CRYPTOIZ RESEARCH

Smart Contract Security Audit

YODESWAP

September 14, 2022

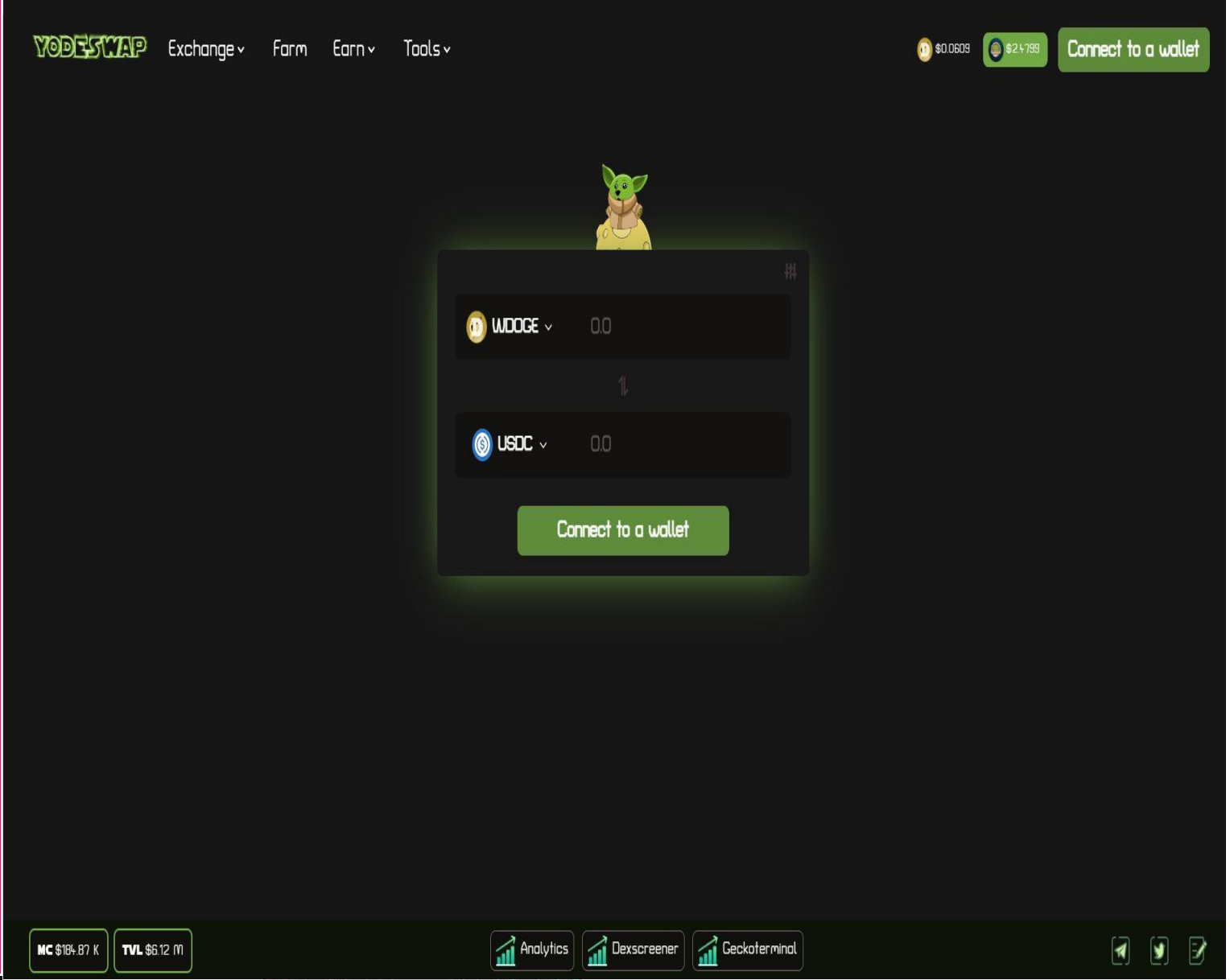
DISCLAIMER

This report presents findings based on our limited project analysis, related to cybersecurity vulnerabilities and issues in smart contract-based frameworks and algorithms, social media and websites as a whole, as well as details of team transparency from those in this report. To get a full picture of our analysis, it is very important that you read the full report. While we have done our best to analyze and produce this report, it should be noted that you should not rely on this report and cannot claim us based on what is said or is not reliable for you, or how we create it, and is important to us. You carry out your own independent investigation before making any decisions. We go into more detail about this in the disclaimer below - be sure to find out in full. To mitigate this risk, it is necessary to conduct a Smart Contract Security Audit, as well as transparency to investors and the public. This audit has been prepared to review key aspects of the project to help investors make informed decisions during their research process. Security is very important in the blockchain space. Our comprehensive smart contract auditing service helps everyone from startups to enterprises run and maintain their blockchain applications. This report does not provide any warranty or guarantee. regarding the completely bug-free nature of the technology analyzed, also gives no indication owner of technology, business model or legal compliance. This report cannot be used in any way to make decisions around investment or involvement with any particular project. This report does not in any way provide investment advice, or should be used as investment advice of any kind. This The report represents an extensive assessment process that intends to help our customers improve the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology

Project Summary

Project Name	Yodeswap
Website	https://yodeswap.dog/
Description	The all-in-one Defi solution provides an array of services and features supporting the DeFi and Web3 spaces, including crypto swaps, staking, and yield farming, and serves as a launch platform for new and exciting projects built on the Dogechain Network.
Platfrom	Dogechain
Network URL	https://rpc.yodeswap.dog/
Chain ID	2000
Language	Solidity
Token	YodeDEX Token
Max Supply	150000000
Symbol	Yode
Token type	ERC-20
Decimals	18
YodeDEX	0x6FC4563460d5f45932C473334d5c1C5B4aEA0E01
Factory	0xAaA04462e35f3e40D798331657cA015169e005d7
Router	0x72d85Ab47fBfc5E7E04a8bcfCa1601D8f8cE1a50
Yodechef	0xf7b1150cb31488bde3eB3201e0FDF1Bd54799712
Timelock	0x31d04A15bc6433cf531EFf681a4056042BCA3E0a
Liquidity provided TX	0x57f15bada14fdf29ff538568219977b277bebecc07
LP Locked 6 Month TX	0x4cb09d6cf30180fce6fed67c80a737b01f018d5be6

Feature YodeSwap



YodeSwap is one of the first automated market-making (AMM), decentralized exchanges (DEX) for the Dogechain Network. The all-in-one Defi solution provides an array of services and features supporting the DeFi and Web3 spaces, including crypto swaps, staking, and yield farming, and serves as a launch platform for new and exciting projects built on the DogeChain Network.

-Earn $DC, Staking, Partner Stake
-Yield Farming
-Swap,Liquidity,Zappero,Import Pool and Locker Token

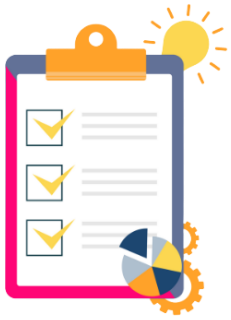
Release Date: $YODE Launched on 16th August 2022 , No presale or premint, Initial liquidity provided with 182,396 DOGE and 16,000 YODE, 1 YODE = $1 or 1 YODE = 11.39975 DOGE.

Category: DeFi

Audit Process Summary

Audit Details

Comprehensive security assessment of your smart contract and website to identify vulnerabilities. Our audit tools include a logical review of your code, with a mathematical approach to ensure your program is working as intended.



Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, To mitigate this risk, it is necessary to conduct a Smart Contract Security Audit, as well as for transparency to investors and the public.

Audit Code Method

- Application security checklist
- Detail information vulnerability
- Accuracy and Readability
- Back-doors and Exploits
- Manual review
- Automatic review
- Unit testing

Tools

- Cryptoiz Tools
- Foundry
- Solc
- Solmate
- Solhint
- Hardhat

Risk Classification

		CODE
HIGH	Problems at this level to smart contract performance/function can be exploited and should be fixed ASAP	#H1-10
MEDIUM	This issue may interfere with certain functions, causing the smart contract to not work properly and system functionality can be improved at a later date.	#M1-10
LOW	functionality is not affected hence bug severity is low. Issues on this level are minor details and warnings that can remain unfixed but would be better fixed.	#L1-10
INFORMATIONAL	Information level is to offer suggestions for improvement of efficacity or security for features with a risk free factor.	#N/A

Issues Checking In Vulnerability Scope

Contract Name	Low	Medium	High	Informational	CODE
DCRewards.sol	0	1	0	0	#S-DC1
Launchpool.sol	1	0	0	0	#S-L2
StakingService.sol	1	0	0	0	#S-S3
xYodeDEXToken.sol	1	0	0	1	#S-X4
YodeDEXToken.sol	0	1	0	1	#S-Y5
Uniswapv2/interfaces					
IERC20.sol	0	0	0	0	N/A
IWWDOGE.sol	0	0	0	0	
IYodedexCallee.sol	0	0	0	0	
IYodedexERC20.sol	0	0	0	0	
IYodedexFactory.sol	0	0	0	0	
IYodedexPair.sol	0	0	0	0	
IYodedexRouter01.sol	0	0	0	0	
IYodedexRouter02.sol	0	0	0	0	
Uniswapv2/interfaces/v1					
IUniswapV1Exchange.sol	0	0	0	0	N/A
IUniswapV1Factory.sol	0	0	0	0	
Uniswapv2/lib					
ERC20.sol	0	0	0	0	N/A
ERC20Detailed.sol	0	0	0	0	
IERC20.sol	0	0	0	0	
IYodedexFactory.sol	0	0	0	0	
TransferHelper.sol	0	0	0	0	
Uniswapv2/lib/GSN					
Context.sol	0	0	0	0	N/A
Uniswapv2/lib/access					
Manageable.sol	0	0	0	0	N/A
Ownable.sol	0	0	0	0	
Uniswapv2/lib/math/					
SafeMath.sol	0	0	0	0	N/A
Uniswapv2/lib/proxy/					
Initializable.sol	0	0	0	0	N/A
Proxy.sol	0	0	0	0	
ProxyAdmin.sol	0	0	0	0	
TransparentcProxy.sol	0	0	0	0	
UpgradeableProxy.sol	0	0	0	0	

Uniswapv2/lib/token/BEP20					
BEP20.sol	0	0	0	0	N/A
IBEP20.sol	0	0	0	0	
SafeBEP20.sol	0	0	0	0	
Uniswapv2/lib/utils					
Address.sol	0	0	0	0	N/A
AddressStringUtil.sol	0	0	0	0	
Create2.sol	0	0	0	0	
EnumerableSet.sol	0	0	0	0	
FixedPoint.sol	0	0	0	0	
Memory.sol	0	0	0	0	
PairNamer.sol	0	0	0	0	
ReentrancyGuard.sol	0	0	0	0	
SafeBEP20Namer.sol	0	0	0	0	
TransferHelper.sol	0	0	0	0	
Uniswapv2/libraries					
IYodedexPair.sol	0	0	0	0	N/A
Math.sol	0	0	0	0	
SafeMath.sol	0	0	0	0	
UQ112x112.sol	0	0	0	0	
YodedexLibrary.sol	0	0	0	0	
Uniswapv2/mathUpdated					
SafeMath.sol	0	0	0	0	N/A
Uniswapv2/					
Multicall.sol	0	0	0	0	N/A
Multicall2.sol	0	0	0	0	
WWDOGE.sol	0	0	0	0	
YodedexERC20.sol	0	0	0	0	
YodedexFactory.sol	0	0	0	0	
YodedexPair.sol	0	0	0	0	
YodedexRouter.sol	0	0	0	0	
yield-farm/					
IYodeChef.sol	0	0	0	0	N/A
IYodedexPair.sol	0	0	0	0	
YodeChef.sol	0	0	0	0	
YodeChefV2.sol	0	0	0	0	
yield-farm/libraries					
BoringERC20.sol	0	0	0	0	N/A
IBoringERC20.sol	0	0	0	0	
yield-farm/rewarders/					
IMultipleRewards.sol	0	0	0	0	N/A
MultipleRewards.sol	0	0	0	0	
Total	3	2	0	2	

Compiling Files Solidity Result

```
[⠒] Compiling...
[⠒] installing solc version "0.6.6"
[⠒] Successfully installed solc 0.6.6
[⠒] installing solc version "0.4.26"
[⠒] Successfully installed solc 0.4.26
[⠒] installing solc version "0.5.16"
[⠒] Successfully installed solc 0.5.16
[⠒] Compiling 1 files with 0.4.26
[⠒] Compiling 26 files with 0.6.6
[⠒] Compiling 206 files with 0.8.16
[⠒] Compiling 9 files with 0.5.16
[⠒] Solc 0.4.26 finished in 86.28ms
[⠒] Solc 0.5.16 finished in 775.55ms
[⠒] Solc 0.6.6 finished in 1.36s
[⠒] Solc 0.8.16 finished in 20.94s
Compiler run successful
```

Total File
Compiling

Analyzed 120 contracts

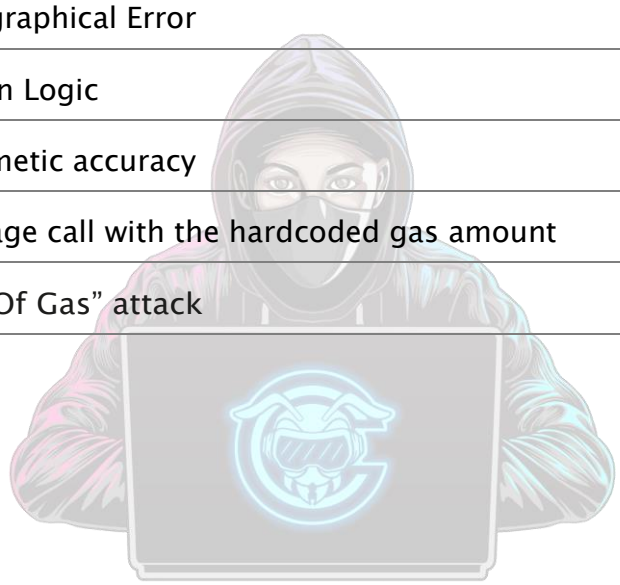
242 Files Result
- 1 Files with 0.4.26 version
- 26 Files with 0.6.6 version
- 206 Files with 0.8.16 version
- 9 Files with 0.5.16 version

Issues Checking Status Manual Review

CODE	Issues Description	Result
#CTZ-001	Compiler Errors / Warnings	Passed
#CTZ-002	Gas Optimization	Passed
#CTZ-003	DoS with block gas limit.	Passed
#CTZ-004	Floating Pragma	Passed
#CTZ-005	DoS with Revert.	Passed
#CTZ-006	Possible delays in data delivery	Passed
#CTZ-007	Timestamp dependence and Block timestamp	N/A
#CTZ-008	Oracle calls.	Passed
#CTZ-009	Outdated Compiler Version	Passed
#CTZ-010	Signature Malleability	Passed
#CTZ-011	Arbitrary from in transferFrom	N/A
#CTZ-012	Modifying storage array by value	Passed
#CTZ-013	Incorrect shift in assembly	Passed
#CTZ-014	Multiple constructor schemes	Passed
#CTZ-015	Name reused	Passed
#CTZ-016	Protected Variables	Passed
#CTZ-017	Public mappings with nested variables	Passed
#CTZ-018	Right-to-Left-Override character	Passed
#CTZ-019	State variable shadowing	Passed
#CTZ-020	Functions Kill / Selfdestruct	Passed
#CTZ-021	Uninitialized state variables	Passed
#CTZ-022	Uninitialized storage variables	Passed
#CTZ-023	Upgradeable contract	Passed
#CTZ-024	Arbitrary from in transferFrom used with permit	N/A
#CTZ-025	Functions that send Ether to arbitrary destinations	N/A

#CTZ-026	Array Length Assignment	Passed
#CTZ-027	Controlled Delegatecall	Passed
#CTZ-028	Payable functions using delegatecall inside a loop	Passed
#CTZ-029	msg.value inside a loop	Passed
#CTZ-030	Reentrancy vulnerabilities	Passed
#CTZ-031	Storage Signed Integer Array	Passed
#CTZ-032	Unchecked transfer	Passed
#CTZ-033	Weak PRNG	N/A
#CTZ-034	Dangerous enum conversion	Passed
#CTZ-035	Incorrect erc20 interface	Passed
#CTZ-036	Incorrect erc721 interface	N/A
#CTZ-037	Dangerous strict equalities	N/A
#CTZ-038	Contracts that lock Ether	Passed
#CTZ-039	Deletion on mapping containing a structure	Passed
#CTZ-040	State variable shadowing from abstract contracts	Passed
#CTZ-041	Tautology or contradiction	Passed
#CTZ-042	Write after write	Passed
#CTZ-043	Misuse of a Boolean constant	Passed
#CTZ-044	Constant functions using assembly code	Passed
#CTZ-045	Constant functions changing the state	Passed
#CTZ-046	Divide before multiply	N/A
#CTZ-047	Dangerous usage of tx.origin	N/A
#CTZ-048	Unchecked low-level calls	Passed
#CTZ-049	Unchecked Send	N/A
#CTZ-050	Uninitialized local variables	Passed
#CTZ-051	Incorrect modifier	Passed
#CTZ-052	Builtin Symbol Shadowing	Passed
#CTZ-053	Local variable shadowing	N/A
#CTZ-054	Uninitialized function pointers in constructors	Passed

#CTZ-055	Declaration usage	Passed
#CTZ-056	Calls inside a loop	Passed
#CTZ-057	Missing events access control	Passed
#CTZ-058	Missing events arithmetic	Passed
#CTZ-059	Dangerous unary expressions	Passed
#CTZ-060	Missing zero address validation	Passed
#CTZ-061	Boolean equality	Passed
#CTZ-062	Unindexed ERC20 event parameters	Passed
#CTZ-063	Function Initializing State	Passed
#CTZ-064	Dead-code	Passed
#CTZ-065	Typographical Error	Passed
#CTZ-066	Design Logic	Passed
#CTZ-067	Arithmetic accuracy	Passed
#CTZ-068	Message call with the hardcoded gas amount	Passed
#CTZ-069	“Out Of Gas” attack	Passed



Unit Testing File Vulnerability Scope

#S-DC1 and #M-5 | #CTZ-037

```
Findings:
❌ DCYODEStaking.updateReward(IERC20) (contracts//#S-DC1.sol:L375-396) uses a dangerous strict equality:
    • _rewardBalance == lastRewardBalance[_token] || _totalxYODE == 0 (contracts/#S-DC1.sol#L386)
```

Description

It checks if the reward balance is the same as the last reward balance, if so, it returns. Use of strict equalities that can be easily manipulated by an attacker.

Recommendation

Don't use strict equality to determine if an account has enough Ether or tokens.

#S-Y5 and #M-7 | #CTZ-049

```
Findings:
❌ YodeDEXToken.rescueTokens(IERC20,uint256) (contracts/#S-Y5:L37-42) ignores return value by
token.tansfer(msg.sender,value) (contracts/#S-Y5#L41)
```

Description

It allows the owner of the token to transfer the tokens to the person who called the function, The return value of an external transfer/transferFrom call is not checked

Recommendation

Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

MANUAL FUNCTION ANALYSIS

Function Name	Details	Description
DOMAIN_SEPARATOR (byte32 / Keccak)	0x46500252b48d281f19c58ecc5c101465953a030393e87f4c95486b7f34b3e1a5	
MINTER_ROLE (byte32 / Keccak)	0x9f2df0fed2c77648de5860a4cc508cd0818c85b8b8a1ab4ceeef8d981c8956a6	
PAUSER_ROLE(byte32 / Keccak)	0x65d7a28e3265b37a6474929f336521b332c1681b933f6cb9f3376673440d862a	
RESCUER_ROLE(byte32 / Keccak)	0xcf6f9f892731e14b8859835f2ff35575f447fb501f46243c4eb8bac19e31a050	
feeTo factory	0x2816ac29a2240f8cb5ee602d55ade39e10e5ed2b	
feeToSetter factory	0x2a2e3486204c9eeeab2bef8faa3356bc19e9db6f	
swapFee	0.5% default and max_SetSwapFee <= 1000	1. The function checks that the fee is greater than 0 and less than 1000. 2. The function checks that the sender is the factory address. 3. The function sets the swap fee. 4. The function sets the dev fee.
devFee	0.33% default setDevFee N/A	
marketingAddress	0x2816ac29a2240f8cb5ee602d55ade39e10e5ed2b	
Minter	MINTER_ROLE (byte32 / Keccak)	1. The function is only accessible to the MINTER_ROLE role. 2. The function checks that the amount to be minted is less than the maximum total supply. 3. The function calls the private _mint function.
Update Pool	1. The function first checks if the current block number is less than the last reward block number. If so, it returns. 2. It then checks if the total LP supply is 0 or the alloc point is 0. If so, it returns. 3. It then calculates the multiplier for the current block. 4. It then calculates the yode reward for the current block. 5. It then mints the yode reward 40 to the marketingAddress.	6. It then mints the yode reward to the pool owner. 7. It then calculates the LP percent. 8. It then calculates the LP's share of the yode reward. 9. It then updates the last reward block number.
YodeChef	uint16 public constant MAXIMUM_DEPOSIT_FEE_RATE = 1000; // 10% uint256 public constant MAXIMUM_HARVEST_INTERVAL = 90 days;	

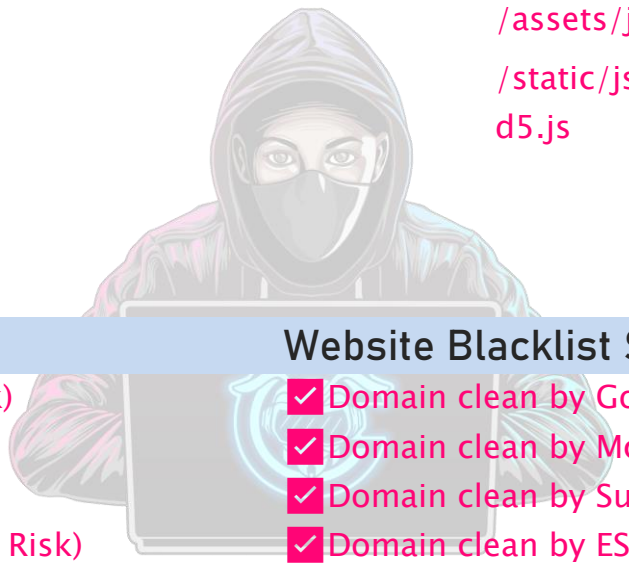
Statistics Token

Holders	2087 Addresses Snapshot 13 September 2022
Transfer	247,892 Transfers Snapshot 13 September 2022
Top 1 Holders	0xc09F5b24C7a40b6AB4a21227FCFB9bebAa9127Dd 93% Tokens (**VestingYode**)
LP address	**0x6fc4563460d5f45932c473334d5c1c5b4aea0e01**

Website Summary

Website URL	UI/UX	Whitepaper	Roadmap	Performance
https://yodeswap.dog/	90%	No whitepaper. ⚠	Yes	90%

SSL	Hosting	Server	Javascript include	Iframe include
Yes	N/A	Vercel	/assets/js/jquery-3.3.1.min.js /assets/js/bootstrap.min.js /assets/js/script.js /assets/js/scroll.js /static/js/main.fd0ced d5.js	No iframes found.



Website Malware & Security	Website Blacklist Status
✓ No malware detected by scan (Low Risk)	✓ Domain clean by Google Safe Browsing
✓ No injected spam detected (Low Risk)	✓ Domain clean by McAfee
✓ No defacements detected (Low Risk)	✓ Domain clean by Sucuri Labs
✓ No internal server errors detected (Low Risk)	✓ Domain clean by ESET
	✓ Domain clean by PhishTank
	✓ Domain clean by Yandex
	✓ Domain clean by Opera

About Us

CRYPTOIZ RESEARCH was established in October 2018 with a focus on media education, community and brand awareness for crypto projects in Indonesia. The first website we used was cryptoiz.net, now we are transforming into cryptoizresearch.com. A comprehensive campaign to improve a positive image, educate, and properly disseminate information through the Cryptoiz Research ecosystem regarding developments in all fields of Blockchain Technology, Cryptocurrencies, NFTs, and many more.

AUDIT.CRYPTOIZRESEARCH.COM

CRYPTOIZ RESEARCH

CRYPTOIZRESEARCH.COM

@CRYPTOIZINDONESIA

NEWS.CRYPTOIZRESEARCH.COM

@CRYPTOIZRESEARCH

STORE.CRYPTOIZRESEARCH.COM

@CRYPTOIZ

LMO.CRYPTOIZRESEARCH.COM

@CRYPTOIZ_IDN