



# Audit Report

## **MetaBudz**

December 2021

Type       BEP20

Address     0x4D5f45C030627c9CA6D555119A0a1Ed290AB1140

Audited by  © coinscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>2</b>
<b>Audit Updates</b>	<b>2</b>
<b>Contract Analysis</b>	<b>3</b>
<b>ST - Stop Transactions</b>	<b>4</b>
<b>Description</b>	<b>4</b>
<b>OTUT - Owner Transfer User's Tokens</b>	<b>5</b>
<b>Description</b>	<b>5</b>
<b>Contract Diagnostics</b>	<b>6</b>
<b>Contract Functions</b>	<b>7</b>
<b>Contract Flow</b>	<b>10</b>
<b>Domain Info</b>	<b>11</b>
<b>Stacking Contract</b>	<b>12</b>
<b>Stacking Contract Review</b>	<b>12</b>
<b>Stacking Contract Functions</b>	<b>13</b>
<b>Stacking Contract Flow</b>	<b>15</b>
<b>Stacking Contract - ST - Stop Transactions</b>	<b>16</b>
<b>Description</b>	<b>16</b>
<b>Recommendation</b>	<b>16</b>
<b>Summary</b>	<b>17</b>
<b>Disclaimer</b>	<b>18</b>
<b>About Coinscope</b>	<b>19</b>

## Contract Review

<b>Contract Name</b>	BudzToken
<b>Compiler Version</b>	v0.5.17+commit.d19bba13
<b>Optimization</b>	200 runs
<b>Licence</b>	NONE
<b>Explorer</b>	<a href="https://bscscan.com/token/0xa1629e42f86680592DCcdAe47B51e8f17c42aD71">https://bscscan.com/token/0xa1629e42f86680592DCcdAe47B51e8f17c42aD71</a>
<b>Symbol</b>	BUDZ
<b>Decimals</b>	18
<b>Total Supply</b>	200,000
<b>Website</b>	<a href="https://metabudz.net/">https://metabudz.net/</a>

## Audit Updates

<b>Initial Audit</b>	11th of December 2021
<b>Corrected</b>	

## Contract Analysis

Pass	Description
✓	Contract Owner is not able to mint new tokens
✓	Contract Owner is not able to burn tokens from specific wallet
✓	Contract Owner is not able to increase fees more than a reasonable percent (10%)
✗	Contract Owner is not able to stop or pause transactions
✗	Contract Owner is not able to transfer tokens from specific address
✓	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
✓	Contract Owner is not able to blacklist wallets from selling

## ST - Stop Transactions

<b>Criticality</b>	high
<b>Location</b>	<a href="https://www.bscscan.com/address/0x4D5f45C030627c9CA6D555119A0a1Ed290AB1140#code#L122">https://www.bscscan.com/address/0x4D5f45C030627c9CA6D555119A0a1Ed290AB1140#code#L122</a>

### Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by calling the `pause` function from the `Pausable` class

```
function transfer(address to, uint value) external returns(bool) {  
    require(paused() == false || msg.sender == owner, 'Cannot transfer  
paused token');  
}
```

### Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

## OTUT - Owner Transfer User's Tokens

<b>Criticality</b>	high
<b>Location</b>	<a href="https://www.bscscan.com/address/0x4D5f45C030627c9CA6D555119A0a1Ed290AB1140#code#L166">https://www.bscscan.com/address/0x4D5f45C030627c9CA6D555119A0a1Ed290AB1140#code#L166</a>

### Description

The contract owner has the authority to transfer the balance of a user's contract to the owner's contract. The owner may take advantage of it by calling the `transferAnyERC20Token` function.

```
function transferAnyERC20Token(address _tokenAddress, uint _tokens) external  
onlyOwner returns (bool success) {  
    return IERC20(_tokenAddress).transfer(owner, _tokens);  
}
```

### Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

# Contract Diagnostics

Pass	Name
✓	Integer Underflow
✓	Parity Multisig Bug
✓	Callstack Depth Attack
✓	Transaction-Ordering Dependency
✓	Timestamp Dependency
✓	Re-Entrancy

# Contract Functions

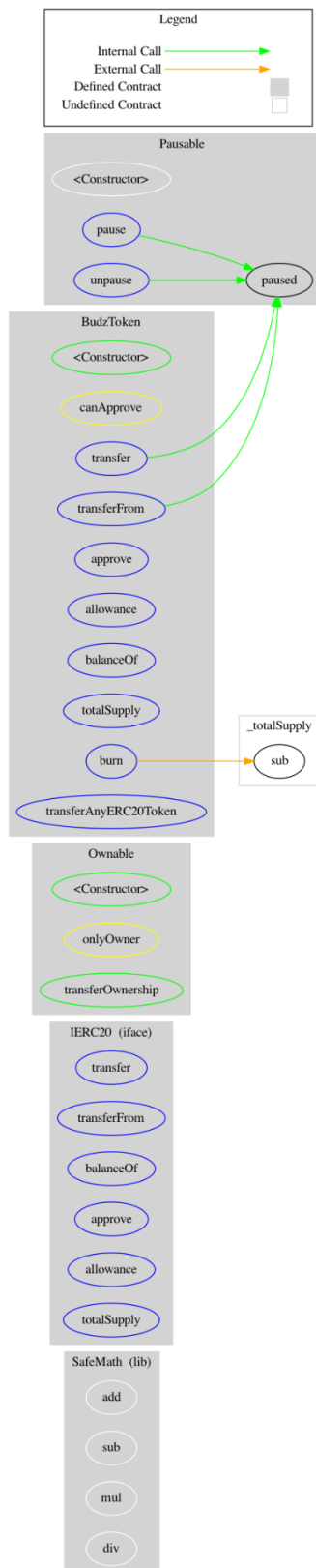
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
IERC20	Interface			
	transfer	External	✓	-
	transferFrom	External	✓	-
	balanceOf	External		-
	approve	External	✓	-
	allowance	External		-
	totalSupply	External		-



Ownable	Implementation			
		Public	✓	-
	transferOwnership	Public	✓	onlyOwner
Pausable	Implementation	Ownable		
		Internal	✓	
	paused	Public		-
	pause	External	✓	onlyOwner
	unpause	External	✓	onlyOwner
BudzToken	Implementation	IERC20, Pausable		
		Public	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	approve	External	✓	canApprove
	allowance	External		-
	balanceOf	External		-
	totalSupply	External		-
	burn	External	✓	onlyOwner

	transferAnyERC20Token	External	✓	onlyOwner
--	-----------------------	----------	---	-----------

# Contract Flow



## Domain Info

<b>Domain Name</b>	metabudz.net
<b>Registry Domain ID</b>	2659150363_DOMAIN_NET-VRSN
<b>Registrar WHOIS Server</b>	whois.namecheap.com
<b>Registrar URL</b>	http://www.namecheap.com
<b>Updated Date</b>	0001-01-01T00:00:00.00Z (wrong information)
<b>Creation Date</b>	2021-12-03T00:54:43.00Z
<b>Registry Expiry Date</b>	2022-12-03T00:54:43.00Z
<b>Registrar</b>	NAMECHEAP INC
<b>Registrar IANA ID</b>	1068

The domain has been created one week before the creation of the audit. It will expire in one year.

There is no public billing information, the creator is protected by the privacy settings.

# Stacking Contract

BudzToken ecosystem contains a contract that is dedicated to stacking. Users have the ability to stack tokens for a period of time and get more tokens as a reward. The Stacking contract incarnates the standard stacking functionality.

## Stacking Contract Review

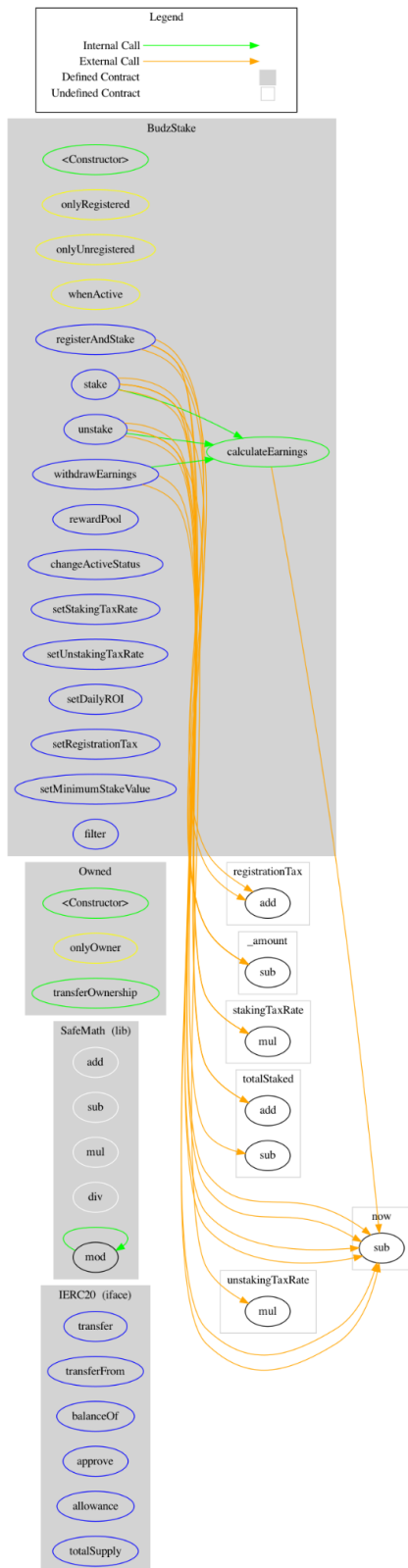
<b>Contract Name</b>	BudzStake
<b>Compiler Version</b>	v0.6.12+commit.27d51765
<b>Optimization</b>	200 runs
<b>Licence</b>	NONE
<b>Explorer</b>	<a href="https://www.bscscan.com/address/0x41B2BA88a0DE89886277d2e8C083884B6dF2ea47">https://www.bscscan.com/address/0x41B2BA88a0DE89886277d2e8C083884B6dF2ea47</a>

# Stacking Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	transfer	External	✓	-
	transferFrom	External	✓	-
	balanceOf	External		-
	approve	External	✓	-
	allowance	External		-
	totalSupply	External		-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Owned	Implementation			
		Public	✓	-
	transferOwnership	Public	✓	onlyOwner
BudzStake	Implementation	Owned		
		Public	✓	-
	registerAndStake	External	✓	onlyUnregistered whenActive

	calculateEarnings	Public		-
	stake	External	✓	onlyRegistered whenActive
	unstake	External	✓	onlyRegistered
	withdrawEarnings	External	✓	-
	rewardPool	External		onlyOwner
	changeActiveStatus	External	✓	onlyOwner
	setStakingTaxRate	External	✓	onlyOwner
	setUnstakingTaxRate	External	✓	onlyOwner
	setDailyROI	External	✓	onlyOwner
	setRegistrationTax	External	✓	onlyOwner
	setMinimumStakeValue	External	✓	onlyOwner
	filter	External	✓	onlyOwner

# Stacking Contract Flow





## Stacking Contract - ST - Stop Transactions

<b>Criticality</b>	high
<b>Location</b>	<a href="https://www.bscscan.com/address/0x41B2BA88a0DE89886277d2e8C083884B6dF2ea47#code#L152">https://www.bscscan.com/address/0x41B2BA88a0DE89886277d2e8C083884B6dF2ea47#code#L152</a>

### Description

The contract owner has the authority to stop the stacking transactions for all users. The owner may take advantage of it by calling the `changeActiveStatus` function.

```
function registerAndStake(uint _amount, address _referrer) external  
onlyUnregistered() whenActive() {  
    require(msg.sender != _referrer, "Cannot refer self");
```

### Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

## Summary

MetaBudz is a DAO system introducing a governance token (\$BUDZ) being backed by a treasury and a staking system. The token has a friendly and growing community. There are some functions that can be abused by the owner, like stopping transactions and transferring the user's funds to the owner's wallet. The stacking contract contains the basic stacking functionality. There are some owner functions that can affect the stacking process, like stopping all the stacking activities. A multi-wallet signing pattern or renouncing the ownership will eliminate all the contract threats.

## Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

CoinScope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The CoinScope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did CoinScope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The CoinScope team disclaims any liability for the resulting losses.

## About Coinscope

CoinScope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

CoinScope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.



The Coinscope.co team

<https://www.coinscope.co>