HackSafe

Smart Contract Security Audit Report

Trust Wallet

May **2022**

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Trust Wallet

Deployer address
0xb2Df0829ff3E1F0D9ecfB2B4784c00BB09f3D1cd

Client contacts
Trust Wallet

Blockchain
Binance smart chain

Website
https://trustwallet.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) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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

HackSafe was commissioned by Trust Wallet to perform an audit of smart contracts:

- https://bscscan.com/address/0x4b0f1812e5df2a09796481ff14017e6005508003#code

Contract Details

Token contract details for 20.05.2022

Contract name	: TrustWalletToken
Contract address	: 0x4B0F1812e5Df2A09796481Ff14017e6005508003
Total supply	: 999,999,999.999999
Token Ticker	: TWT
Decimals	: 18
Token Holders	: 274,785 address
Transactions count	: 3,014,999
Contract deployer address	: 0xb2Df0829ff3E1F0D9ecfB2B4784c00BB09f3D1cd
owner address	: 0xb2Df0829ff3E1F0D9ecfB2B4784c00BB09f3D1cd

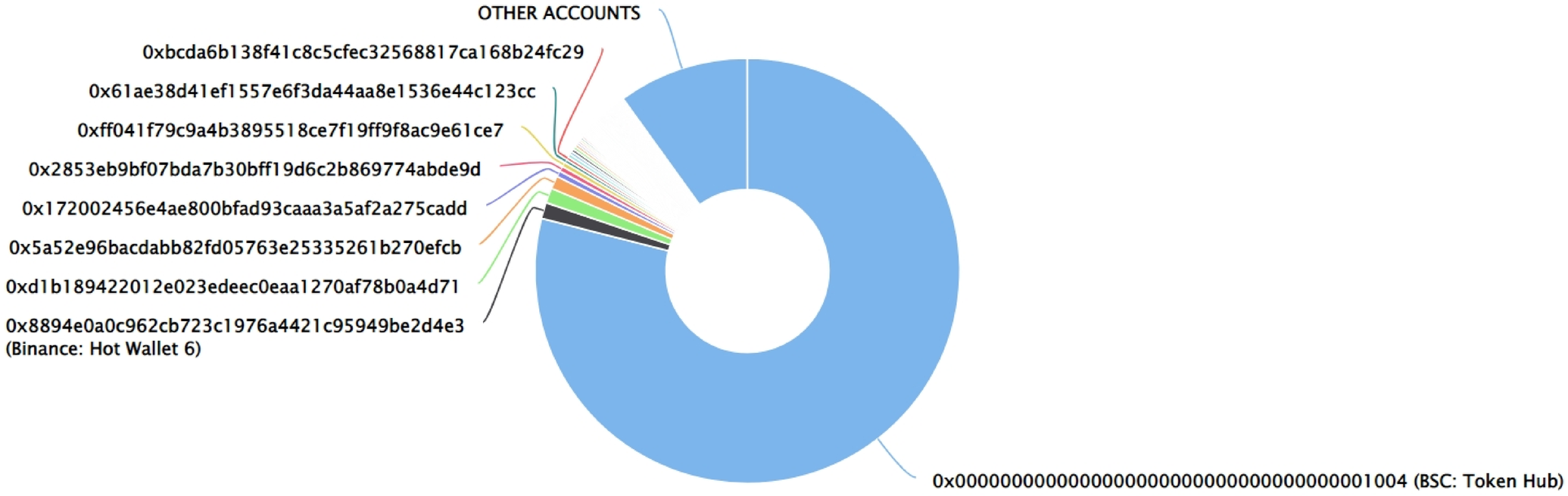
Trust Wallet Token Distribution

The top 100 holders collectively own 90.05% (900,472,914.74 Tokens) of Trust Wallet

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 274,790

Trust Wallet Top 100 Token Holders

Source: BscScan.com



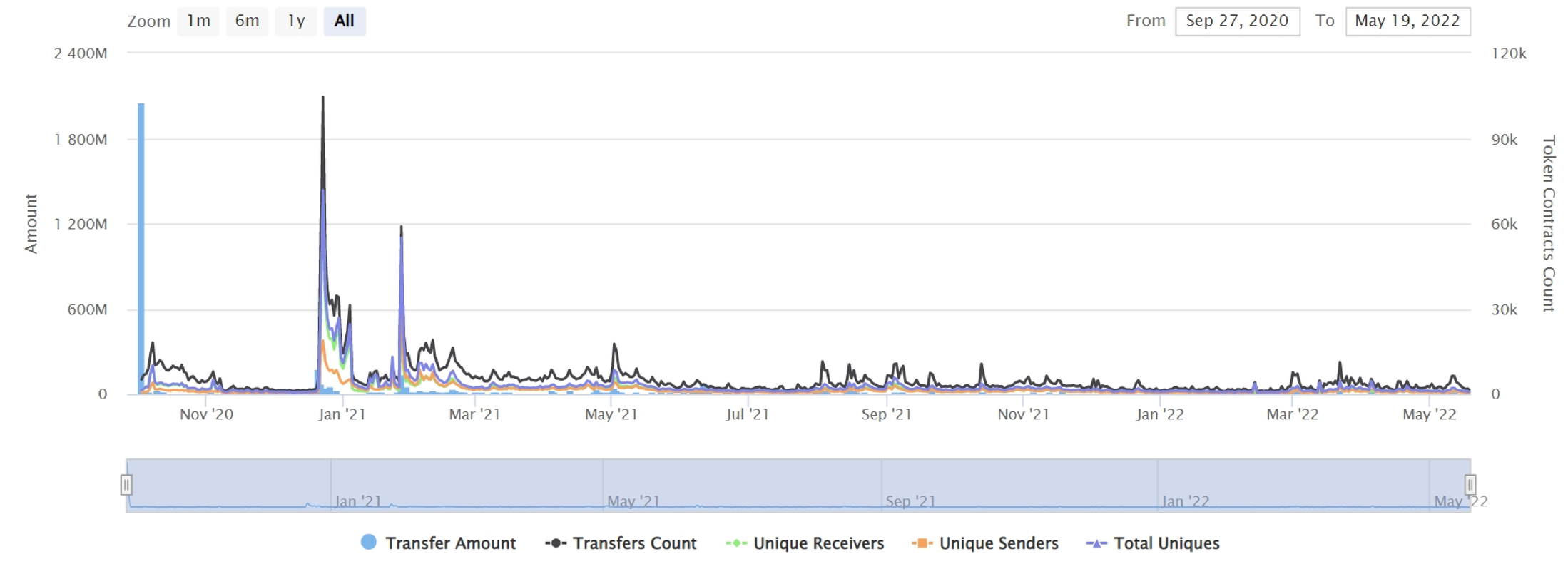
Trust Wallet Top 20 Token Holders

(A total of 900,472,914.74 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	BSC: Token Hub	789,808,119.69056916	78.9808%
2	Binance: Hot Wallet 6	12,283,442.739075067188007994	1.2283%
3	0xd1b189422012e023edeec0eaa1270af78b0a4d71	11,410,000	1.1410%
4	0x5a52e96bacdabb82fd05763e25335261b270efcb	10,000,000	1.0000%
5	0x172002456e4ae800bfad93caaa3a5af2a275cadd	4,434,999.98102	0.4435%
6	0x2853eb9bf07bda7b30bff19d6c2b869774abde9d	3,957,557.435813471812038461	0.3958%
7	0xff041f79c9a4b3895518ce7f19ff9f8ac9e61ce7	3,428,454.4	0.3428%
8	0x61ae38d41ef1557e6f3da44aa8e1536e44c123cc	2,579,910	0.2580%
9	0xbcda6b138f41c8c5cfec32568817ca168b24fc29	2,480,700	0.2481%
10	0x955dac9dd949ea7ba492373d5fe8a70558b43195	2,401,623	0.2402%
11	0x36d25bbdf3b46c1b03c2243a84d5f254f1898d02	2,320,326.72644212	0.2320%
12	0xe55c337b56f83af6735a0a481c58d6b0d009758a	2,254,384.5554521	0.2254%
13	0x829eab27aa0101e2b58a66b36f8afb08abf9878c	2,202,794.52863	0.2203%
14	0xf53109bb46b37d030b8cd7dbb09972d078553647	1,965,977.47209	0.1966%
15	0x95909361ad5c56312c94aa213b1b858ad2f1b8bf	1,801,038.02377391	0.1801%
16	Gate.io	1,644,509.999380071524324648	0.1645%
17	0x457294278eada6a037314c6df9e214c9fdd7de99	1,567,000.868830491616184151	0.1567%
18	0x6082dae7ec7450cdb0801ff565b17fa1449010ff	1,562,711.332	0.1563%
19	0xd6216fc19db775df9774a6e33526131da7d19a2c	1,411,778.039602916767732597	0.1412%
20	0x52db9a93aaf32c0f4cfea8d3bad4b1d148981f70	1,369,642.000709011174360718	0.1370%

Trust Wallet Token Distribution

Trust Wallet Contract overview



Contract functions details

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

+ [Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

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

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

+ ERC20 (Context, IERC20, IERC20Metadata)
    - [Pub] <constructor> #
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf

Contract functions details

- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
  -[Pub] increaseAllowance#
  -[Pub] decreaseAllowance#
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _setupDecimals#
  -[Int] _beforeTokenTransfer

+ ERC20Burnable (Context, ERC20)
  -[Pub] burn #
  -[Pub] burnFrom #

+ [Lib] SafeERC20
  -[Int] safeTransfer #
  -[Int] safeTransferFrom #
  -[Int] safeApprove #
  -[Int] safeIncreaseAllowance #
  -[Int] safeDecreaseAllowance #
  -[Pvt] _callOptionalReturn

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

+ [Lib] Math
  -[Int] max
  -[Int] min
  -[Int] average

Contract functions details

+ TrustWalletToken (ERC20, ERC20Burnable, Ownable)
    -[Pub] <constructor> #
    -[Pub] getOwner

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	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.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Low issue
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues

No critical severity issue found.

High Severity Issues

No high severity issue found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

Three low severity issues found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.6.12 the contract should contain the following line:

  pragma solidity 0.6.12;

2. Scoping and Declarations.

Return same value.

- **Description**

  The getOwner and owner functions return the same address.

- **Location:**

  getOwner and owner functions.

- **Recommendation:**

  We advise to remove any one of the mentioned function which can help you to develop clean coding style and save some computational gas too.

3. Scoping and Declarations.

Unused function.

- **Description**

  The sendValue, functionCall, functionCallWithValue, _functionCallWithValue do nothing In the contract.

- **Location:**

  sendValue, functionCall, functionCallWithValue, _functionCallWithValue functions.

- **Recommendation:**

  We advise to remove the mentioned function which can help you to develop clean coding style and save some computational gas too.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- Trust Wallet Contract:
    - Owner can renounce ownership.
    - Owner can transfer ownership.

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe 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.