Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

December, 2021

Audit Details

Audited project

Sharity

Deployer address

0xfefdf420adb69f86a396c1a5c35f2b0b2a07e6b3

Client contacts:

Sharity team

Blockchain

Ethereum

Project website:

https://sharitytoken.com/

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 Sharity to perform an audit of smart contracts:
https://etherscan.io/address/0x2df488b8a4270bac5c2ce5ff467a0c5fd2aa49d6#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

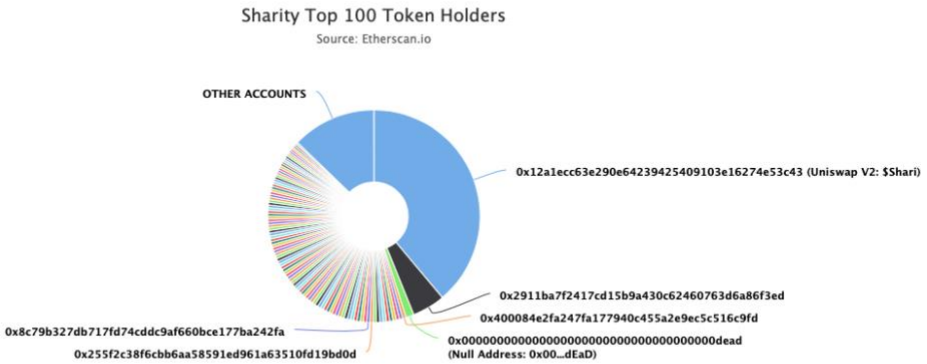
Token contract details for 24.12.2021

Contract name	Sharity
Contract address	0x2df488b8A4270bAc5C2cE5FF467A0C5fd2AA49d6
Total supply	50,000,000,000,000,000
Token ticker	$Shari
Decimals	9
Token holders	213
Transactions count	1,571
Top 100 holders dominance	87.20%
Current router	0x7a250d5630b4cf539739df2c5dacb4c659f2488d
buyFee/ sellFee/ transferFee	600 / 600 / 0
marketing/charity/dev/burn/ total ratios	3/1/1/1/5
lpPair	0x12a1ecc63e290e642394254091 03e16274e53c43
Contract deployer address	0xfefdf420adb69f86a396c1a5c35f2b0b2a07e6b3
Contract's current owner address	0xd84d657e4f5116c93df0a91614c60b1fff41dbc7

Sharity Token Distribution

The top 100 holders collectively own 87.20% (43,599,287,450,886,500.00 Tokens) of Sharity

Token Total Supply: 50,000,000,000,000,000.00 Token | Total Token Holders: 213

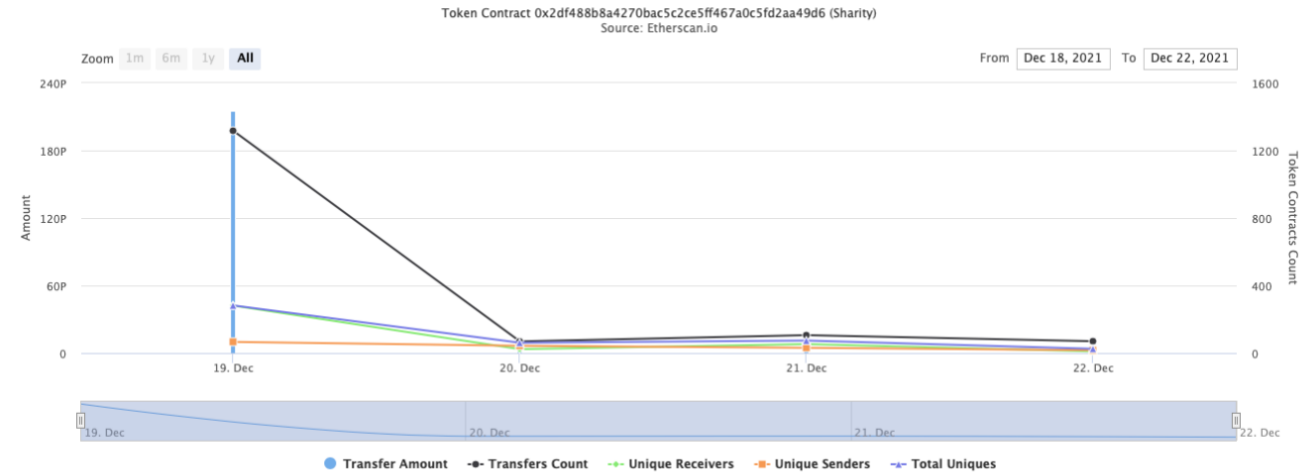


(A total of 43,599,287,450,886,500.00 tokens held by the top 100 accounts from the total supply of 50,000,000,000,000,000.00 token)

Sharity Contract Interaction Details

Time Series: Token Contract Overview

Sun 19, Dec 2021 - Wed 22, Dec 2021



Sharity Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Uniswap V2: $Shari	19,442,575,823,911,100.544668071	38.8852%
2	0x2911ba7f2417cd15b9a430c62460763d6a86f3ed	2,500,000,000,000,000	5.0000%
3	Null Address: 0x00...dEaD	625,693,062,074,812.719319393	1.2514%
4	0x400084e2fa247fa177940c455a2e9ec5c516c9fd	249,999,999,999,999.907391857	0.5000%
5	0x10a27adb2f4935f82ef252dc3072bf08aba0f06f	249,999,999,999,999.001787182	0.5000%
6	0x6e9f7445c18cb71718cff5ec9f5f3ef53c988dd1	249,999,999,999,999.000954333	0.5000%
7	0xb60b06bfbd120c76e4dc87b5ca4b2a060f5a229c	249,999,999,999,991.000438516	0.5000%
8	0x28fa5de8873c3af321af3bef2d30bd481cbfd9da	249,902,000,000,000.000784656	0.4998%
9	0xea4df31ab24048fd968925a77432c32002980fe2	249,866,258,729,918.190521568	0.4997%
10	0x38c650839866eab988d2648deb094c7214cf1b44	249,363,273,643,312.414770423	0.4987%

Contract functions details

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

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IFactoryV2
  - [Ext] getPair
  - [Ext] createPair #

+ [Int] IV2Pair
  - [Ext] factory
  - [Ext] getReserves

+ [Int] IRouter01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidityETH ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IRouter02 (IRouter01)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] AntiSnipe
  - [Ext] checkUser #
  - [Ext] setLaunch #
  - [Ext] setLpPair #
  - [Ext] setProtections #
  - [Ext] setGasPriceLimit #
  - [Ext] removeSniper #
  - [Ext] getSniperAmt
  - [Ext] removeBlacklisted #
  - [Ext] isBlacklisted
  - [Ext] transfer #
  - [Ext] setBlacklistEnabled #
  - [Ext] setBlacklistEnabledMultiple #
  - [Ext] getCooldownTime

- [Ext] setCooldownEnabled #
- [Ext] setCooldownTime #

+ Sharity (Context, IERC20)
- [Pub] <Constructor> ($)
- [Ext] <Fallback> ($)
- [Pub] owner
- [Ext] transferOwner #
  - modifiers: onlyOwner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] allowance
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] approve #
- [Prv] _approve #
- [Pub] approveContractContingency #
  - modifiers: onlyOwner
- [Ext] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] setNewRouter #
  - modifiers: onlyOwner
- [Ext] setLpPair #
  - modifiers: onlyOwner
- [Ext] changeRouterContingency #
  - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Pub] isExcludedFromFees
- [Pub] setExcludedFromFees #
  - modifiers: onlyOwner
- [Ext] setInitializer #
  - modifiers: onlyOwner
- [Ext] setBlacklistEnabled #
  - modifiers: onlyOwner
- [Ext] setBlacklistEnabledMultiple #
  - modifiers: onlyOwner
- [Ext] removeBlacklisted #
  - modifiers: onlyOwner
- [Pub] isBlacklisted
- [Pub] getSniperAmt
- [Ext] removeSniper #
  - modifiers: onlyOwner
- [Ext] setProtectionSettings #
  - modifiers: onlyOwner
- [Ext] setGasPriceLimit #
  - modifiers: onlyOwner
- [Pub] getCooldownTime
- [Ext] setCooldownEnabled #
  - modifiers: onlyOwner

- [Ext] setCooldownTime #
  - modifiers: onlyOwner
- [Ext] setTaxes #
  - modifiers: onlyOwner
- [Ext] setRatios #
  - modifiers: onlyOwner
- [Ext] setMaxWalletSize #
  - modifiers: onlyOwner
- [Pub] getMaxWallet
- [Ext] setSwapSettings #
  - modifiers: onlyOwner
- [Ext] setWallets #
  - modifiers: onlyOwner
- [Pub] setContractSwapEnabled #
  - modifiers: onlyOwner
- [Prv] _hasLimits
- [Int] _transfer #
- [Prv] contractSwap #
  - modifiers: lockTheSwap
- [Prv] _checkLiquidityAdd #
- [Pub] enableTrading #
  - modifiers: onlyOwner
- [Ext] sweepContingency #
  - modifiers: onlyOwner
- [Prv] _finalizeTransfer #
- [Int] _basicTransfer #
- [Int] takeTaxes #

($) = 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.	Passed
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. Non fixed solidity version

Issue:

- Solidity version is not fixed. Contract use operators, that works different way on different solidity versions.

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.6.0 <0.9.0;
```

Recommendation:
Fix solidity version to one or reduce versions range.

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

- Owner can transfer whole ownership.
- Owner can change Uniswap router address.
- Owner can include in LpPair array.
- Owner can exclude from the fee.
- Owner can change antisnipe address.
- Owner can enable/disable antisnipe blacklist.
- Owner can remove sniper addresses.
- Owner can change protection settings.
- Owner can change antisnipe gas limit.
- Owner can change antisnipe cooldown settings.
- Owner can change fees and ratios.
- Owner can change max wallet size.
- Owner can change swapThreshold and swapAmount.
- Owner can change marketing, charity and development address.
- Owner can enable/disable contractSwapEnabled.
- Owner can enable trading.
- Owner can withdraw contract ETHs.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. Contract contain interfaces that is not audited, some functions may work different ways.

Liquidity locking details provided by the team:
https://app.unicrypt.network/amm/uni-v2/pair/0x12a1ecc63e290e642394254091 03e16274e53c43

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.