

PEX Audit

Pure



February 26th 2023

Audit Details

Pure

Auditor's - Papa Exchange 

Website - itspurecoin.com



Blockchain - Binance Smart Chain





Disclaimer

PapaExchange LLP will be referred to as PEX per this report

- **PEX** audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.
- **PEX** does not provide any warranty on its released reports. We should not be used as a decision to invest into an audited project please do your own research. **PEX** provides transparent reports to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within its Smart Contract.
- Each company or project shall be liable for its own security flaws and functionalities. **PEX** presence is to analyze, audit and assess the client's smart contract's code.

Scope of Work

- The main focus of this report/audit, is to document an accurate assessment of the condition of the smart contract and whether it has any security flaws in the implementation of the contract. **PURE** team agreed and provided us with the files that needed to be tested (Through Github, Bscscan, files, etc.). **PEX** will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository where available, which has been provided by the project. Code is reviewed manually and with the use of software using industry best practices.



Background

- **PEX** was commissioned by **PURE** to perform an audit of smart contract:
 - Contract Address - **0xcb9a965ea4aff34f83fe3dac339d60d0c1251a0e**

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.

Pure

Pure is a revolutionary new currency and CRM system allowing small businesses to manage their entire business at absolutely no cost while accepting crypto - **and cutting traditional processing fees in half!**

Social Media

Twitter - <https://twitter.com/itspurecoin>

Telegram - <https://t.me/purecoinofficial>

YouTube - <https://www.youtube.com/channel/UCGmgExHq4HNDRuWkAw3JALA>



Contract Details

Project Name - Pure

Token Description - Utility Token

Compiler Version - v0.8.17

Current Holders - 111 Addresses

Current Transaction Count - 1028 Transfers

Total Supply - 100,000,000 Pure Tokens

Token Ticker - PURE

Decimals - 18

Top 100 Holder % - 100% of Tokens held by Top 100

LP Lock - 100% of LP is locked on PinkLock

Contract Address

0xcb9a965ea4aff34f83fe3dac339d60d0c1251a0e

Contract Deployer Address

0xd042667E10C9AE56959bC89C47f09EC395fCc910

Contract Owner Address

0xd61ede44750a42671d9a25f6b1540a19170c7a39

KYCd by - Fuddoxx

Launch Type - Private Sale/Fair Launch

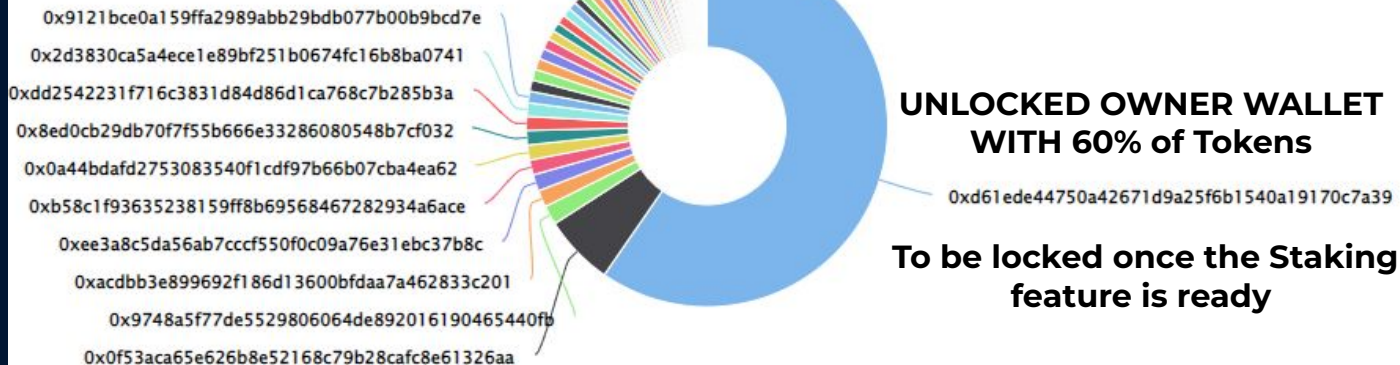
Top 100 Holders

Top 100 Holder Dominance is 100%



Pure Coin Top 100 Token Holders

Source: BscScan.com



A total of 99,997,586.77 tokens held by the top 100 wallets from the total 100 Million token supply

Pure LP Token Holders

1. **0x407993575c91ce7643a4d4cCACc9A98c36eE1BBE - 100% locked on PinkLock until May 21st 2023**



Owner Privileges/Fees

Privileges

Unlocked owners wallet with **60%** total supply **to be locked** once Staking platform is complete

Ownership has **NOT** been renounced. The owner has privileges and has authority to make some changes now. Owner entitled to **pause/resume Trading at any time**, **cooldown trading can be enabled**, **can limit/maximize trade limit and change Tax fees.**

Fees

Buy - 3% Sell - 12.5%

Owner must keep fees at 20% or lower. This is below our recommended percentage of 25%.

Adjustable Functions

1. addExcludeFromLimits
2. airdropToWallets
3. approve
4. burnTokens
5. decreaseAllowance
6. disableTransferDelay
7. enableTrading *
8. excludeFromFees
9. excludeFromMaxTransaction
10. forceSwapback
11. increaseAllowance
12. removeExcludedFromLimits
13. removeLimits
14. removeSellLimits
15. renounceOwnership *
16. setAutomatedMarketMakerPair
17. setDevAddress
18. setGlobalLimit
19. setGlobalLimitPeriod
20. setGlobalLimitsActiveStatus
21. setLimits *
22. setOperationsAddress
23. setPriceImpactLimit
24. transfer
25. transferForeignToken
26. transferFrom
27. transferOwnership
28. updateBuyFees *
29. updateMaxBuyAmount
30. updateMaxSellAmount
31. updateSellFees *
32. updateSwapTokensAtAmount
33. withdrawStuckETH

Weakness/Vulnerabilities

SCAN RESULTS

SWC-129 —> Unencrypted Private Data On-Chain = **PASSED**

SWC-130 —> Code With No Effect = **PASSED**

SWC-131 —> Message Call with Hardcoded Gas Amount = **PASSED**

SWC-132 —> Hash Collisions with Multiple Variable Length Arguments = **PASSED**

SWC-133 —> Unexpected Ether Balance = **PASSED**

SWC-134 —> Presence of Unused Variables = **PASSED**

SWC-135 —> Right-to-Left Override Control Character {U+202E} = **PASSED**

SWC-136 —> Typographical Error = **PASSED**

Weakness/Vulnerabilities

CONTINUED

SWC-119 —> Shadowing State Variables = **PASSED**

SWC-120 —> Weak Source of Randomness From Chain Attributes = **LOW ISSUE**

SWC-121 —> Missing Protection Against Signature Replay Attacks = **PASSED**

SWC-122 —> Lack of Proper Signature Verification = **PASSED**

SWC-123 —> Requirement Violation = **PASSED**

SWC-124 —> Write to Arbitrary Storage Location = **PASSED**

SWC-125 —> Incorrect Inheritance Order = **PASSED**

SWC-126 —> Insufficient Gas Griefing = **PASSED**

Weakness/Vulnerabilities

CONTINUED

SWC-127 → Arbitrary Jump with Function Type Variable = **PASSED**

SWC-128 → DoS with Block Gas Limit = **PASSED**

SWC-113 → DoS with Failed Call = **PASSED**

SWC-114 → Transaction Order Dependence = **PASSED**

SWC-115 → Authorization Through Tx. Origin = **LOW ISSUE**

SWC-116 → Block Values as a Value for Time = **PASSED**

SWC-117 → Signature Malleability = **PASSED**

SWC-118 → Incorrect Constructor Name = **PASSED**

Weakness/Vulnerabilities

CONTINUED

SWC-105 → Unprotected Ether Withdrawal = PASSED

SWC-106 → Unprotected SELF DESTRUCT Instruction = PASSED

SWC-107 → Reentrancy = PASSED

SWC-108 → State Variable Default Visibility = PASSED

SWC-109 → Uninitialized Storage Pointer = PASSED

SWC-110 → Assert Violation = PASSED

SWC-111 → Use of Deprecated Solidity Functions = PASSED

SWC-112 → Delegate Call to Untrusted Callee = PASSED

Weakness/Vulnerabilities

MythX passing

SWC-101 → Integer Overflow and Underflow = **PASSED**

SWC-102 → Outdated Compiler Version = **PASSED**

SWC-103 → Floating Pragma = **PASSED**

SWC-104 → Unlocked Call Return Value = **PASSED**

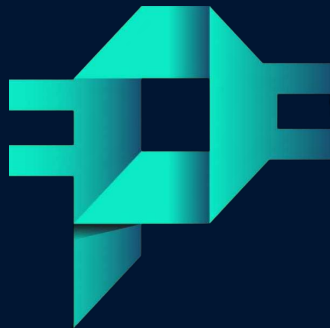
Low issue = Low-level weakness/vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution.

SOLHINT LINTER, Solidity Static Analysis using REMIX IDE **did not find** any serious issues.

Overall Assessment

Satisfactory

Pure has successfully passed the Pex Audit



Closing Notes

Whilst there are limitless ownable callable functions that have the potential to be dangerous, they are not overtly so. Trust in the team would mitigate many of these risks. Please make sure you do your own research. If in doubt please contact the project team.

Always make sure to inspect **all values and variables**.

This includes, but is not limited to: • Ownership • Proper Ownership Renouncement (if any) • Taxes • Transaction/Wallet Limits • Token Distributions • Timelocks • Liquidity Locks • Any other owner-adjustable settings or variables.

