



Techrate1



Techrate



TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details



Audited project

Pride



Deployer address

0xdf6fEE057222d2F7933C215C11e5150bD2efc53E



Client contacts:

Pride team



Blockchain

Binance Smart Chain



Project website:

<https://certifiedpride.org>

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 Pride to perform an audit of smart contracts:

<https://bscscan.com/address/0x97698acc3141edf3e9fa70d20ca39cf6602990f1#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

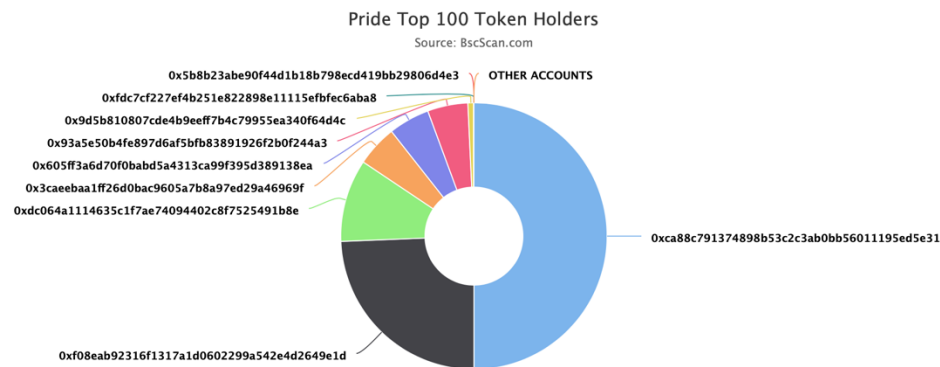
Token contract details for 12.11.2021

Contract name	Pride
Contract address	0x97698ACc3141EdF3e9Fa70d20Ca39CF6602990F1
Total supply	210,000,000,000
Token ticker	LGBT
Decimals	18
Token holders	33
Transactions count	55
Top 100 holders dominance	100.00%
Contract deployer address	0xdf6fEE057222d2F7933C215C11e5150bD2efc53E
Contract's current owner address	0x93a5E50B4FE897d6af5bfB83891926f2B0F244a3

Pride Token Distribution

The top 100 holders collectively own 100.00% (210,000,000,000.00 Tokens) of Pride

Token Total Supply: 210,000,000,000.00 Token | Total Token Holders: 33

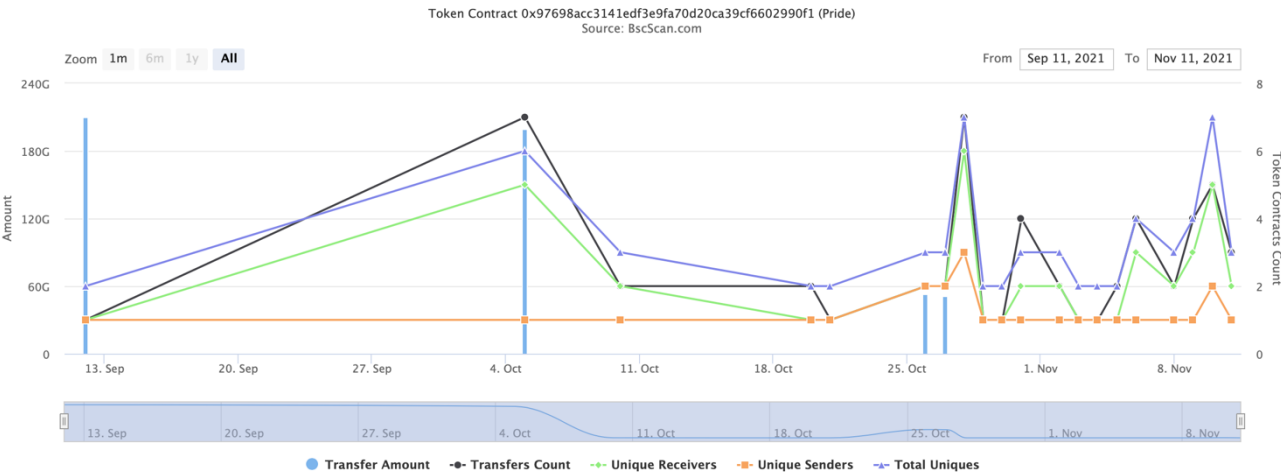


(A total of 210,000,000,000.00 tokens held by the top 100 accounts from the total supply of 210,000,000,000.00 token)


Pride Contract Interaction Details

Time Series: Token Contract Overview

Sun 12, Sept 2021 - Thu 11, Nov 2021



Pride Top 10 Token Holders

Rank	Address	Quantity	Percentage
1	0xca88c791374898b53c2c3ab0bb56011195ed5e31	105,000,000,100	50.0000%
2	 0xf08eab92316f1317a1d0602299a542e4d2649e1d	51,185,587,200	24.3741%
3	0xdc064a1114635c1f7ae74094402c8f7525491b8e	21,000,000,000	10.0000%
4	0x3caeebaa1ff26d0bac9605a7b8a97ed29a46969f	10,500,000,000	5.0000%
5	0x605ff3a6d70f0babd5a4313ca99f395d389138ea	10,500,000,000	5.0000%
6	0x93a5e50b4fe897d6af5bfb83891926f2b0f244a3	10,290,408,394.437178362097817093	4.9002%
7	0x9d5b810807cde4b9eef7b4c79955ea340f64d4c	1,500,032,000	0.7143%
8	0xfdc7cf227ef4b251e822898e11115efbfec6aba8	5,000,000	0.0024%
9	0x5b8b23abe90f44d1b18b798ecd419bb29806d4e3	3,968,000	0.0019%
10	0xc6f204fe38140413d509768ebebec674144a1cc7	2,944,000	0.0014%



Contract functions details

- + [Lib] SafeMath
 - [Int] mul
 - [Int] div
 - [Int] sub
 - [Int] add
- + Ownable
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
- + Pausable (Ownable)
 - [Pub] pause #
 - modifiers: onlyOwner,whenNotPaused
 - [Pub] unpause #
 - modifiers: onlyOwner,whenPaused
- + ERC20Basic
 - [Pub] balanceOf
 - [Pub] transfer #
- + ERC20 (ERC20Basic)
 - [Pub] allowance
 - [Pub] transferFrom #
 - [Pub] approve #
- + StandardToken (ERC20)
 - [Pub] transfer #
 - [Pub] balanceOf
 - [Pub] transferFrom #
 - [Pub] approve #
 - [Pub] allowance
 - [Pub] increaseApproval #
 - [Pub] decreaseApproval #
 - [Int] _blackList #
- + PausableToken (StandardToken, Pausable)
 - [Pub] transfer #
 - modifiers: whenNotPaused
 - [Pub] transferFrom #
 - modifiers: whenNotPaused
 - [Pub] approve #
 - modifiers: whenNotPaused
 - [Pub] increaseApproval #
 - modifiers: whenNotPaused
 - [Pub] decreaseApproval #
 - modifiers: whenNotPaused
 - [Pub] blacklistAddress #
 - modifiers: whenNotPaused,onlyOwner
- + CoinToken (PausableToken)
 - [Pub] <Constructor> #

- [Pub] burn #
- [Int] _burn #
- [Pub] mint #
 - 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.	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

No low severity issues found.

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

- Owner can pause / unpause contract.

```
/**
 * @dev called by the owner to pause, triggers stopped state
 */
function pause() onlyOwner whenNotPaused public {
    paused = true;
    emit Pause();
}

/**
 * @dev called by the owner to unpause, returns to normal state
 */
function unpause() onlyOwner whenPaused public {
    paused = false;
    emit Unpause();
}
```

- Owner can add / remove addresses from blacklist.

```
function blacklistAddress(address listAddress, bool isBlackListed) public whenNotPaused onlyOwner returns (bool success) {
    return super._blackList(listAddress, isBlackListed);
}
```

- Owner can mint any amount of tokens.

```
function mint(address account, uint256 amount) onlyOwner public {

    totalSupply = totalSupply.add(amount);
    balances[account] = balances[account].add(amount);
    emit Mint(address(0), account, amount);
    emit Transfer(address(0), account, amount);
}
```

Conclusion

Smart contracts do not contain high severity issues! Smart contracts contain owner privileges.

Liquidity locking details are NOT provided by the team.

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.



[Techrate1](#)



[Techrate](#)



[Techrate_audits](#)