



# **RugFreeCoins Audit**



## **Splash Token**

### **Smart Contract Security Audit**

**March 16, 2022**



# Contents

Audit details	3
Disclaimer	4
Background	5
About the project	6
Target market and the concept	11
Potential to grow with score points	12
Total Points	12
Contract details	13
Top token holders	14
Security issue checking status	15
Owner privileges	16
Wave Token	18
Contract details	18
Top token holders	19
Owner privileges	20
Buddy system contract	21
Contract details	21
Security issue checking status	23
Owner privileges	24
The tap contract	26
Contract details	26
Security issue checking status	26
Owner privileges	27
Theshore (staking contract)	30
Security issue checking status	30
Owner privileges	30
Contract code function details	31
Contract description table	32
Audit conclusion	38

# Audit details



## Audited project

Splash Token

## Contract Address

### Splash Token:

0x4ec58f9d205f9c919920313932cc71ec68d123c7

### TheWell aka fountain:

0xe3e99ab3a48dd54cad5cfa451aceb9ce03937df9

### TheShore aka resevior:

0x7f732c3743a1679c95955b10fbb9ae8465ed1a1e

### The Tap aka faucet:

0x4b597058b2c10710420d27073a7d83aece517219

### Wave token aka BR34P token:

0xbc6f589171d6d66eb44ebcc92dff570db4208da

### Buddy system:

0x39027379F0e3835f8A3C4E6cf5e96777De0894A6



## Client contact

Splash Team



## Blockchain

Avalanche smart chain



## Project website

<https://splassive.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 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 Rugfreecoins and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rugfreecoins) owe no duty of care towards you or any other person, nor does Rugfreecoins 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 Rugfreecoins 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, Rugfreecoins hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rugfreecoins, 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

Rugfreecoins was commissioned by Libero Financial Token to perform an audit of the smart contract.

Splash Token

**<https://snowtrace.io/address/0x4ec58f9d205f9c919920313932cc71ec68d123c7>**

The well aka fountain

**<https://snowtrace.io/address/0xe3e99ab3a48dd54cad5cfa451aceb9ce03937df9#code>**

The Shore aka reservoir:

**<https://snowtrace.io/address/0x7f732c3743a1679c95955b10fbb9ae8465ed1a1e#code>**

The Tap aka faucet:

**<https://snowtrace.io/address/0x4b597058b2c10710420d27073a7d83aece517219#code>**

Wave token aka BR34P token:

**<https://snowtrace.io/address/0xbc6f589171d6d66eb44ebcc92dff570db4208da#code>**

Buddy system:

**<https://snowtrace.io/address/0x39027379F0e3835f8A3C4E6cf5e96777De0894A6#code>**

The focus of this audit is to verify that the smart contract is secure, resilient and working according to the specifications.

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

# About the project

Splash Network is the latest project developed by Splassive Team.

The official token of the Splash Network is Splash (SPLASH) on the Avalanche Chain (AVAX) which captures value by being scarce, deflationary, censorship-resistant, and by being built on a robust, truly decentralized blockchain.

The recommended exchange for trading Splash is the Well contract which can be found directly on the platform's website, as it allows to waive the initial 10% tax on buys and provides the lowest prices and highest liquidity, resulting in less slippage for larger trades.


## Tokenomics

- **Splash Contract**
- ❖ 10% tax when buying, selling and transferring (excluding buy from the Splash website page).

The recommended exchange for trading splash is THE WELL contract which can be found directly on the platforms website which provides the lowest prices and highest liquidity, resulting in less slippage for larger trades. For other exchanges, such as PancakeSwap, it is recommended to always cross-check the token address against the splash address provided on splassive.com as there are many scams and fake splash tokens currently being listed. Splash can be deposited into splash's the tap contract to provide a consistent 2% daily return (up to 360% of initial principal amount) for participation over time. Additionally, players can add their wbnb into the shore contract to become a permanent liquidity provider for splash and earn wbnb rewards indefinitely from multiple dividend streams and income generated from Exchange fees. Splash is the only deflationary daily ROI token that pays stakers and referrers from a tax on transactions and not through inflation!

- The well aka fountain

SPLASH: S i V E



## 08 THE WELL

THE WELL is the splash network's solution for players that want benefit from noninflationary Yield farming through adding liquidity to SPLASH. Players can participate by adding AVAX to the shore Contract to earn passive perpetual AVAX rewards, while also providing locked liquidity to the SPLASH ecosystem! AVAX Rewards are paid out instantly and through a persisting SPLASH protocol from the dividend pool.

THE WELL helps provide long-term price support and an ever-rising potential price floor, as permanently locked liquidity is added to the SPLASH token on the splash network's Swap exchange. Not only are players able to receive perpetual AVAX dividends using THE WELL, but THE WELL ensures that the floor of liquidity for SPLASH is hardened, providing permanently locked liquidity and long-term price support. When you enter the shore contract you are swapping AVAX for a token called DROP that is held by the shore contract and represents your share of the SPLASH/AVAX liquidity pool. Drop will not fluctuate in value and is pegged 1:1 with SPLASH x AVAX (SPLASH's native liquidity pool token).

The amount of DROP held by a player determines their share of the dividends that they will receive from the shore's instant and daily dividend pools. When you swap AVAX for drop and vice versa there is a 10% tax that is used to pay AVAX rewards to people in the shore and lock liquidity in the SPLASH-AVAX liquidity pool. 2% of the AVAX used to buy drop is immediately distributed to people in the shore, 5% goes into the shore pool which pays out 2% of its balance every day to people in the shore, and 3% is permanently locked in the SPLASH liquidity pool! Your share of the shore will fluctuate overtime; decreasing as more DROP are purchased by other players. You can always increase your Share by compounding or purchasing more drop. We have also implemented a 1% fee on SPLASH-AVAX swaps and this fee goes into the shore dividend pool that is distributed daily proportional to players Drop holdings. This creates an additional stream of AVAX into the shore contract which is not dependent on more people Buying drop by entering the shore!

- **The Shore aka reservoir**

Players can add their WBNB to become permanent liquidity provider for splash and earn WBNB rewards.

❖ Entry Fee	=	10%
❖ Exit Fee	=	10%
❖ Drip Fee	=	50%
❖ Instant Fee	=	20%

- **The Tap aka faucet**

5% tax goes into the tap pool that is used to pay daily ROIs and referral bonuses.

❖ 2% daily return upto 360%

The tap's compound mechanism uses your current available splash dividends and redeposits them into the tap contract, compounding your long-term earnings by increasing your daily cash flow and also by increasing your max pay-out. There is only a 5% tax on compounding transactions instead of the 10% tax that is put on other splash transactions. This 5% tax goes into the tap pool that is used to pay daily ROIs and referral bonuses. The splash from this tax is also paired with AVAX from the shore liquidity staking contract and locked in the splashAVAX liquidity pool.

Splash can be deposited into splash's tap contract to provide a consistent 2% daily return (up to 360% of the initial principal amount) for participation over time. Additionally, players can add their AVAX into the shore contract to become a permanent liquidity provider for splash and earn AVAX rewards indefinitely from multiple dividend streams and income generated from exchange fees. Splash is the only deflationary daily ROIs token that pays stakers and referrers from a tax on transactions and not through inflation! Net deposit value = (deposits + airdrops + rolls) – claims.





## THE TAP

The splash network's the tap is a low-risk, high reward contract that operates similarly to a high yield certificate of deposit. Players can participate by purchasing splash from the platform's swap page, joining another user's Splasive team (10 splash minimum requirement) depositing splash to the tap contract earns a consistent 2% daily return of their splash (360% maximum payout) passively. Players can also compound their earnings through regular deposits, rolling rewards as well as team based referrals. Unlike many other platforms promising a consistent daily % return, the tap's contract cannot drain and will always be able to provide the splash that has been rewarded. Splash rewards come from a 10% tax on all splash transactions excluding buys from the platform's swap page. If there is ever a situation where the tax pool is not enough to pay splash rewards new splash will be minted to ensure rewards are paid out. Given the ingenious game theory behind the splash network, the probability that the system will need to mint new splash to pay rewards is extremely low. Since splash deposited into the tap are sent to a burn address and splash is constantly being locked in the liquidity pool through the shore contract, splash is the only deflationary daily ROI platform. The best strategy for splash is to focus on real world adoption by building out your team through direct referrals, as you will receive bonus rewards from referrals on their deposits and downline bonuses from players, they refer based on the amount of WAVE held in your wallet (see section titled 'referral system/reward structure' for more information). By doing so, you will dramatically accelerate your Roi period and allow your team's chain to grow out organically. Not only are players able to passively increase their splash holdings in the tap through participation over time, but the tap also incentivizes players to participate actively by providing lucrative referral rewards for holding WAVE in their wallet and building out their team. There is also an airdrop feature which is a great way to ensure that your account is in positive net deposit value standing, give back to your team, and also build up referrals through frequent giveaways.

- Wave token aka BR34P token

- **Buddy system**

In order to successfully make a deposit into the tap staking contract, you will first need to join someone else's team by either clicking their referral link or by manually adding their wallet address into the buddy referral system (minimum requirement 10 splash). In order to receive referral rewards, players must hold WAVE in their wallet and the depth of the rewards received will be determined by their individual WAVE tier requirements. In addition, accounts must have positive deposit status for direct referral bonus rewards as well. Not only will you get bonuses from your downline referrals, but you will also get a 2.5% deposit/compounding bonus when you deposit under a "team wallet" which means someone who has 5 or more direct referrals. A rate sheet is included below for how much WAVE must be held to receive 10% bonus rewards on deposits from your downline.

If an account is not net positive when the player in their downline deposits, or if they do not hold enough WAVE to receive referral bonuses at that level of downline or they were the last person to be credited with a referral bonus from that player, the bonus will go further upline until it hits a player who is eligible for the referral bonuses. Using this round robin system, we have eliminated the incentive for self-referring and other bad behavior which is used to leech referral systems, while still greatly rewarding team building through referrals! If a player plays like a solo player, they will not get team Based rewards. Rewards are paid as a direct deposit. This will directly and immediately enhance longevity of the platform and also promote long term team building. The WAVE tier requirements for downline referral bonus are as follows...



Downlines accessible	WAVE in wallet
1	5,000
2	10,000
3	20,000
4	30,000
5	40,000
6	50,000
7	60,000
8	75,000
9	85,000
10	100,000
11	110,000
12	120,000
13	135,000
14	190,000
15	200,000

## Roadmap

- ❖ Splash pre-sale - WHITELIST ONLY
- ❖ Splash LAUNCH - 24-48 hours after pre-sale
- ❖ Splash NFT game - 2-3 weeks after launch
- ❖ Splash Farm will also be launched within the game
- ❖ Splash DAO- 2-3 weeks after launch

# Target market and the concept

## Target market

- ❖ Anyone who's interested in the Crypto space with long-term investment plans.
- ❖ Anyone who's ready to earn a passive income by holding tokens.
- ❖ Anyone who's interested in trading tokens.
- ❖ Anyone who's ready in refer users and earn rewards
- ❖ Anyone who's ready in staking and earn rewards.
- ❖ Anyone who's interested in taking part with Splash play and earn rewards.
- ❖ Anyone who's interested in taking part with the future plans of the Splash token.
- ❖ Anyone who's interested in making financial transactions with any other party using Splash as the currency.

# Potential to grow with score points

1.	Project efficiency	10/10
2.	Project uniqueness	10/10
3	Information quality	9/10
4	Service quality	10/10
5	System quality	9/10
6	Impact on the community	10/10
7	Impact on the business	10/10
8	Preparing for the future	10/10
Total Points		<b>9.75/10</b>



# Splash Token Contract (tax 10%)

## Contract details

**Token contract details for 16<sup>th</sup> March 2022**

Contract name	Splash Token
Contract address	0x4ec58f9D205F9c919920313932cc71EC68d123C7
Token supply	1,000,000
Token ticker	Splash
Decimals	18
Token holders	4,002
Transaction count	31,285
Top 100% holders dominance	99.65%
Vault address	0x050633b351be6952fad9464622e33368e51af140
Contract deployer address	0xae22D494De9dD10b92915a72e4d0c44DaeE4B9E0
Contract's current owner address	0xae22d494de9dd10b92915a72e4d0c44daee4b9e0

# Top token holders

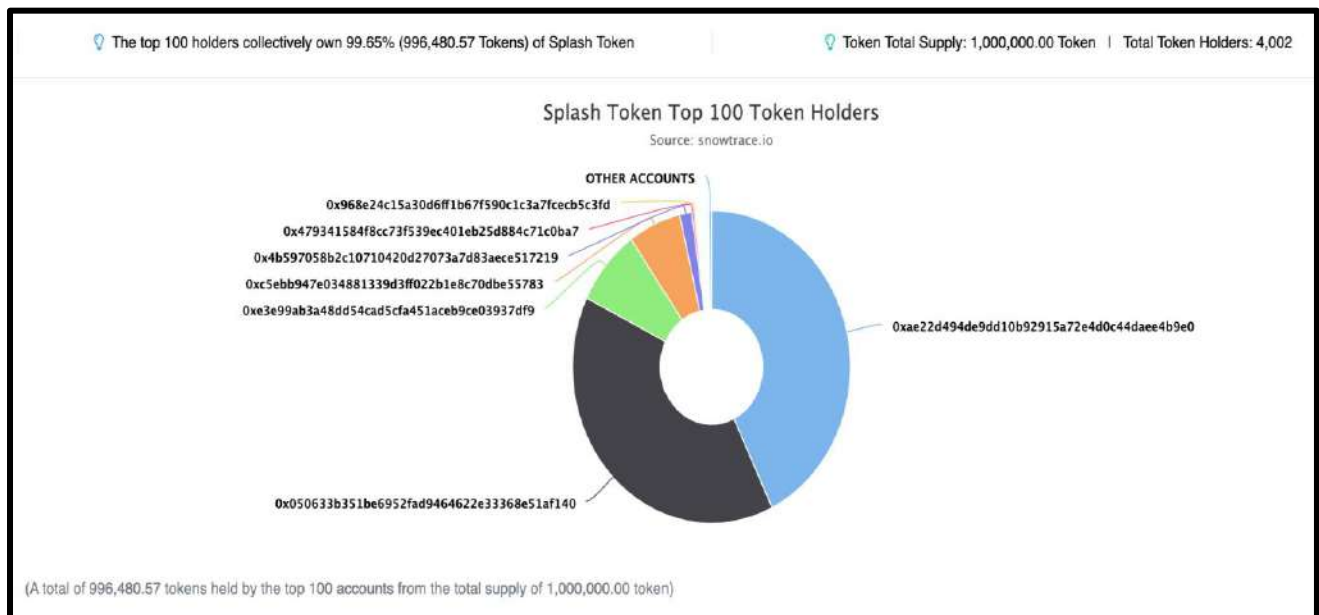
## Top 10 token holders



(A total of 984,622.95 tokens held by the top 10 accounts from the total supply of 1,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xae22d494de9dd10b92915a72e4d0c44dae4b9e0	428,358.667346283982940535	42.8359%
2	0x050633b351be6952fad9464622e33368e51af140	394,242.361850411939877244	39.4242%
3	0xe3e99ab3a48dd54cad5cfa451aceb9ce03937df9	79,378.84005984690161362	7.9379%
4	0xc5ebb947e034881339d3ff022b1e8c70dbe55783	61,047.254487620672780833	6.1047%
5	0x4b597058b2c10710420d27073a7d83aee517219	14,066.673501076346373129	1.4067%
6	0x479341584f8cc73f539ec401eb25d884c71c0ba7	2,429.012705420443429374	0.2429%
7	0x968e24c15a30d6ff1b67f590c1c3a7fceb5c3fd	1,908.175105021545677675	0.1908%
8	0x4ec2dcdfb3c165da62dd1367cb42fe7551524984	1,362.503429125316416575	0.1363%
9	0xf682bf6eb26fd1083f0b499d958634fe453cf146	1,040.000000000000000001	0.1040%
10	0x5c95679a83363ae561453627a0376fca9bb7587b	789.460287806152036198	0.0789%

## Top 100 token holders



## Security issue checking status

### ❖ High severity issues

No high severity issues found.

### ❖ Medium severity issues

No medium severity issues found.

### ❖ Low severity issues

Using an outdated solidity version.

```
pragma solidity ^0.4.25;
```

Recommend: update it to the latest version

# Owner privileges

- ❖ The owner can add whitelist wallets.

```
ftrace | funcSig
function addAddressToWhitelist(address addr↑)
  public
  onlyOwner
  returns (bool success↑)
{
  if (!whitelist[addr↑]) {
    whitelist[addr↑] = true;
    emit WhitelistedAddressAdded(addr↑);
    success↑ = true;
  }
}
```

- ❖ The owner can remove address from whitelist.

```
ftrace | funcSig
function removeAddressFromWhitelist(address addr↑)
  public
  onlyOwner
  returns (bool success↑)
{
  if (whitelist[addr↑]) {
    whitelist[addr↑] = false;
    emit WhitelistedAddressRemoved(addr↑);
    success↑ = true;
  }
}
```



- ❖ The owner can mint new tokens.

```
ftrace | funcSig
function mint(address _to↑, uint256 _amount↑)
    public
    onlyWhitelisted
    canMint
    returns (bool)
{
    require(_to↑ != address(0));
    totalSupply_ = totalSupply_.add(_amount↑);
    balances[_to↑] = balances[_to↑].add(_amount↑);
    emit Mint(_to↑, _amount↑);
    emit Transfer(address(0), _to↑, _amount↑);
    return true;
}
```

- ❖ The owner can add custom tax rate to each wallet.

```
ftrace | funcSig
function setAccountCustomTax(address account↑, uint8 taxRate↑)
    external
    onlyOwner
{
    require(taxRate↑ >= 0 && taxRate↑ <= 100, "Invalid tax amount");
    _hasCustomTax[account↑] = true;
    _customTaxRate[account↑] = taxRate↑;
}
```

- ❖ The owner can remove custom tax from wallet.

```
ftrace | funcSig
function removeAccountCustomTax(address account↑) external onlyOwner {
    _hasCustomTax[account↑] = false;
}
```

# Wave Token

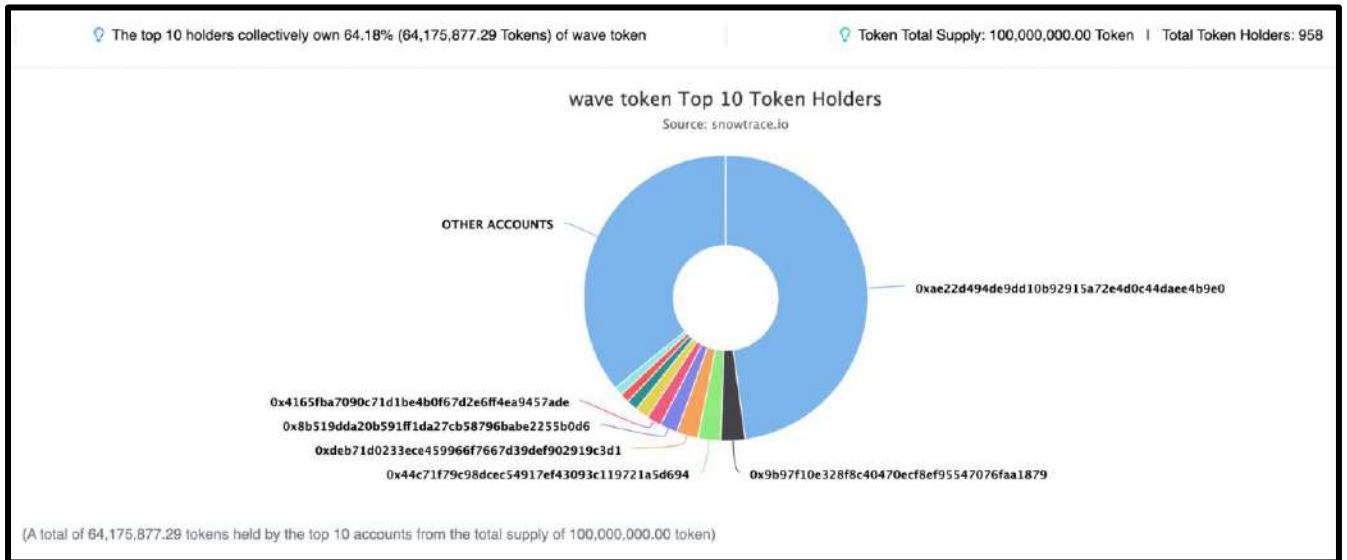
## Contract details

### Token contract details for 16<sup>th</sup> March 2022

Contract name	Wave Token
Contract address	0xbc6f589171d6d66EB44ebCC92dFFb570Db4208da
Token supply	1,000,000
Token ticker	Wave
Decimals	18
Token holders	958
Transaction count	5,633
Top 100% holders dominance	85.51%
Contract deployer address	0xae22D494De9dD10b92915a72e4d0c44DaeE4B9E0
Contract's current owner address	Not public

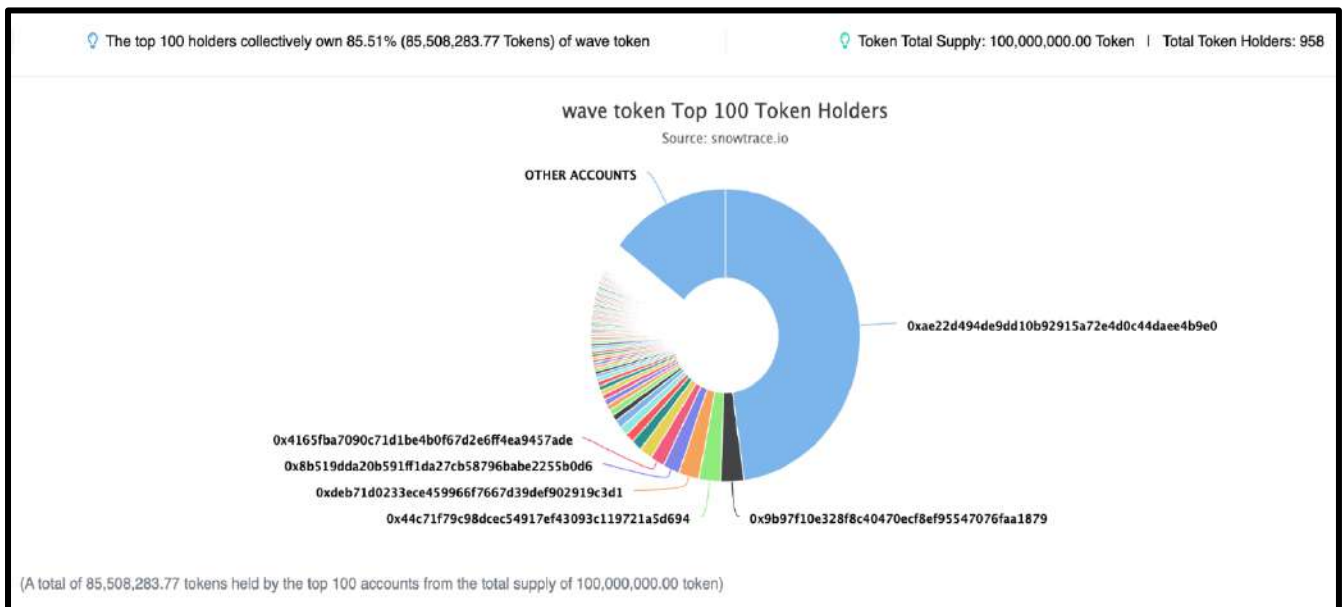
# Top token holders

## Top 10 token holders



Rank	Address	Quantity (Token)	Percentage
1	0xae22d494de9dd10b92915a72e4d0c44dae4b9e0	47,810,241.436729644662050359	47.8102%
2	0x9b97f10e328f8c40470ecf8ef95547076faa1879	2,761,684.100134923164204444	2.7617%
3	0x44c71f79c98dcec54917ef43093c119721a5d694	2,593,156.56440071	2.5932%
4	0xdeb71d0233ece459966f7667d39def902919c3d1	2,450,189.296723226263944701	2.4502%
5	0x8b519dda20b591ff1da27cb58796babe2255b0d6	2,000,649.87282551746289801	2.0006%
6	0x4165fba7090c71d1be4b0f67d2e6ff4ea9457ade	1,685,947.769940990417343303	1.6859%
7	0x145b759a549c1121cf2a658ee48c39d130b3bead	1,556,554	1.5566%
8	0xd12b87b4bb9ee50127ee76031304133ae0a80515	1,257,601.158733834538853025	1.2576%
9	0x80ff59d3518ca8954c5c2a642fc3d553486a9bbd	1,059,852.699195879898841982	1.0599%
10	0x4ec2dcd1b3c165da62dd1367cb42fe7551524984	1,000,000.387771682971431862	1.0000%

## Top 100 token holders



## Owner privileges

- ❖ The owner can add or update buddies.

```
ftrace | funcSig
function updateBuddy(address buddy↑) public {
    require(
        buddyOf(buddy↑) != address(0) ||
        (buddy↑ == owner && buddy↑ != msg.sender),
        "upline not found"
    );
    require(buddyOf(msg.sender) == address(0), "Already have buddy!");
    address upline = buddy↑;
    buddies[msg.sender] = buddy↑;

    do {
        Treeofbuddies[msg.sender].push(upline); // do while loop
        upline = buddyOf(upline);
    } while (upline != address(0));

    emit onUpdateBuddy(msg.sender, buddy↑);
}
```



# Buddy system contract

## Contract details

**Token contract details for 16<sup>th</sup> March 2022**

Contract name	Buddy System
Contract address	0x39027379F0e3835f8A3C4E6cf5e96777De0894A6
Token supply	-
Token ticker	-
Decimals	-
Token holders	-
Transaction count	-
Top 100% holders dominance	99.65%
Contract deployer address	0xae22D494De9dD10b92915a72e4d0c44DaeE4B9E0

# Splash Liquidity Token

## Contract details

**This contract is like an exchange user can buy and sell splash tokens with this contract**

Contract name	Splash Liquidity Token
Contract address	0x39027379F0e3835f8A3C4E6cf5e96777De0894A6
Token supply	46.847269
Token ticker	DROPS
Decimals	18
Token holders	2
Transaction count	23
Contract deployer address	0xae22D494De9dD10b92915a72e4d0c44DaeE4B9E0

# Security issue checking status

## ❖ High severity issues

The owner can pause the contract.

```
ftrace | funcSig
function unpause() public onlyOwner {
    isPaused = false;
}

ftrace | funcSig
function pause() public onlyOwner {
    isPaused = true;
}
```

## ❖ Medium severity issues

No medium severity issues found.

## ❖ Low severity issues

No low severity issues found.

# Owner privileges

- ❖ The owner can add/remove whitelist address.

```
ftrace | funcSig
function addAddressToWhitelist(address addr↑)
    public
    onlyOwner
    returns (bool success↑)
{
    if (!whitelist[addr↑]) {
        whitelist[addr↑] = true;
        emit WhitelistedAddressAdded(addr↑);
        success↑ = true;
    }
}

/**
 * @dev add addresses to the whitelist
 * @param addrs addresses
 */
ftrace | funcSig
function addAddressesToWhitelist(address[] memory addrs↑)
    public
    onlyOwner
    returns (bool success↑)
{
    for (uint256 i = 0; i < addrs↑.length; i++) {
        if (addAddressToWhitelist(addrs↑[i])) {
            success↑ = true;
        }
    }
    return success↑;
}
```



```

ftrace | funcSig
function addAddressToWhitelist(address addr↑)
    public
    onlyOwner
    returns (bool success↑)
{
    if (!whitelist[addr↑]) {
        whitelist[addr↑] = true;
        emit WhitelistedAddressAdded(addr↑);
        success↑ = true;
    }
}

/**
 * @dev add addresses to the whitelist
 * @param addrs addresses
 */
ftrace | funcSig
function addAddressesToWhitelist(address[] memory addrs↑)
    public
    onlyOwner
    returns (bool success↑)
{
    for (uint256 i = 0; i < addrs↑.length; i++) {
        if (addAddressToWhitelist(addrs↑[i])) {
            success↑ = true;
        }
    }
    return success↑;
}

```

- ❖ The owner can pause/unpause contract

```

ftrace | funcSig
function unpause() public onlyOwner {
    isPaused = false;
}

ftrace | funcSig
function pause() public onlyOwner {
    isPaused = true;
}

```

# The tap contract

## Contract details

Token contract details for 16<sup>th</sup> March 2022

Contract name	The tap
Contract address	0x4ec58f9D205F9c919920313932cc71EC68d123C7
Contract deployer address	0xae22D494De9dD10b92915a72e4d0c44DaeE4B9E0
Contract's current owner address	0xae22d494de9dd10b92915a72e4d0c44daee4b9e0
The Drip Vault address	0x050633b351be6952fad9464622e33368e51af140

## Security issue checking status

❖ **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

- ❖ The owner can change total airdrop amount.

```
ftrace | funcSig
function setTotalAirdrops(uint256 newTotalAirdrop↑) public onlyOwner {
    total_airdrops = newTotalAirdrop↑;
}
```

- ❖ The owner can change total users.

```
ftrace | funcSig
function setTotalUsers(uint256 newTotalUsers↑) public onlyOwner {
    total_users = newTotalUsers↑;
}
```

- ❖ The owner can change total deposit amount.

```
ftrace | funcSig
function setTotalDeposits(uint256 newTotalDeposits↑) public onlyOwner {
    total_deposited = newTotalDeposits↑;
}
```

- ❖ The owner can change total withdraw amount.

```
ftrace | funcSig
function setTotalWithdraw(uint256 newTotalWithdraw↑) public onlyOwner {
    total_withdraw = newTotalWithdraw↑;
}
```

- ❖ The owner can change total bnb amount.

```
ftrace | funcSig
function setTotalBNB(uint256 newTotalBNB↑) public onlyOwner {
    total_bnb = newTotalBNB↑;
}
```

- ❖ The owner can change total tax fee.

```
ftrace | funcSig
function setTotalTX(uint256 newTotalTX↑) public onlyOwner {
    total_txs = newTotalTX↑;
}
```

- ❖ The owner can change payout rate.

```
/****** Administrative Functions *****/
ftrace | funcSig
function updatePayoutRate(uint256 _newPayoutRate↑) public onlyOwner {
    payoutRate = _newPayoutRate↑;
}
```

- ❖ The owner can change max referral levels.

```
ftrace | funcSig
function updateRefDepth(uint256 _newRefDepth↑) public onlyOwner {
    ref_depth = _newRefDepth↑;
}
```

- ❖ The owner can change referral bonus.

```
ftrace | funcSig
function updateRefBonus(uint256 _newRefBonus↑) public onlyOwner {
    ref_bonus = _newRefBonus↑;
}
```

- ❖ The owner can change minimum initial deposit amount.

```
ftrace | funcSig
function updateInitialDeposit(uint256 _newInitialDeposit↑) public onlyOwner {
    minimumInitial = _newInitialDeposit↑;
}
```



- ❖ The owner can change compound tax maximum upto 20%.

```
ftrace | funcSig
function updateCompoundTax(uint256 _newCompoundTax↑) public onlyOwner {
    require(_newCompoundTax↑ >= 0 && _newCompoundTax↑ <= 20);
    CompoundTax = _newCompoundTax↑;
}
```

- ❖ The owner can change exit tax maximum up to 20%.

```
ftrace | funcSig
function updateExitTax(uint256 _newExitTax↑) public onlyOwner {
    require(_newExitTax↑ >= 0 && _newExitTax↑ <= 20);
    ExitTax = _newExitTax↑;
}
```

# Theshore (staking contract)

## Security issue checking status

- ❖ **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











**No owner functions detected**

# Contract code function details









No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	low
		visibility specifiers	pass
		Gas consumption	pass
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Selfdestruct function security	pass
3	Business security	Access control of owners	high
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass
13	Event security		pass













# Contract description table











Below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions and implementations with its visibility and mutability.



















Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation			
L		Public !		NO!
L	transferOwnership	Public !		onlyOwner
Whitelist	Implementation	Ownable		
L	addAddressToWhitelist	Public !		onlyOwner
L	addAddressesToWhitelist	Public !		onlyOwner
L	removeAddressFromWhitelist	Public !		onlyOwner
L	removeAddressesFromWhitelist	Public !		onlyOwner
SafeMath	Library			
L	mul	Internal 		
L	div	Internal 		
L	sub	Internal 		
L	add	Internal 		





<b>BEP20Basic</b>	<b>Interface</b>			
L	totalSupply	External !		NO !
L	balanceOf	External !		NO !
L	transfer	External !		NO !
<b>BasicToken</b>	<b>Implementation</b>	<b>BEP20Basic</b>		
L	totalSupply	Public !		NO !
L	transfer	Public !		NO !
L	balanceOf	Public !		NO !
<b>BEP20</b>	<b>Implementation</b>	<b>BEP20Basic</b>		
L	allowance	Public !		NO !
L	transferFrom	Public !		NO !
L	approve	Public !		NO !
<b>StandardToken</b>	<b>Implementation</b>	<b>BEP20, BasicToken</b>		
L	transferFrom	Public !		NO !
L	approve	Public !		NO !
L	allowance	Public !		NO !
L	increaseApproval	Public !		NO !
L	decreaseApproval	Public !		NO !

MintableToken	Implementation	StandardToken, Whitelist		
L	mint	Public !		onlyWhitelisted canMint
L	finishMinting	Public !		onlyWhitelisted canMint
SplashToken	Implementation	MintableToken		
L		Public !		Ownable
L	setVaultAddress	Public !		onlyOwner
L	mint	Public !		NO !
L	finishMinting	Public !		onlyOwner canMint
L	calculateTransactionTax	Internal 		
L	transferFrom	Public !		NO !
L	transfer	Public !		NO !
L	calculateTransferTaxes	Public !		NO !
L	remainingMintableSupply	Public !		NO !
L	cap	Public !		NO !
L	mintedSupply	Public !		NO !
L	statsOf	Public !		NO !
L	mintedBy	Public !		NO !
L	setAccountCustomTax	External !		onlyOwner
L	removeAccountCustomTax	External !		onlyOwner

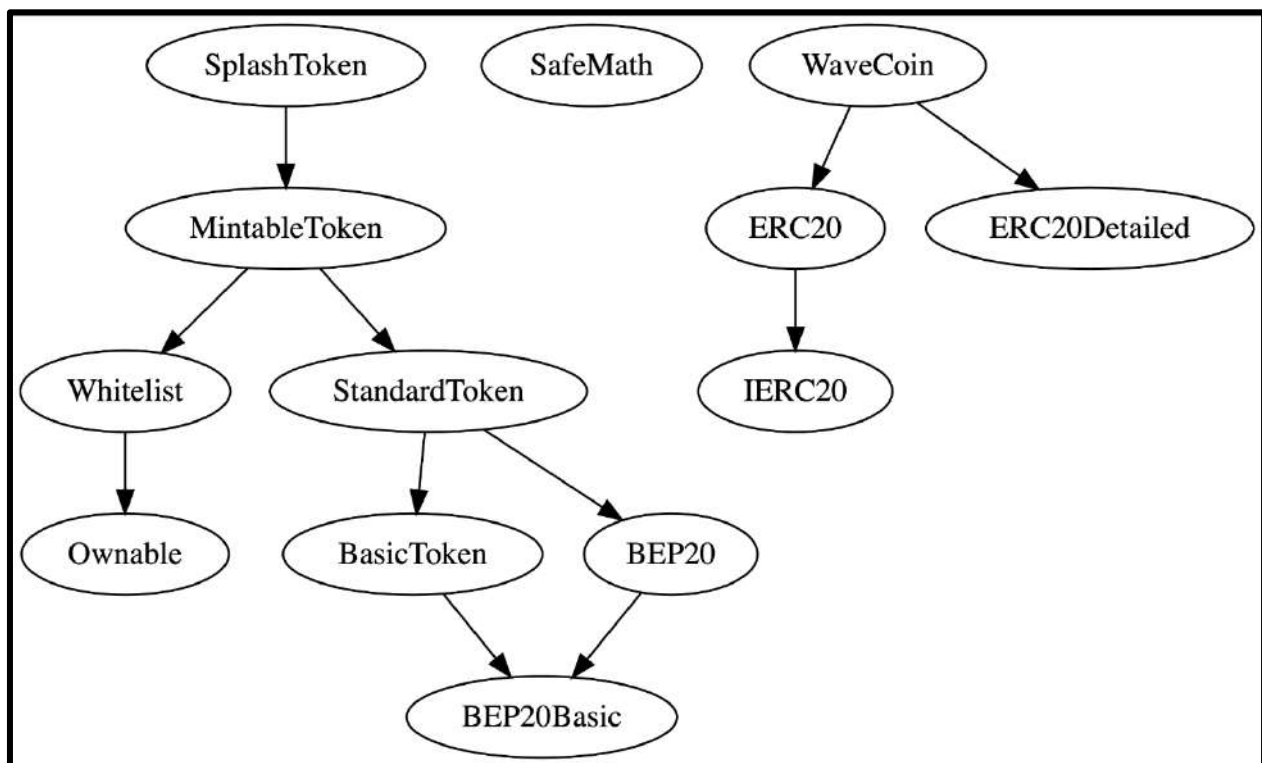
L	excludeAccount	External !		onlyOwner
L	includeAccount	External !		onlyOwner
L	isExcluded	Public !		NO !
<b>SafeMath</b>	<b>Library</b>			
L	add	Internal 		
L	sub	Internal 		
L	mul	Internal 		
L	div	Internal 		
L	mod	Internal 		
<b>IERC20</b>	<b>Interface</b>			
L	totalSupply	External !		NO !
L	balanceOf	External !		NO !
L	transfer	External !		NO !
L	allowance	External !		NO !
L	approve	External !		NO !
L	transferFrom	External !		NO !
<b>ERC20</b>	<b>Implementation</b>	<b>IERC20</b>		
L	totalSupply	Public !		NO !
L	balanceOf	Public !		NO !

L	transfer	Public !		NO !
L	allowance	Public !		NO !
L	approve	Public !		NO !
L	transferFrom	Public !		NO !
L	increaseAllowance	Public !		NO !
L	decreaseAllowance	Public !		NO !
L	_transfer	Internal 		
L	_mint	Internal 		
L	_burn	Internal 		
L	burn	Public !		NO !
L	_approve	Internal 		
L	_burnFrom	Internal 		
<b>ERC20Detailed</b>	<b>Implementation</b>			
L		Public !		NO !
L	name	Public !		NO !
L	symbol	Public !		NO !
L	decimals	Public !		NO !
<b>WaveCoin</b>	<b>Implementation</b>	<b>ERC20, ERC20Detailed</b>		
L		Public !		ERC20Detailed

## Legend

Symbol	Meaning
	Function can modify state
	Function is payable

## Inheritance Hierarchy





# Audit conclusion

RugFreeCoins team has performed an in-depth testing, line by line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations and hacks. According to the smart contract audit.

Smart contract functional Status: **PASSED**

Number of risk issues: **2**

Solidity code functional issue level: **LOW SEVERITY ISSUES**

Number of owner privileges: **21**

Centralization risk correlated to the active owner: **HIGH (The owner has substantial control within the ecosystem, but it's required and align with the project's use case)**

Smart contract active ownership: **YES.**