Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

BrandPad

Deployer address

0x3d07f0bb9bfc314d412044dcad441347b1c294c1

Client contacts:

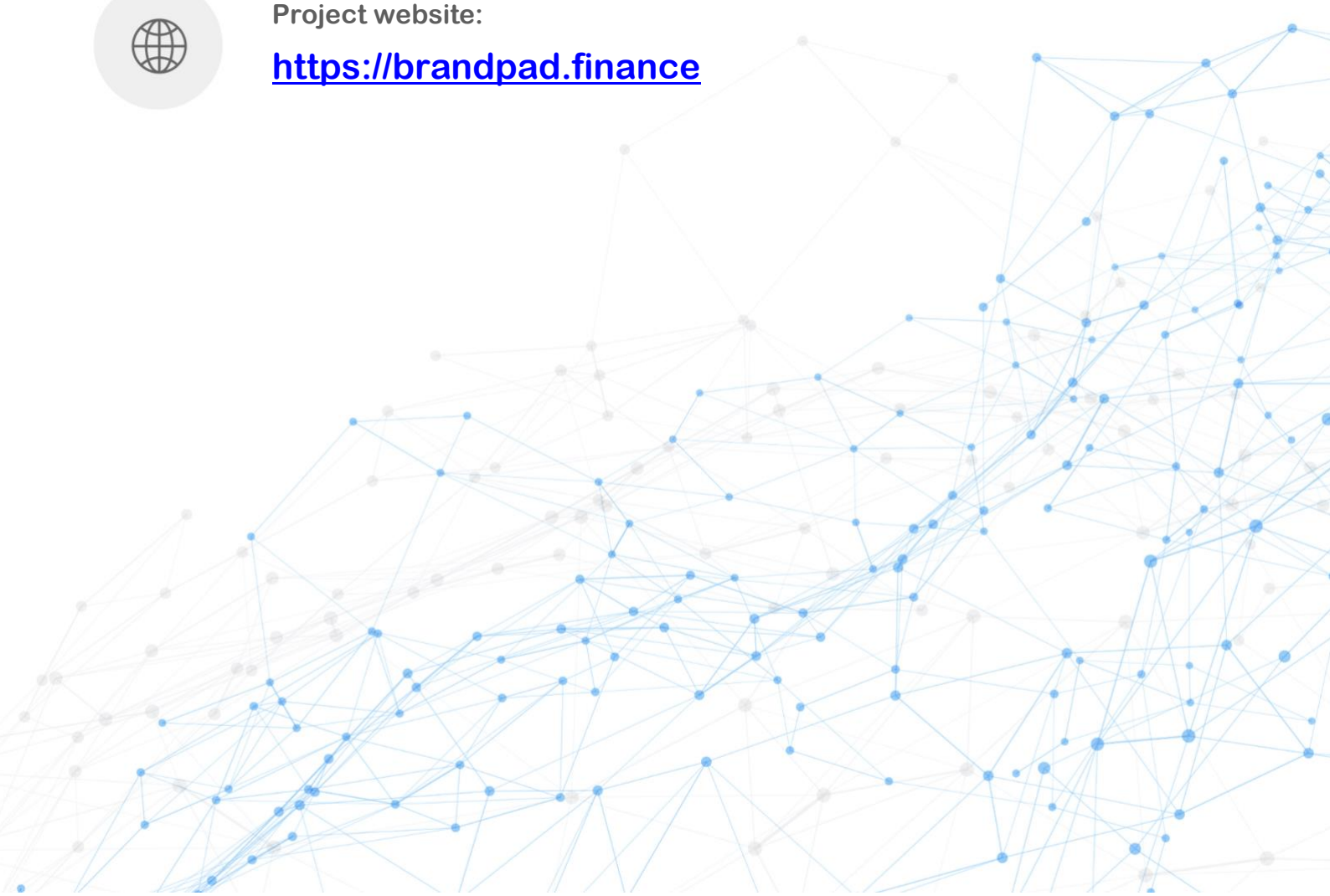
BrandPad team

Blockchain

Binance Smart Chain

Project website:

https://brandpad.finance



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 BrandPad to perform an audit of smart contracts:

https://bscscan.com/address/0x4d993ec7b44276615bb2f6f20361ab34fbf0ec49#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

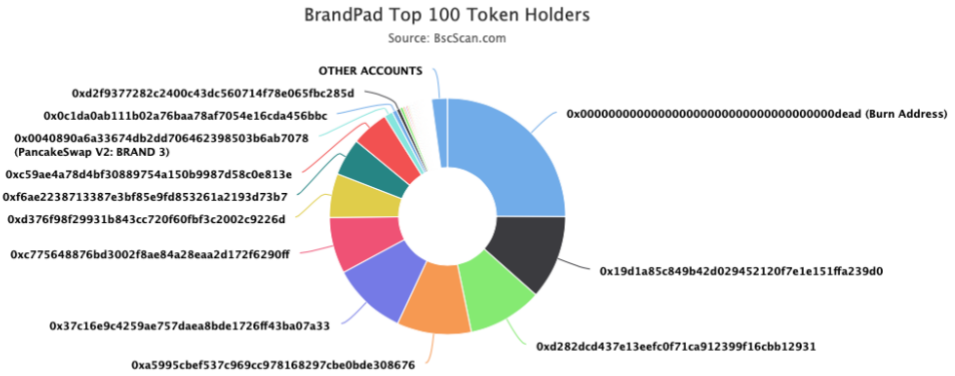
Token contract details for 22.08.2021

Contract name	BrandPad
Contract address	0x4d993ec7b44276615bB2F6F20361AB34FbF0ec49
Total supply	188,100,000
Token ticker	BRAND
Decimals	9
Token holders	2,413
Transactions count	13,711
Top 100 holders dominance	97.83%
Tax fee	3
Total fees	3762107474619976
Contract deployer address	0x3d07f0bb9bfc314d412044dcad441347b1c294c1
Contract's current owner address	0x3d07f0bb9bfc314d412044dcad441347b1c294c1

BrandPad Token Distribution

The top 100 holders collectively own 97.83% (184,020,328.87 Tokens) of BrandPad

Token Total Supply: 188,100,000.00 Token | Total Token Holders: 2,413

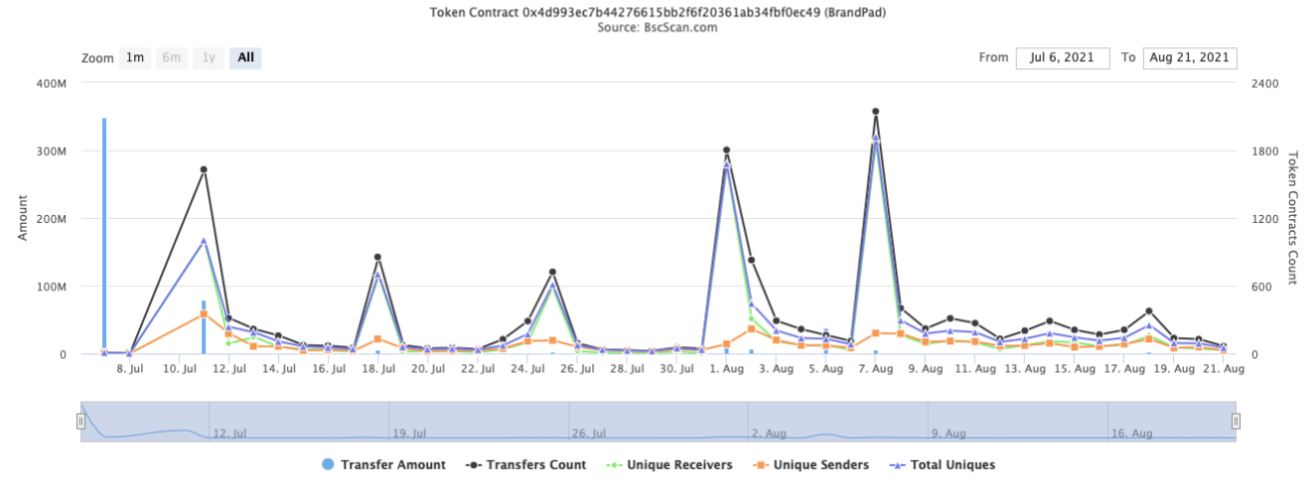


(A total of 184,020,328.87 tokens held by the top 100 accounts from the total supply of 188,100,000.00 token)

BrandPad Contract Interaction Details

Time Series: Token Contract Overview

Wed 7, Jul 2021 - Sat 21, Aug 2021



BrandPad Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	47,119,023.816750884	25.0500%
2	0x19d1a85c849b42d029452120f7e1e151ffa239d0	21,650,721.574264261	11.5102%
3	0xd282dcd437e13eefc0f71ca912399f16cbb12931	19,189,918.306119497	10.2020%
4	0xa5995cbef537c969cc978168297cbe0bde308676	19,189,918.306119497	10.2020%
5	0x37c16e9c4259ae757daea8bde1726ff43ba07a33	19,189,634.800545545	10.2018%
6	0xc775648876bd3002f8ae84a28eaa2d172f6290ff	14,447,580.038410365	7.6808%
7	0xd376f98f29931b843cc720f60fbf3c2002c9226d	11,317,624.837388462	6.0168%
8	0xf6ae2238713387e3bf85e9fd853261a2193d73b7	9,594,817.400272772	5.1009%
9	0xc59ae4a78d4bf30889754a150b9987d58c0e813e	9,594,817.400272772	5.1009%
10	PancakeSwap V2: BRAND 3	2,208,638.090718602	1.1742%

Contract functions details

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

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

+ Ownable (Context)
  - [Pub] <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 #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ BrandPad (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Ext] increaseAllowance #
  - [Ext] decreaseAllowance #
  - [Pub] isExcluded
  - [Pub] isFeeless
  - [Pub] totalFees
  - [Ext] reflect #
  - [Pub] reflectionFromToken

- [Pub] tokenFromReflection
- [Ext] excludeAccount #
  - modifiers: onlyOwner
- [Ext] includeAccount #
  - modifiers: onlyOwner
- [Ext] setFeeless #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Ext] setFeePercent #
  - 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.	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. Out of gas

Issue:

- The function includeInAccount() 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.

```
ftrace | funcSig
function includeAccount(address account⬆) external onlyOwner {
    require(_isExcluded[account⬆], "Account is already included");
    uint256 length = _excluded.length;
    for (uint256 i = 0; i < 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.

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

Recommendation:
Check that the excluded array length is not too big.

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

- Owner can change _tFeePercent.

```
ftrace | funcSig
function setFeePercent(uint256 fee⬆) external onlyOwner {
    require(fee⬆ >= 1, "Fee is too small");
    require(fee⬆ <= 10, "Fee is too big");
    _tFeePercent = fee⬆;
}
```

- Owner can exclude and include addresses in fees.

```
ftrace | funcSig
function setFeeless(address account⬆, bool isFeeless_⬆) external onlyOwner {
    _isFeeless[account⬆] = isFeeless_⬆;
    emit MarkedFeeless(account⬆, isFeeless_⬆);
}
```

Conclusion

Smart contracts contain low 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.