TechRate
Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	Wall Street Decentral Token
Deployer address:	0x73fa3b86b27da17608cf79d325945c06657c6cce
Client contacts:	Wall Street Decentral Token team
Blockchain:	Ethereum
Project website:	http://WallStreetDecentral.com

April, 2021
TechRate

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 Wall Street Decentral to perform an audit of smart contracts:

- *https://etherscan.io/address/0x02b6361bbec213bcc34756bbd2877831d92a6c84#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.

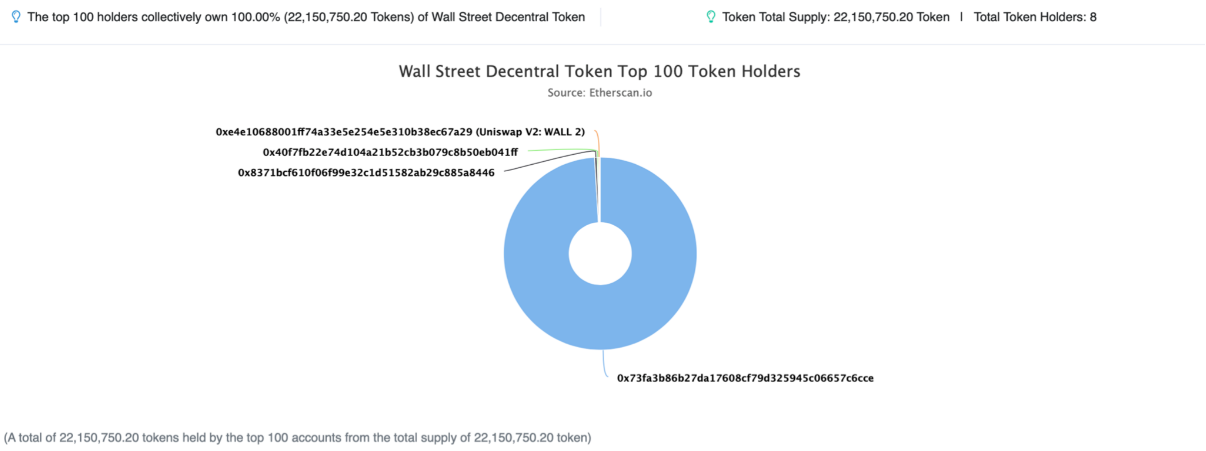
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 17.04.2021.

Contract name:	WALLToken
Contract address:	0x02b6361bbec213bcc34756bbd2877831d92a6c84
Total supply:	22_150_750_200_000_000_000_000_000
Token ticker:	WALL
Decimals:	18
Token holders:	8
Transactions count:	25
Top 100 holders dominance:	100 %
Contract deployer address:	0x73fa3b86b27da17608cf79d325945c06657c6cce
Contract’s current owner address:	0x73fa3b86b27da17608cf79d325945c06657c6cce
Main cap:	50_000_000_000_000_000_000_000_000
Available to mint:	3_261_182_582_800_000_000_000_000_000
Token tradable:	True
Migration phase open:	False
Tokens per eth:	45682
Whitelisted number:	5
Main end date:	1620464400
Max total supply:	3_333_333_333_000_000_000_000_000_000

WALLToken token distribution



The top 100 holders collectively own 100.00% (22,150,750.20 Tokens) of Wall Street Decentral Token

Token Total Supply: 22,150,750.20 Token | Total Token Holders: 8

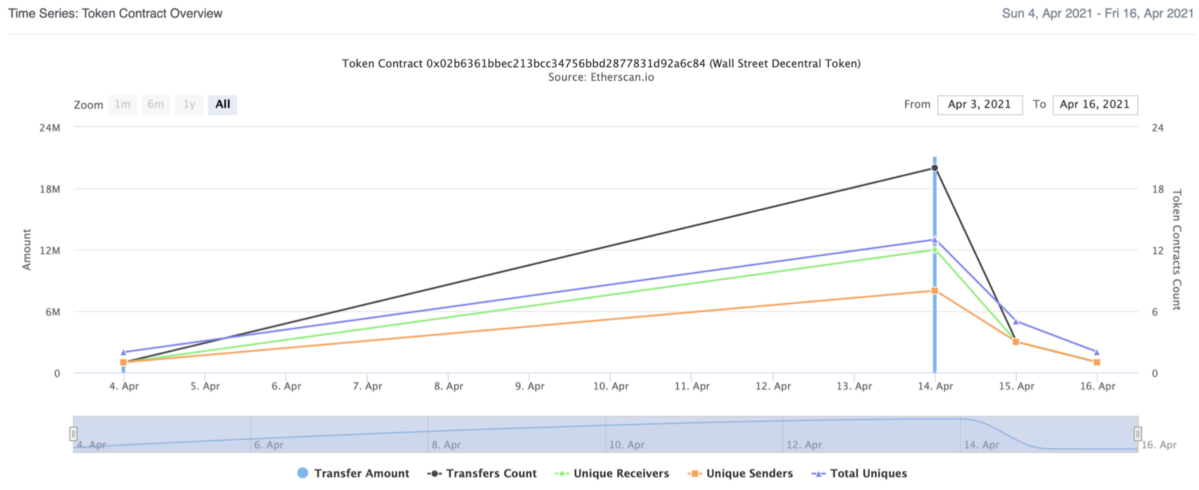
Wall Street Decentral Token Top 100 Token Holders

Source: Etherscan.io

0xe4e10688001ff74a33e5e254e5e310b38ec67a29 (Uniswap V2: WALL 2)
0x40f7fb22e74d104a21b52cb3b079c8b50eb041ff
0x8371bcf610f06f99e32c1d51582ab29c885a8446
0x73fa3b86b27da17608cf79d325945c06657c6cce

(A total of 22,150,750.20 tokens held by the top 100 accounts from the total supply of 22,150,750.20 token)

WALLToken contract interaction details



Time Series: Token Contract Overview

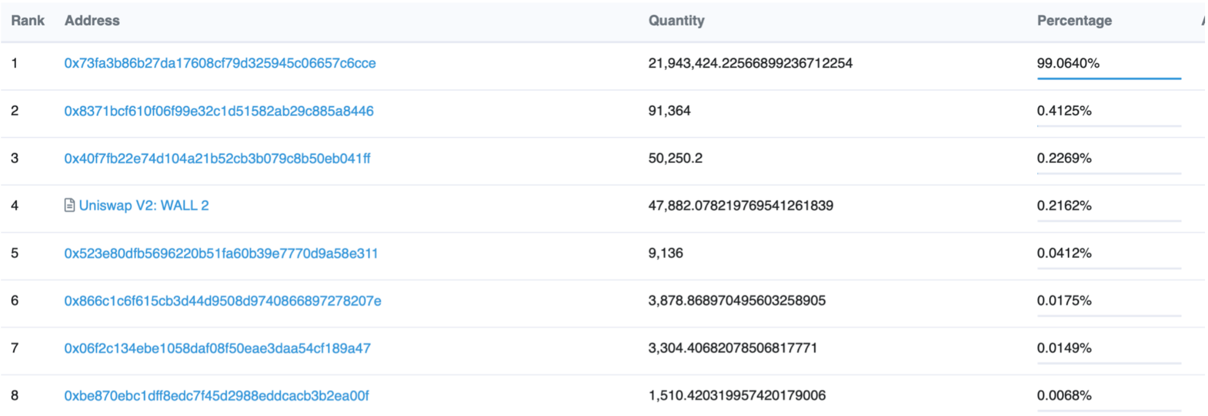
Sun 4, Apr 2021 - Fri 16, Apr 2021

Token Contract 0x02b6361bbec213bcc34756bbd2877831d92a6c84 (Wall Street Decentral Token)

Source: Etherscan.io

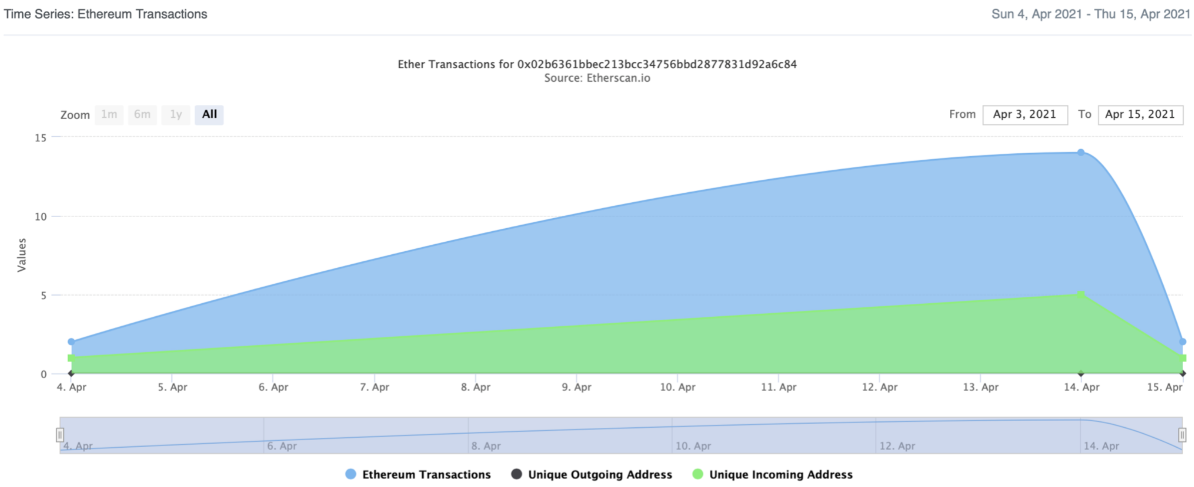
From Apr 3, 2021 To Apr 16, 2021

WALLToken top 8 token holders



Rank	Address	Quantity	Percentage
1	0x73fa3b86b27da17608cf79d325945c06657c6cce	21,943,424.22566899236712254	99.0640%
2	0x8371bcf610f06f99e32c1d51582ab29c885a8446	91,364	0.4125%
3	0x40f7fb22e74d104a21b52cb3b079c8b50eb041ff	50,250.2	0.2269%
4	Uniswap V2: WALL 2	47,882.078219769541261839	0.2162%
5	0x523e80dfb5696220b51fa60b39e7770d9a58e311	9,136	0.0412%
6	0x866c1c6f615cb3d44d9508d9740866897278207e	3,878.868970495603258905	0.0175%
7	0x06f2c134ebe1058daf08f50eae3daa54cf189a47	3,304.40682078506817771	0.0149%
8	0xbe870ebc1dff8edc7f45d2988eddcacb3b2ea00f	1,510.420319957420179006	0.0068%

WALLToken transactions



Time Series: Ethereum Transactions

Sun 4, Apr 2021 - Thu 15, Apr 2021

Ether Transactions for 0x02b6361bbec213bcc34756bbd2877831d92a6c84
Source: Etherscan.io

Zoom 1m 6m 1y All

From Apr 3, 2021 To Apr 15, 2021

Contract functions details

```
+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] mul

+  Owned
  - [Pub] <Constructor> #
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] acceptOwnership #
  - [Pub] addAdmin #
    - modifiers: onlyOwner
  - [Pub] removeAdmin #
    - modifiers: onlyOwner

+  Wallet (Owned)
  - [Pub] <Constructor> #
  - [Pub] setWallet #
    - modifiers: onlyOwner

+  ERC20Interface
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] transferFrom #
  - [Pub] approve #
  - [Pub] allowance

+  ERC20Token (ERC20Interface, Owned)
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] allowance

+  LockSlots (ERC20Token)
  - [Int] registerLockedTokens #
  - [Pub] lockedTokens
  - [Pub] unlockedTokens
  - [Pub] isAvailableLockSlot
  - [Int] unlockedTokensInternal #
  - [Prv] pNumberOfLockedTokens
```

```
+  WALLIcoDates (Owned)
   - [Pub] <Constructor> #
      - modifiers: checkDateOrder
   - [Pub] setDateMainStart #
      - modifiers: onlyOwner,checkDateOrder
   - [Pub] setDateMainEnd #
      - modifiers: onlyOwner,checkDateOrder
   - [Pub] isMainFirstDay
   - [Pub] isMain

+  WALLToken (ERC20Token, Wallet, LockSlots, WALLIcoDates)
   - [Pub] <Constructor> #
   - [Pub] <Fallback> ($)
   - [Pub] availableToMint
   - [Pub] firstDayTokenLimit
   - [Pub] ethToTokens
   - [Pub] tokensToEth
   - [Pub] addToWhitelist #
      - modifiers: onlyAdmin
   - [Pub] addToWhitelistMultiple #
      - modifiers: onlyAdmin
   - [Int] pWhitelist #
   - [Pub] updateTokensPerEth #
      - modifiers: onlyOwner
   - [Pub] makeTradeable #
   - [Pub] openMigrationPhase #
      - modifiers: onlyOwner
   - [Pub] mintTokens #
      - modifiers: onlyOwner
   - [Pub] mintTokensMultiple #
      - modifiers: onlyOwner
   - [Pub] mintTokensLocked #
      - modifiers: onlyOwner
   - [Pub] mintTokensLockedMultiple #
      - modifiers: onlyOwner
   - [Prv] pMintTokens #
   - [Prv] buyTokens #
   - [Pub] requestTokenExchangeMax #
   - [Pub] requestTokenExchange #
   - [Pub] transferAnyERC20Token #
      - modifiers: onlyOwner
   - [Pub] transfer #
   - [Pub] transferFrom #
   - [Ext] transferMultiple #

($) = 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.	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 found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

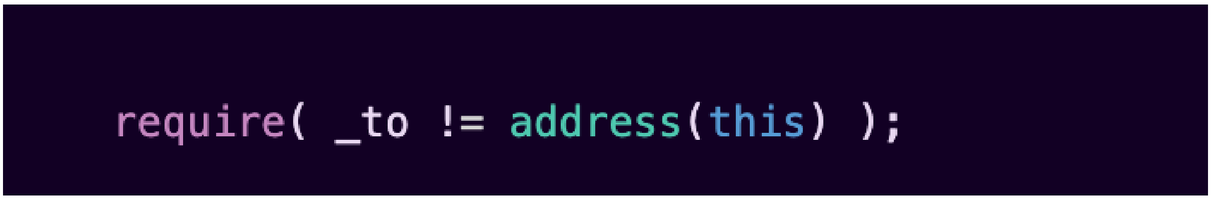
1. Known vulnerabilities of ERC-20 token

Issue:

Lack of transaction handling mechanism issue. WARNING! This is a very common issue and it already caused millions of dollars losses for lots of token users! More details here.

Recommendation:

Add the following code to the transfer(address _to, ...) and transferFrom(address _from, address _to, ...) functions:



```
require( _to != address(this) );
```

2. Wallet address

Issue:

Wallet address, which could be changed by the owner, after receiving the tokens can buy tokens from the contract in cycle, because he will receive ethers back after each buy.

Recommendation:

It could be better to transfer the funds to the wallet address only after the sale ends.

Owner privileges

- ❏ Owner can add admins.
- ❏ Owner can change the wallet address.
- ❏ Owner can change the start and end dates of the sale.
- ❏ Owner can add to the whitelist.

- Owner can change the tokens per eth rate.
- Owner can mint tokens until the max total supply is not reached.

Conclusion

Smart contracts do not contain high severity issues.

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.