TechRate

AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project

BASE REWARD

Deployer address

0xd7655a7584910be99dc20a8b2975591e9fdc0d90

Client contacts:

BASE REWARD team

Blockchain

Binance Smart Chain

Project website:

https://basereward.online/

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 BASE REWARD to perform an audit of smart contracts:

- https://bscscan.com/address/0x0d499b25bce7aa72bb6c50e434e2ed26fe1e785d#code
- https://bscscan.com/address/0x5b8a03DcaE042A2bC37262db8648EB5432076333#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 06.09.2021

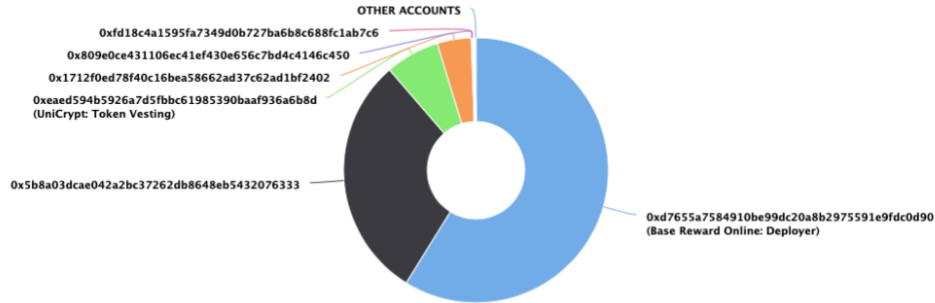|	
Contract name	BASE REWARD
Contract address	0x0d499B25Bce7Aa72bb6c50E434E2Ed26fE1e785D 0x5b8a03DcaE042A2bC37262db8648EB5432076333
Total supply	12,000,000
Token ticker	BRT
Decimals	18
Token holders	767
Transactions count	14,163
Top 100 holders dominance	99.90%
Compound fee	10000000000000000000
Harvest fee	10000000000000000000
Stake fee	3500000000000000
Unstake fee	10000000000000000000
Contract deployer address	0xd7655a7584910be99dc20a8b2975591e9fdc0d90
Contract's current owner address	0x000000000000000000000000000000000000dead

BASE REWARD Token Distribution

BASE REWARD TOKEN Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS
0xfd18c4a1595fa7349d0b727ba6b8c688fc1ab7c6
0x809e0ce431106ec41ef430e656c7bd4c4146c450
0x1712f0ed78f40c16bea58662ad37c62ad1bf2402
0xeaed594b5926a7d5fbbc61985390baaf936a6b8d
(UniCrypt: Token Vesting)
0x5b8a03dcae042a2bc37262db8648eb5432076333
0xd7655a7584910be99dc20a8b2975591e9fdc0d90
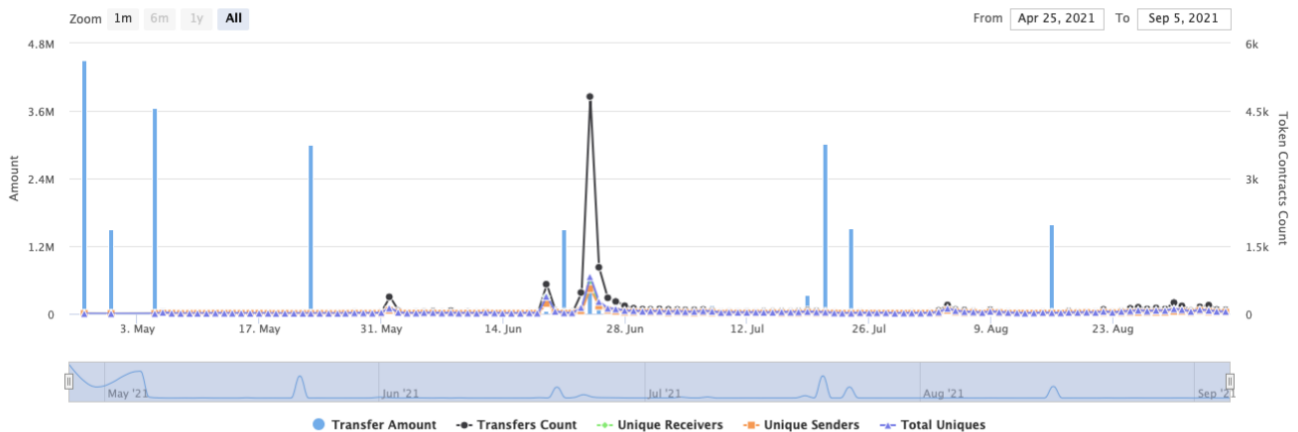(Base Reward Online: Deployer)

(A total of 11,988,475.13 tokens held by the top 100 accounts from the total supply of 12,000,000.00 token)

BASE REWARD Contract Interaction Details

Time Series: Token Contract Overview   Tue 27, Apr 2021 - Sun 5, Sept 2021

Token Contract 0x0d499b25bce7aa72bb6c50e434e2ed26fe1e785d (BASE REWARD TOKEN)
Source: BscScan.com

Zoom 1m 6m 1y All   From Apr 25, 2021 To Sep 5, 2021

● Transfer Amount -●- Transfers Count -+- Unique Receivers -■- Unique Senders -▲- Total Uniques

BASE REWARD Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Base Reward Online: Deployer	7,063,041.978400857304453456	58.8587%
2	0x5b8a03dcae042a2bc37262db8648eb5432076333	3,578,323.18568492115572149	29.8194%
3	UniCrypt: Token Vesting	792,000	6.6000%
4	0x1712f0ed78f40c16bea58662ad37c62ad1bf2402	500,000	4.1667%
5	0x809e0ce431106ec41ef430e656c7bd4c4146c450	8,000	0.0667%
6	0xfd18c4a1595fa7349d0b727ba6b8c688fc1ab7c6	7,282	0.0607%
7	0xce4e19ce89d293ba159895bba66f888844f5839f	3,500	0.0292%
8	PancakeSwap V2: BRT 20	3,437.868776687218015675	0.0286%
9	0xaa3d85ad9d128dfecb55424085754f6dfa643eb1	2,781.736076266934269944	0.0232%
10	0x221ea84a91acb81acff5cb9e0ce3ba2f822bc44c	2,044.296372095656994375	0.0170%

BaseRewardToken Contract functions details

+ **Context**
  - [Int] _msgSender
  - [Int] _msgData
+ **Ownable** (Context)
  - [Int] **<Constructor>** #
  - **[Pub]** owner
  - **[Pub]** renounceOwnership #
    - modifiers: onlyOwner
  - **[Pub]** transferOwnership #
    - modifiers: onlyOwner
+ **[Lib]** Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - **[Prv]** _functionCallWithValue #
+ **[Lib]** SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod
+ **[Int]** IBEP20
  - **[Ext]** totalSupply
  - **[Ext]** balanceOf
  - **[Ext]** transfer #
  - **[Ext]** allowance
  - **[Ext]** approve #
  - **[Ext]** transferFrom #
+ **BEP20** (Context, IBEP20)
  - **[Pub]** **<Constructor>** #
  - **[Pub]** name
  - **[Pub]** symbol
  - **[Pub]** decimals
  - **[Pub]** totalSupply
  - **[Pub]** balanceOf
  - **[Pub]** transfer #
  - **[Pub]** allowance
  - **[Pub]** approve #
  - **[Pub]** bansferFrom #
  - **[Pub]** increaseAllowance #
  - **[Pub]** decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #

- [Int] _burn #
  - [Int] _approve #
  - [Int] _setupDecimals #
  - [Int] _beforeTokenTransfer #
+ BEP20Capped (BEP20)
  - [Pub] <Constructor> #
  - [Pub] cap
  - [Int] _beforeTokenTransfer #
+ BaseRewardToken (BEP20Capped, Ownable)
  - [Pub] <Constructor> #
    - modifiers: BEP20,BEP20Capped
  - [Ext] <Fallback> ($)
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Pub] burn #
    - modifiers: onlyOwner
($) = payable function
= non-constant function

BRTStaking Contract functions details

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

+ Context
  - [Int] <Constructor> #
  - [Int] _msgSender
  - [Int] _msgData

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

+ ReentrancyGuard
- [Int] <Constructor> #

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

+ [Int] IBEP20
- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] SafeBEP20
- [Int] safeTransfer #
- [Int] safeTransferFrom #
- [Int] safeApprove #
- [Int] safeIncreaseAllowance #
- [Int] safeDecreaseAllowance #
- [Prv] _callOptionalReturn #

+ BRTStaking (Ownable)
- [Pub] <Constructor> #
- [Ext] <Fallback> ($)
- [Pub] balanceOf
- [Pub] getRewardTokensPerSec
- [Pub] calculateReward
- [Pub] stake ($)
- [Pub] unstake ($)
- [Pub] harvest ($)
- [Pub] compound ($)
- [Int] calculateTime
- [Int] _updateUserInfo #
- [Int] handleFee #
- [Int] _stake #
- [Ext] executeHalving #
  - modifiers: onlyOwner
- [Ext] setStakeFee #
  - modifiers: onlyOwner
- [Ext] setUnStakeFee #
  - modifiers: onlyOwner
- [Ext] setHarvestFee #
  - modifiers: onlyOwner
- [Ext] setCompoundFee #

- modifiers: onlyOwner
- **[Ext]** setDev **#**
  - modifiers: onlyOwner
- **[Ext]** setOwnerSharePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setDevSharePercent **#**
  - 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.	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. Reentrancy

Issue:

- **BRTStaking contract has ReentrancyGuard library but does not use it.**

Recommendation:
Use nonReentrant modifier to prevent reentrancy attacks.

2. Abuse of authority (Not an issue while owner is renounced)

Issue:

- **The function burn() can be called only by the owner of the BaseRewardToken contract. Owner can burn any amount of tokens from any address without any approve.**

Recommendation:
Do not let anybody access users' balances.

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

- **BRTStaking:**

    - **Owner can change stake, unStake, harvest and compound fee.**
    - **Owner can execute halving.**
    - **Owner can change dev address.**
    - **Owner can change owner and dev share percents.**

- **BaseRewardToken:**

    - **Owner can mint under capitalization.**
    - **Owner can burn.**

Conclusion

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

Liquidity locking details are provided by the team:

Team locked token:
- https://app.unicrypt.network/amm/pancake-v2/token/0x0d499b25bce7aa72bb6c50e434e2ed26fe1e785d

Burned liquidity:
- https://bscscan.com/token/0x0d499b25bce7aa72bb6c50e434e2ed26fe1e785d

---

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.