Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

HODL 2.0

Deployer address

0x728a0b0b113e915a64ddb2182F62F2661CC617B0

Client contacts:

HODL 2.0 team

Blockchain

Binance Smart Chain

Project website:

https://hodltoken.net/

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 below 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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.

Background

TechRate was commissioned by HODL 2.0 to perform an audit of smart contracts:
https://bscscan.com/address/0x5788105375ecf7f675c29e822fd85fcd84d4cd86#code

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.

Contracts Details

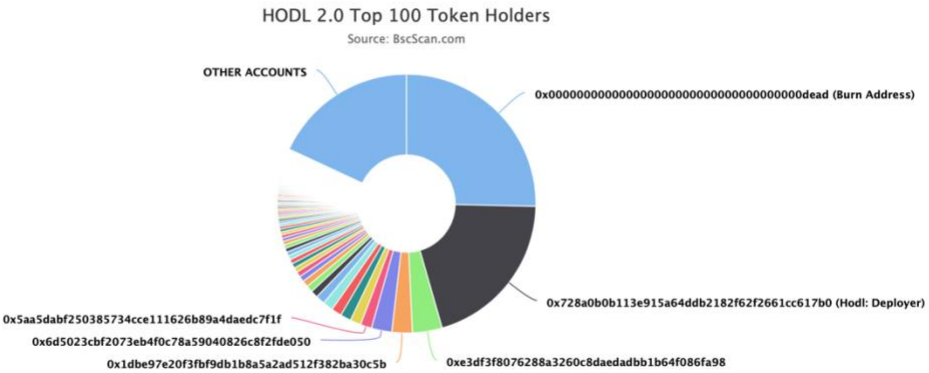
Token contract details for 07.08.2021

Contract name	HODL 2.0
Contract address	0x5788105375ecF7F675C29e822FD85fCd84d4cd86
Total supply	1,000,000,000,000,000
Token ticker	HODL
Decimals	9
Token holders	12,781
Transactions count	53,353
Top 100 holders dominance	81.92%
Total gasfee distributed	197268750000000000000
Total reinvested	1370982668447440134551
Total fees	1910816448527035117027
Pancake V2 pair	0x6d5023cbf2073eb4f0c78a59040826c8f2fde050
Contract deployer address	0x728a0b0b113e915a64ddb2182F62F2661CC617B0
Contract's current owner address	0x728a0b0b113e915a64ddb2182f62f2661cc617b0

HODL 2.0 Token Distribution

The top 100 holders collectively own 81.92% (819,198,910,121,063.00 Tokens) of HODL 2.0

Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 12,781

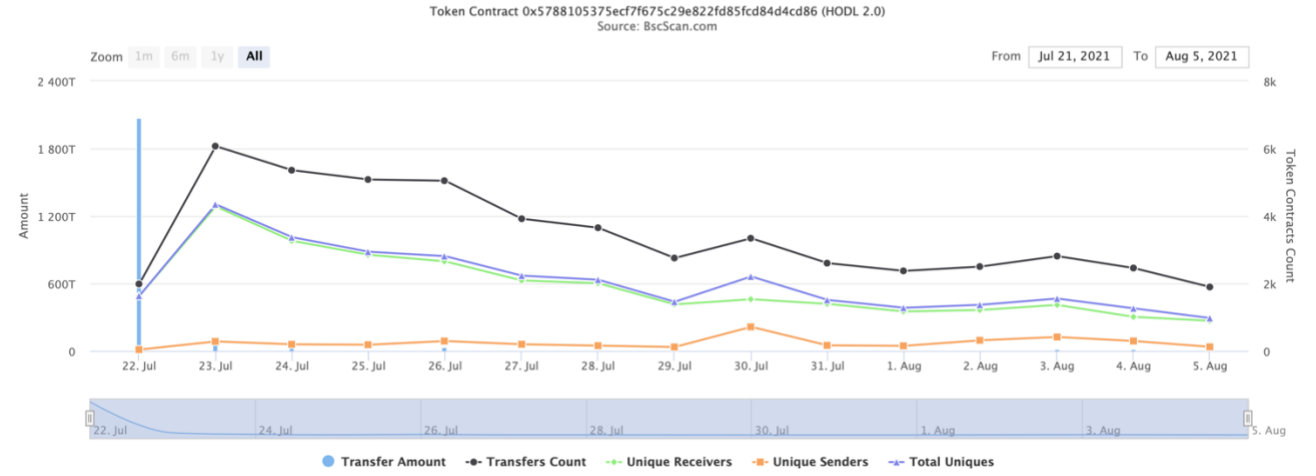


(A total of 819,198,910,121,063.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

HODL 2.0 Contract Interaction Details

Time Series: Token Contract Overview

Thu 22, Jul 2021 - Thu 5, Aug 2021



HODL 2.0 Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	253,486,155,587,114.841679436	25.3486%
2	Hodl: Deployer	202,098,319,160,577.187490633	20.2098%
3	0xe3df3f8076288a3260c8daedadbb1b64f086fa98	37,221,280,150,435.689797844	3.7221%
4	0x1dbe97e20f3fbf9db1b8a5a2ad512f382ba30c5b	25,553,807,772,713.674329328	2.5554%
5	0x6d5023cbf2073eb4f0c78a59040826c8f2fde050	25,490,032,681,810.140761512	2.5490%
6	0x5aa5dabf250385734cce111626b89a4daedc7f1f	13,976,601,119,707.630239606	1.3977%
7	0xf932f1e0f77303694d52eb2b8a34d12dfb6e78e7	13,615,641,889,861.941761982	1.3616%
8	0x5510c5c0b00e2b3119e5a553d891037bda6cd2c7	13,479,415,356,068.39539836	1.3479%
9	0xd425a54073513c7a5cdefc43ed11f0001cc08188	12,896,491,405,440.095251367	1.2896%
10	0x58b9c37b71994bb703ac8c109032add25e52adce	12,757,417,783,320.209272582	1.2757%

Contract functions details

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IWBNB
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] <Fallback> ($)
  - [Ext] deposit ($)
  - [Ext] withdraw #
  - [Ext] totalSupply
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #

    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

+ [Int] IPancakeFactory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Int] IPancakePair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IPancakeRouter01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #

  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IPancakeRouter02 (IPancakeRouter01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Lib] Utils
  - [Prv] random
  - [Pub] calculateBNBReward
  - [Pub] calculateTopUpClaim
  - [Pub] swapTokensForEth #
  - [Pub] swapETHForTokens #
  - [Pub] swapTokensForTokens #
  - [Pub] getAmountsout
  - [Pub] addLiquidity #

+ ReentrancyGuard
  - [Pub] <Constructor> #

+ HODLV2 (Context, IBEP20, Ownable, ReentrancyGuard)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcludedFromReward
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Prv] _transferBothExcluded #
  - [Pub] excludeFromFee #

  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Pub] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setExcludeFromMaxTx #
  - modifiers: onlyOwner
- [Pub] calculateBNBReward
- [Pub] getRewardCycleBlock
- [Pub] redeemRewards #
  - modifiers: isHuman,nonReentrant
- [Prv] topUpClaimCycleAfterTransfer #
- [Prv] ensureMaxTxAmount
- [Pub] disruptiveTransfer ($)
- [Prv] swapAndLiquify #
- [Pub] activateContract #
  - modifiers: onlyOwner
- [Pub] changerewardCycleBlock #
  - modifiers: onlyOwner
- [Pub] changereservewallet #
  - modifiers: onlyOwner
- [Pub] changemarketingwallet #
  - modifiers: onlyOwner
- [Pub] changeteamwallet #
  - modifiers: onlyOwner
- [Pub] changereinvestwallet #
  - modifiers: onlyOwner
- [Pub] reflectionfeestartstop #
  - modifiers: onlyOwner
- [Pub] migrateToken #

  - modifiers: onlyOwner
- [Pub] migrateWBnb #
  - modifiers: onlyOwner
- [Pub] migrateBnb #
  - modifiers: onlyOwner
- [Pub] changethreshHoldTopUpRate #
  - modifiers: onlyOwner
- [Pub] changeselltax #
  - modifiers: onlyOwner
- [Pub] changebnbclaimtax #
  - modifiers: onlyOwner
- [Pub] changereinvesttax #
  - modifiers: onlyOwner
- [Pub] changeclaimgasfee #
  - modifiers: onlyOwner
- [Pub] changeminTokenNumberToSell #
  - modifiers: onlyOwner
- [Pub] changeminTokenNumberUpperlimit #
  - modifiers: onlyOwner
- [Pub] changerewardHardcap #
  - modifiers: onlyOwner
- [Pub] changemarketingshare #
  - modifiers: onlyOwner
- [Pub] changebuybackshare #
  - modifiers: onlyOwner
- [Pub] changeteamshare #
  - modifiers: onlyOwner
- [Pub] changebuyBackUpperLimit #
  - modifiers: onlyOwner
- [Pub] changebuyBackthresholdLimit #
  - modifiers: onlyOwner
- [Pub] changemintoken #
  - modifiers: onlyOwner
- [Pub] changemaxtoken #
  - modifiers: onlyOwner
- [Pub] setBuyBackEnabled #
  - modifiers: onlyOwner

($) = payable function
= non-constant function

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.	Low issues
10.	Methods execution permissions.	Passed
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.	Low issues
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 found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
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 function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

2. Wrong reward transfer.

Issue:

- The function `redeemRewards()` uses _transferStandard(only reflection transfer) function to send expectedtoken amount to user. If this address or contract address would be excluded from reward, it will be a high issue.
- The function `migrateToken()` uses _transferStandard(only reflection transfer) function to send contract balance values to address from the argument. If this address or contract address would be excluded from reward, it will be a high issue.

Recommendation:
Add checking for exclusions and proper send methods.

Owner privileges (In the period when the owner is not renounced)

- Owner can change the tax and liquidity fee.
- Owner can change the maximum transaction amount.
- Owner exclude from and include in restricting max transaction amount.
- Owner can activate contract (enables below preset).
- Owner can change reward cycle block.
- Owner can enable and disable reflection fee.
- Owner can change thresh hold top up rate.
- Owner can exclude from the fee.
- Owner can change reserve, marketing, team and reinvest wallets.
- Owner can withdraw tokens and BNBs from the contract.
- Owner can change threshHoldTopUpRate.
- Owner can change sell tax.
- Owner can change BNB reward and reinvest taxes.
- Owner can change claimgas fee.
- Owner can change minTokenNumberToSell and minTokenNumberUpperlimit values.
- Owner can change marketing, team and buyback share.
- Owner can change buyback upper and threshold limit.
- Owner can change min and max token.
- Owner can disable buyback.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:
https://app.unicrypt.network/amm/pancake-v2/pair/0x6D5023CBF2073eb4f0C78A59040826c8F2FDe050

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.