



**DESSERT**  
FINANCE

## Yield Protocol (YLD)

BEP-20 Audit

Performed at block **19694287**

PERFORMED BY DESSERT FINANCE

FOR CONTRACT ADDRESS: **0x9723c96b1B92cddC036588FD08A6b92607906B57**

## INITIAL DISCLAIMER

Dessert Finance provides due-diligence project audits for various projects. Dessert Finance in no way guarantees that a project will not remove liquidity, sell off team supply, or otherwise exit scam.

Dessert Finance does the legwork and provides public information about the project in an easy-to-understand format for the common person.

Agreeing to an audit in no way guarantees that a team will not remove *all* liquidity (“Rug Pull”), remove liquidity slowly, sell off tokens, quit the project, or completely exit scam. There is also no way to prevent private sale holders from selling off their tokens. It is ultimately your responsibility to read through all documentation, social media posts, and contract code of each individual project to draw your own conclusions and set your own risk tolerance.

Dessert Finance in no way takes responsibility for any losses, nor does Dessert Finance encourage any speculative investments. The information provided in this audit is for information purposes only and should not be considered investment advice. Dessert Finance does not endorse, recommend, support, or suggest any projects that have been audited. An audit is an informational report based on our findings, We recommend you do your own research, we will never endorse any project to invest in.

# Table of Contents



1. Contract Code Audit – Token Overview
2. BEP-20 Contract Code Audit – Overview
3. BEP-20 Contract Code Audit – Vulnerabilities Checked
4. Contract Code Audit – Contract Ownership
5. Contract Code Audit – Owner Accessible Functions
6. Liquidity Ownership – Locked / Unlocked
7. Contract Code Audit – Mint Functions
8. Contract Transaction Fees
9. Website Overview
10. Social Media
11. Top Token Holders/Wallets
12. Location Audit
13. Review of Team
14. Roadmap
15. Disclaimers

# Contract Code Audit – Token Overview





# BEP-20 Contract Code Audit – Overview

Dessert Finance was commissioned to perform an audit on Yield Protocol (YLD)

```
pragma solidity ^0.8.0;
import "openzeppelin-solidity/contracts/token/ERC20/utils/SafeERC20.sol";
import "openzeppelin-solidity/contracts/access/Ownable.sol";

contract LockTaken is Ownable {
    bool public isOpen = false;
    mapping(address => bool) private _whitelist;
    modifier whitelist(address from, address to) {
        require(!isOpen || _whitelist[from] || _whitelist[to], "Not Open");
        _;
    }

    constructor() {
        _whitelist[msg.sender] = true;
        _whitelist[address(this)] = true;
    }

    function openTrade() public onlyOwner {
        isOpen = true;
    }

    function includeWhitelist(address user, bool status) external onlyOwner {
        _whitelist[user] = status;
    }
}

interface IPancakeSwapRouter {
    function factory() external pure returns (address);
    function WETH() external pure returns (address);
    function swapExactETHForTokens(uint amountIn, address[] calldata path, address to, uint deadline) external payable returns (uint amountOut, address[] calldata path);
    function swapExactTokensForTokens(uint amountIn, uint amountOut, address[] calldata path, address to, uint deadline) external returns (uint amountOut, address[] calldata path);
    function swapETHForExactTokens(uint amountOut, address[] calldata path, address to, uint deadline) external payable returns (uint amountIn, address[] calldata path);
    function swapTokensForExactETH(uint amountOut, address[] calldata path, address to, uint deadline) external returns (uint amountIn, address[] calldata path);
}

interface IPancakeSwapFactory {
    function createPair(address tokenA, address tokenB) external returns (address pair);
}

contract Yield is Ownable, LockTaken, ERC20 {
    string private _name = "Yield Protocol";
    string private _symbol = "YLD";

    mapping(address => bool) private _isPair;
    mapping(address => uint256) private _balances;
    mapping(address => mapping(address => uint256)) private _allowances;
    mapping(address => uint256) private _lastYieldTime;
    mapping(address => bool) private _yieldFrozent;
    mapping(address => bool) private _feeExempt;
    mapping(address => uint256) private _apyGain;
    mapping(address => uint256) private _collAmounts;
    mapping(address => uint256) private _collTimestamps;
    mapping(address => uint256) private _penaltyTriggered;

    uint8 public constant yieldDecimals = 6;
    uint8 public constant ERC20AS = 1;
}
```

## Contract Address

0x9723c96b1B92cddC036588FD08A6b92607906B57

## TokenTracker

Yield Protocol (YLD)

## Contract Creator

0xaf8e4a38bfed672909ca6629e19d698b5111dae1

## Source Code

Contract Source Code Verified

## Contract Name

Yield

## Other Settings

default evmVersion

## Compiler Version

v0.8.15+commit.e14f2714

## Optimization Enabled

Yes with 200 runs

Code is truncated to fit the constraints of this document.

[The code in its entirety can be viewed here.](#)

The contract code is **verified** on BSCScan.

# BEP-20 Contract Code Audit – Vulnerabilities Checked

Vulnerability Tested	AI Scan	Human Review	Result
Compiler Errors	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow	Complete	Complete	✓ Low / No Risk
Integer Underflow	Complete	Complete	✓ Low / No Risk
Correct Token Standards Implementation	Complete	Complete	✓ Low / No Risk
Timestamp Dependency for Crucial Functions	Complete	Complete	✓ Low / No Risk
Exposed _Transfer Function	Complete	Complete	✓ Low / No Risk
Transaction-Ordering Dependency	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Variable	Complete	Complete	✓ Low / No Risk
Use of Deprecated Functions	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
State Variable Default Visibility	Complete	Complete	✓ Low / No Risk
Deployer Can Access User Funds	Complete	Complete	✓ Low / No Risk

The contract code is verified on BSCScan.

The vulnerabilities listed above were not found in the token's Smart Contract.

# Contract Code Audit – Contract Ownership

Contract Ownership has not been renounced at the time of Audit



The contract ownership is not currently renounced.

We have placed the contract owner address below for your viewing:

[0xaf8e4a38bfed672909ca6629e19d698b5111dae1](https://etherscan.io/address/0xaf8e4a38bfed672909ca6629e19d698b5111dae1)

The address above has authority over the ownable functions within the contract.

This allows the owner to call certain functions within the contract. Any compromise to the owner wallet may allow these privileges to be exploited.

We recommend:

- Establishing a Time-Lock with reasonable latency
- Assignment of privileged roles to multi-signature wallets

# Contract Code Audit – Owner Accessible Functions

Function Name	Parameters	Visibility	Audit Notes
openTrade		public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
includeToWhiteList	address _user, bool status	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
launch		external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
withdrawBNB		external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
multiSendTokens	address[] calldata addresses, uint256[] calldata amounts	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
sweepTokens	IERC20 tokenAddress	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setPower	uint24 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setCapPerTx	uint24 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setMinTierForLowerFees	uint256 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setBL	uint256 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setSellPeriod	uint256 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setBaseYield	uint256 r	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setYieldStatus	bool status	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setSwapBackDetails	uint256 min, bool status	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setPair	address _address, bool status	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setFeeReceivers	address _treasuryReceiver, address _devWallet	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setFeeExemptStatus	address _address, bool status	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setExemptFromYield	address _address, bool status	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setTolerance	uint256 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
addYieldPenalty	address _address	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setFees	uint256 newLiquidityFee, uint256 newtreasuryFee	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setSellFees	uint256 newLiquidityFee, uint256 newtreasuryFee	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setTransferFees	uint256 newLiquidityFee, uint256 newtreasuryFee	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setDevFees	uint256 num, uint256 den	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setFeeDenominator	uint256 newDenominator	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setMaxYieldTier	uint256 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setTierAdvanceTime	uint256 n	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.

The functions listed above can be called by the contract owner.



# Liquidity Ownership – Locked / Unlocked

No locked liquidity information has been found.



This page will contain links to locked liquidity for the project if we are able to locate that information. Locked liquidity information was not found on the project's website.

# Contract Code Audit – Mint Functions

This Contract Cannot Mint New YLD Tokens.



We do understand that sometimes mint functions are essential to the functionality of the project.

**A mint function was not found in the contract code.**

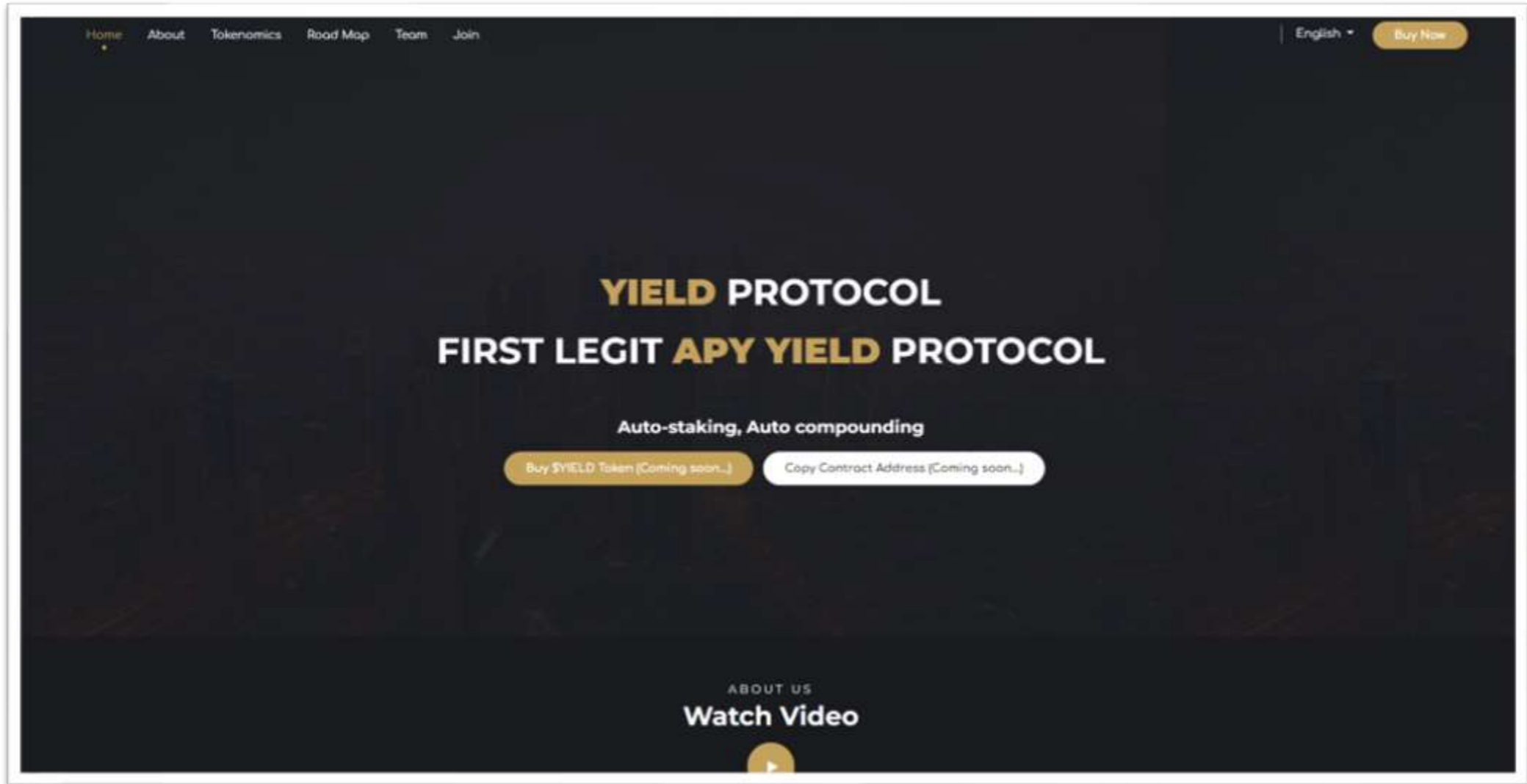
# Contract Transaction Fees

At the time of Audit the transaction fees (“tax”) listed below are the fees associated with trading. These fees are taken from every buy and sell transaction unless otherwise stated.



# Website Part 1 – Overview

[www.yield-token.com](http://www.yield-token.com)



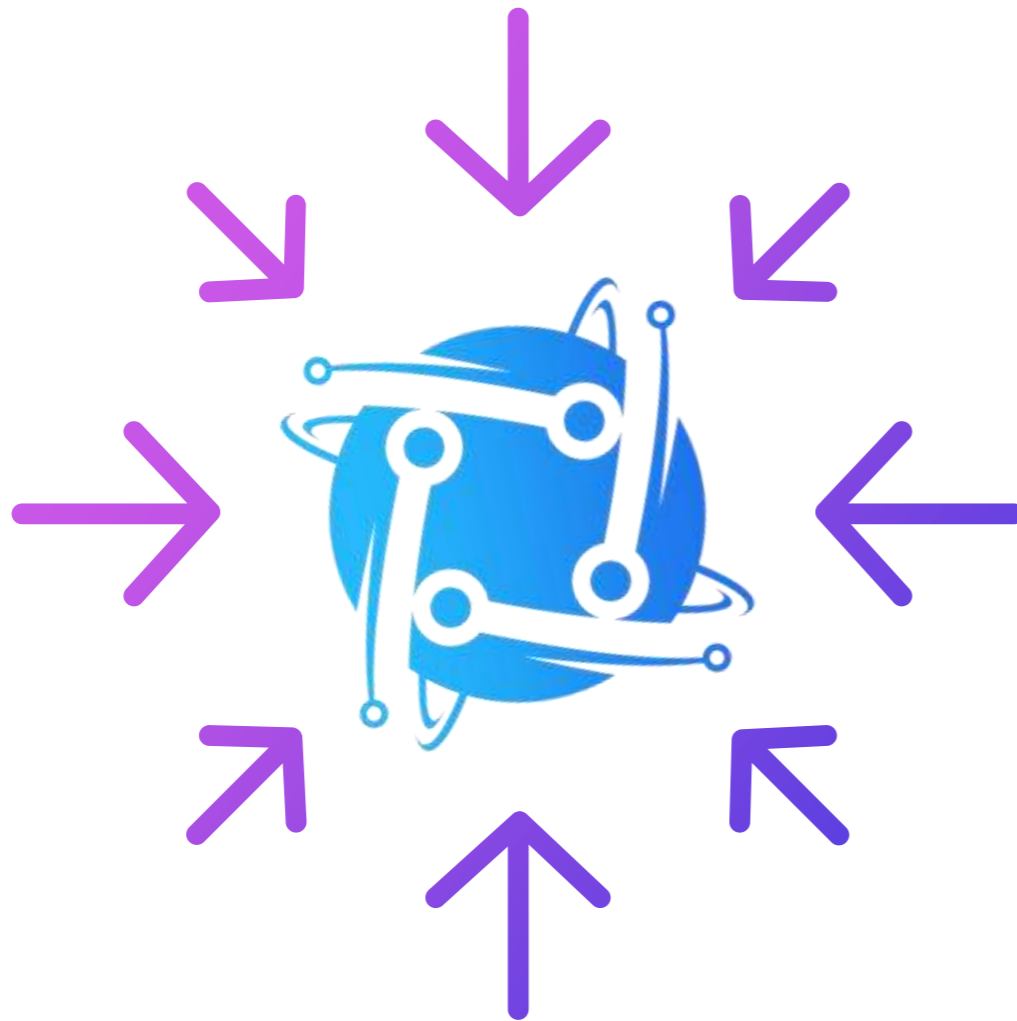
Above images are actual snapshots of the current live website of the project.

Website was registered on 07/11/2022, registration expires 07/11/2023.

**X** This meets the 3 year minimum we like to see on new projects.



## Website Part 2 – Checklist



- ✓ Mobile Friendly
- ✓ No JavaScript Errors
- ✓ Spell Check
- ✓ SSL Certificate

The website contained no JavaScript errors. No typos, or grammatical errors were present, and we found a valid SSL certificate allowing for access via https.

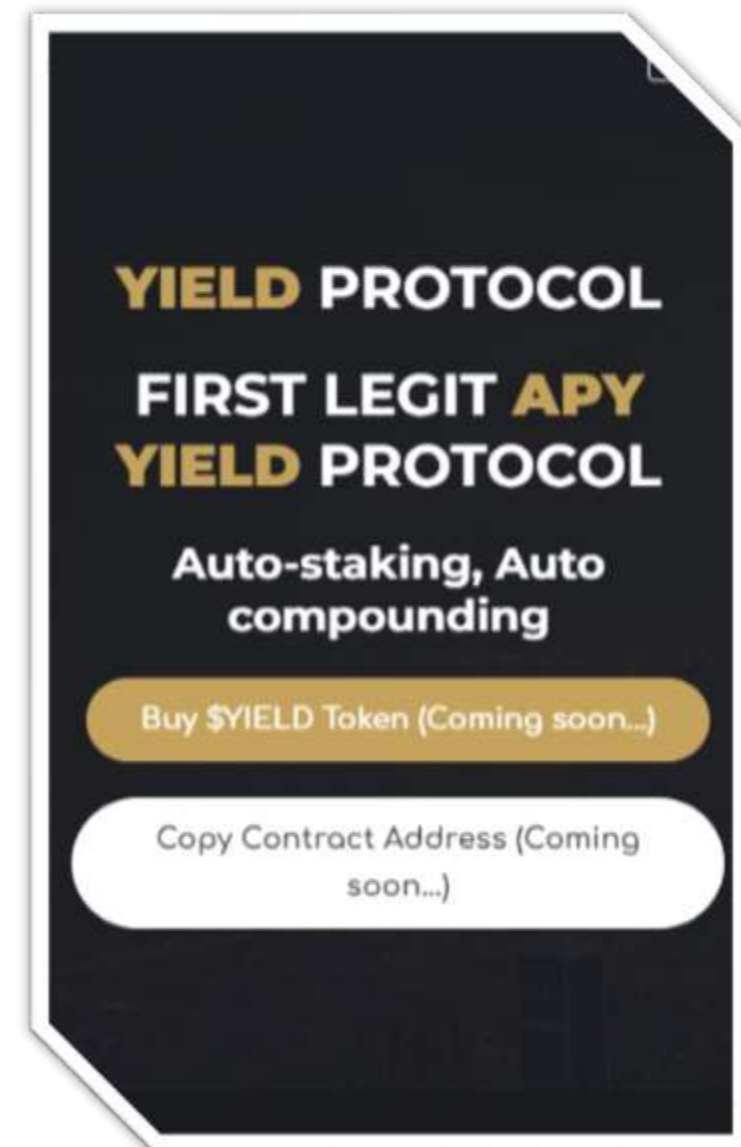
No additional issues were found on the website.



# Website Part 3 – Responsive HTML5 & CSS3

No issues were found on the Mobile Friendly check for the website. All elements loaded properly and browser resize was not an issue. The team has put a considerable amount of thought and effort into making sure their website looks great on all screens.

No severe JavaScript errors were found. No issues with loading elements, code, or stylesheets.



# Website Part 4 (GWS) – General Web Security



## SSL CERTIFICATE

A valid SSL certificate was found. Details are as follows:

Offered to: yield-token.com

Issued by: Sectigo RSA

Valid Until: 07/12/2023



## CONTACT EMAIL

A valid contact email was found on the official website. Contact email is listed as shown below:

Contact

N/A



## SPAM / MALWARE / POPUPS

No malware found

No injected spam found

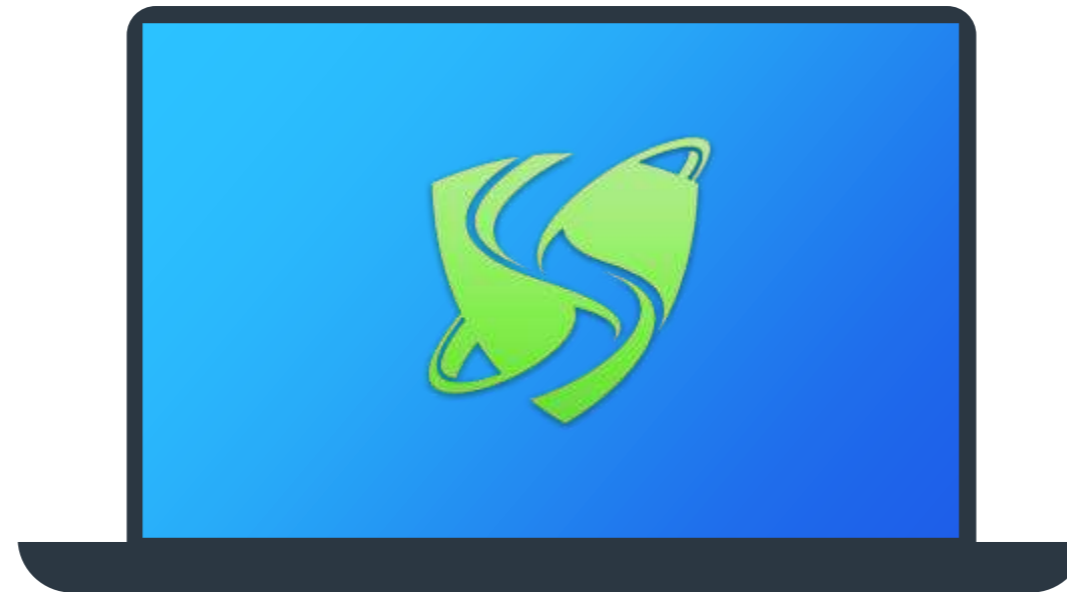
No internal server errors

No popups found

Domain is marked clean by Google, McAfee, Sucuri Labs, & ESET



# Social Media



We were able to locate a variety of Social Media networks for the project.

All links have been conveniently placed below.



[Twitter](#)



[Telegram](#)

**X** At least 3 social media networks were found.

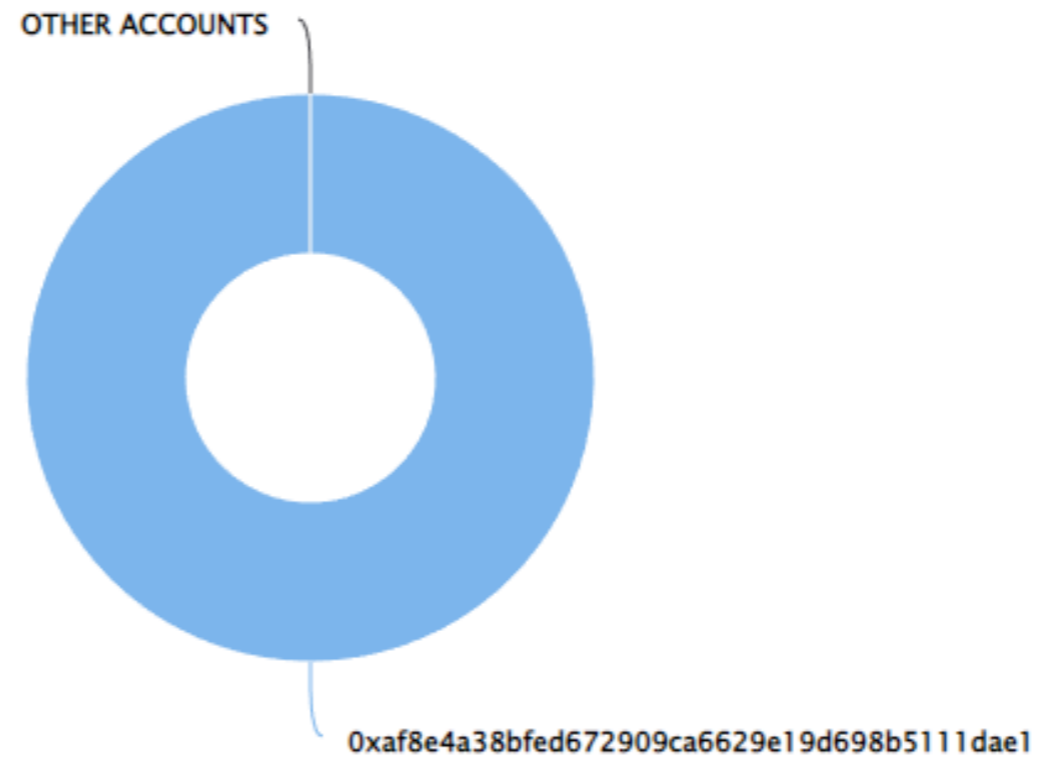
# Top Token Holders

The entire supply was in one wallet at the time of audit. We expect this to change as the project goes through initial distribution phases. Please use the link below to view the most up-to-date holder information.

[Click here to view the most up-to-date list of holders](#)

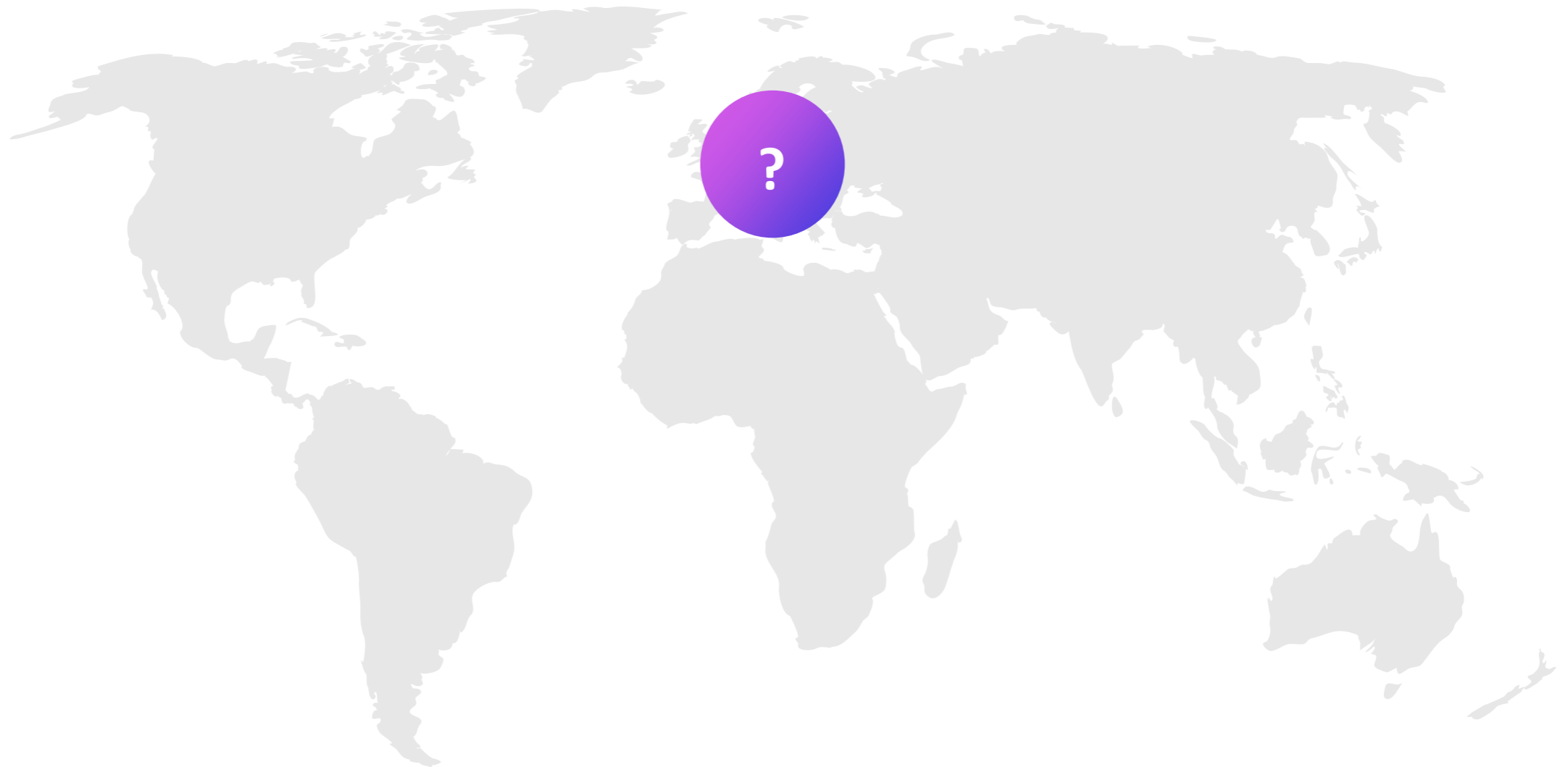
## Yield Protocol Top 100 Token Holders

Source: BscScan.com



# Location Audit

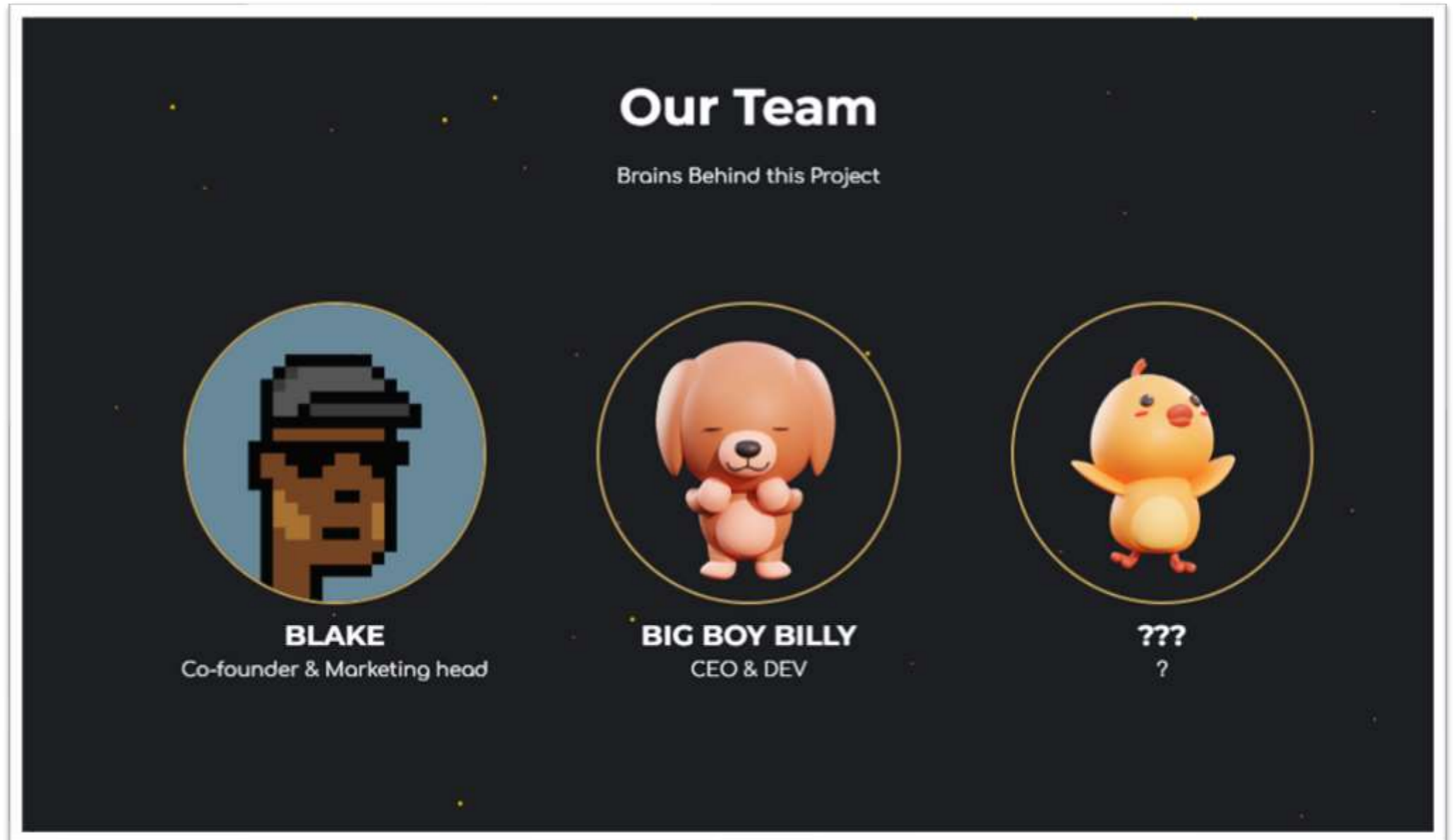
We were unable to identify a primary location for the project at this time or a location has not been declared.





# Team Overview

The following information about the team was located on the projects website.



# Roadmap

*A roadmap was found on the official website, we have conveniently placed it on this page for your viewing.*



# Disclaimer



The opinions expressed in this document are for general informational purposes only and are **not intended to provide specific advice or recommendations for any individual or on any specific investment**. It is only intended to provide education and public knowledge regarding projects. This audit is only applied to the type of auditing specified in this report and the scope of given in the results. Other unknown security vulnerabilities are beyond responsibility. Dessert Finance only issues this report based on the attacks or vulnerabilities that already existed or occurred before the issuance of this report. For the emergence of new attacks or vulnerabilities that exist or occur in the future, Dessert Finance lacks the capability to judge its possible impact on the security status of smart contracts, thus taking no responsibility for them. The smart contract analysis and other contents of this report are based solely on the documents and materials that the contract provider has provided to Dessert Finance or was publicly available before the issuance of this report (issuance of report recorded via block number on cover page), if the documents and materials provided by the contract provider are missing, tampered, deleted, concealed or reflected in a situation that is inconsistent with the actual situation, or if the documents and materials provided are changed after the issuance of this report, Dessert Finance assumes no responsibility for the resulting loss or adverse effects. Due to the technical limitations of any organization, this report conducted by Dessert Finance still has the possibility that the entire risk cannot be completely detected. Dessert Finance disclaims any liability for the resulting losses.

Dessert Finance provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Even projects with a low risk score have been known to pull liquidity, sell all team tokens, or exit-scam. Please exercise caution when dealing with any cryptocurrency related platforms.

The final interpretation of this statement belongs to Dessert Finance.

Dessert Finance highly advises against using cryptocurrencies as speculative investments and they should be used solely for the utility they aim to provide.



# Thank You

DESSERT FINANCE PROJECT AUDIT HAS BEEN COMPLETED FOR YIELD PROTOCOL (YLD) AT BLOCK NUMBER: **19694287**

**THIS AUDIT IS ONLY VALID IF VIEWED ON [HTTPS://WWW.DSSERTSWAP.FINANCE](https://www.dessertswap.finance)**

[www.dessertswap.finance](http://www.dessertswap.finance)  
<https://t.me/dessertswap>