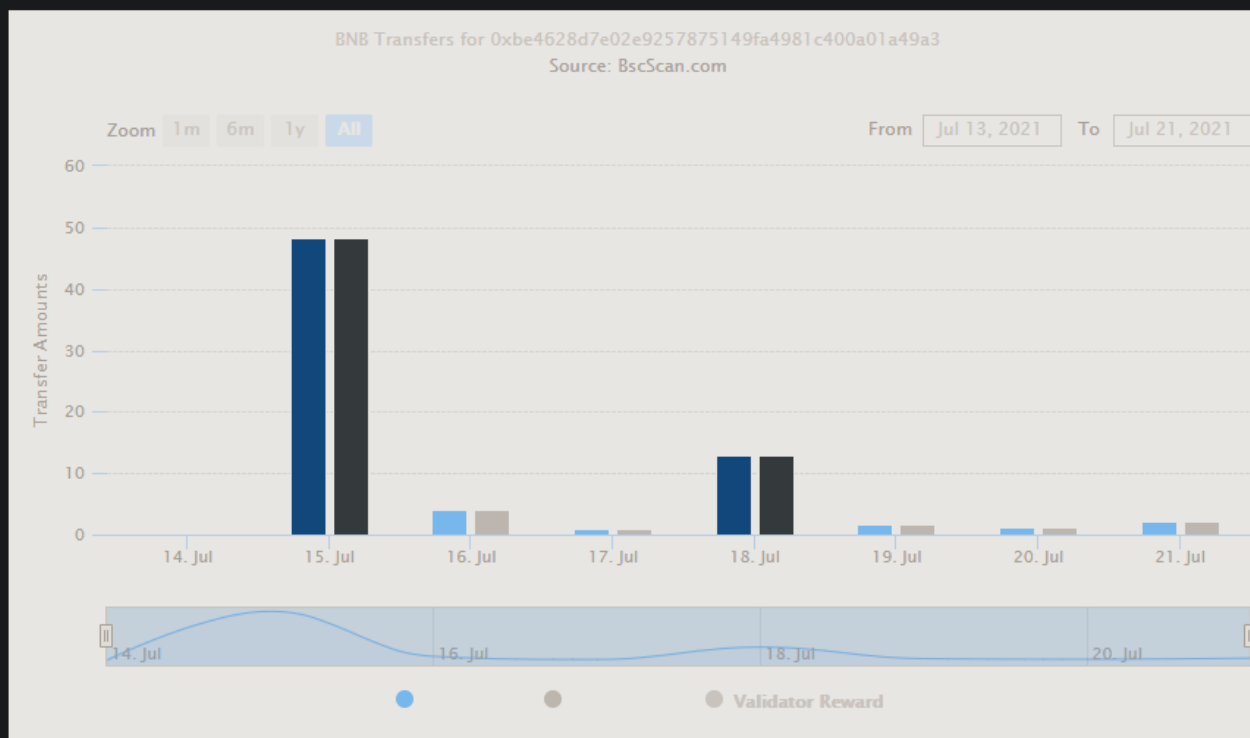
On Mon 19, Jul 2021

USD 52.91



Time Series: BNB Transfers

Tue 13, Jul 2021 - Tue 20, Jul 2021





Contract Functions

Public

View

```
owner()
geUnlockTime()
name()
symbol()
decimals()
totalSupply()
balanceOf(address account)
allowance(address owner, address spender)
isExcludedFromReward(address account)
totalFees()
reflectionFromToken(uint256 tAmount, bool deductTransferFee)
tokenFromReflection(uint256 rAmount)
isExcludedFromFee(address account)
```

Virtual

```
unlock()
increaseAllowance(address spender, uint256 addedValue)
decreaseAllowance(address spender, uint256 subtractedValue)
```

Executables

```
transfer(address recipient, uint256 amount)
approve(address spender, uint256 amount)
transferFrom(address sender, address recipient, uint256 amount)
deliver(uint256 tAmount)
```

Owner Executables

```
renounceOwnership()
transferOwnership(address newOwner)
lock(uint256 time)
excludeFromReward(address account)
includeInReward(address account)
excludeFromFee(address account)
includeInFee(address account)
setTaxFeePercent(uint256 taxFee)
setLiquidityFeePercent(uint256 liquidityFee)
setMaxTxPercent(uint256 maxTxPercent)
setSwapAndLiquifyEnabled(bool _enabled)
```




Checklist

Compiler errors.	Passed
Possible delays in data delivery.	Passed
Timestamp dependence.	Low Severity
Integer Overflow and Underflow.	Passed
DoS with Revert.	Passed
DoS with block gas limit.	Passed
Methods execution permissions.	Passed
Economy model of the contract.	Passed
Private user data leaks.	Passed
Malicious Event log.	Passed
Scoping and Declarations.	Passed
Uninitialized storage pointers.	Passed
Arithmetic accuracy.	Passed
Design Logic.	Passed
Cross-function race conditions.	Passed
Fallback function security.	Passed
Safe Open Zeppelin contracts implementation and usage.	Passed
Whitepaper-Website-Contract correlation.	Passed



Potential Issues

Zero Address Owner – Low severity issue

As of 07/23/2021 when the Audit took place the contract remains locked preventing from being able to view the owner address. This doesn't prove to be an issue

No logic issues found

The contract code was based on a currently existing and already running consolidated token (<https://daddydoge.finance/>). As the Smart Contract didn't suffer logical changes, just values, the execution of each function can be marked as thoroughly tested.



Owner privileges

- The owner can Exclude or Add an address from the rewards program.

```
function excludeFromReward(address account) public onlyOwner() {
    // require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, "
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

function includeInReward(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The owner can Exclude or Add an address from being taxed.

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```



- The owner can change the Tax percentages at any time.
- The owner can set the maximum amount of a transaction at any time.

```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}

function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}

function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner() {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(
        10**2
    );
}
```

- The owner can toggle the automatic liquidity swap at any time.

```
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
    swapAndLiquifyEnabled = _enabled;
    emit SwapAndLiquifyEnabledUpdated(_enabled);
}
```

- Additionally, the owner can execute the standard functions related to the Ownable Library.



Conclusions

The Smart Contract code passed the audit successfully on the Binance Mainnet.

There were only two warnings raised:

- At the time the Smart Contract was audited the owner address could not be visualized as it was under a lock. This means that currently the Zero Address is the owner of the contract so no OnlyOwner function can be performed. Once the timelock lifts up the actual owner address will be visible and the privileges will return to said address.

No changes need to be done to the Smart Contract as of 07/23/2021.