PEX Audit

The Big Experiment

February 18th 2023

PEX
EST 2021
AUDIT

Audit Details

The Big Experiment

Auditor's - Papa Exchange

Website - www.bigxtoken.io

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.
  Big X 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 **BIG X** to perform an audit of smart contract:
  ● Contract Address
  0xC30f68eae0Ce9Bce279f4006eb4d456E6e2ABda6
  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.

EST 2021
AUDIT

The Big Experiment

The Big Experiment is a community focused deflationary project based on the Binance Smart Chain (BSC) aimed at solving environmental impacts traditionally associated with the mining and farming of crypto assets. We're setting out to create balance in the crypto space. A place where all investors are rewarded, simply for holding.

Social Media

Twitter - https://twitter.com/BigX_Official

Telegram - https://t.me/BigXOfficial

PFX EST 2021 AUDIT

Contract Details

Project Name - The Big Experiment

Token Description - Deflationary Token

Compiler Version - v0.8.9

Current Holders - 170 Addresses

Current Transaction Count - 2726

Total Supply - 1,000,000,000,000 Tokens

Token Ticker - BIGX

Decimals - 18

Top 100 Holder % - 96.06%

LP Lock - 86% locked for 6 months on Launch Lab Locker
https://locker.launchlab.online
13.5% locked for 6 months on Deep Lock IO
https://deeplock.io/lock/0xc5F7ABf09c80C76Ec0A6f0B0c94113036Ee2D677

Contract Address

0xC30f68eae0Ce9Bce279f4006eb4d456E6e2ABda6

Contract Deployer Address

0x314bfebc283d6d79dd535d8a023705f0551a5c85

Contract Owner Address

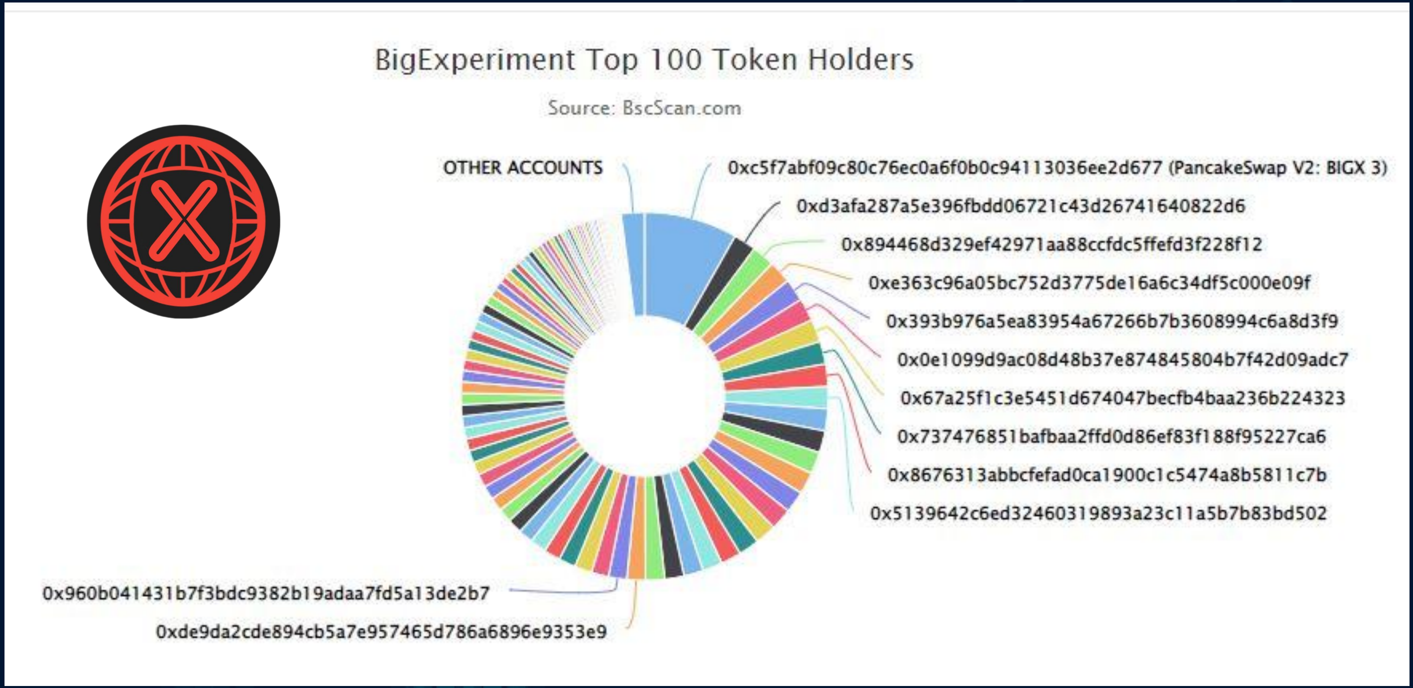
0x4fe2fbbf7389f16216ecd9dfd3c624f45b7661de

KYCd by - Fuddoxx

Launch Type - Stealth

Top 100 Holders

Top 100 Holder Dominance is 97.95%



BigExperiment Top 100 Token Holders

Source: BscScan.com

A total of 979,541,496,001.66 tokens held by the top 100 wallets from the total 1 trillion token supply

Big X LP TokenHolders

1. Launch Labs - 86%

2. Deep Lock - 13.5%

3. 0x4fe2fbbf7389f16216ecd9dfd3c624f45b7661d - 0.3%

4. 0x0ed943ce24baebf257488771759f9bf482c39706 - 0.2%

Owner Privilages/Fees

Privilages

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, change Buy/Sell fees, set true or false values and exclude rewards**.

Fees

Buy - 6% Sell - 6%

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

Adjustable Functions

(After Contract Deployment)

1. approve
2. claim
3. decreaseAllowance
4. disableTransferDelay
5. enableTrading *
6. excludeFromDividends
7. excludeFromFees
8. excludeFromMaxTransaction
9. excludeMultipleAccountsFromFees
10. includeInDividends
11. increaseAllowance
12. marketingTokens
13. processDividendTracker
14. removeLimits
15. renounceOwnership *
16. setAutomatedMarketMakerPair
17. transfer
18. transferFrom
19. transferOwnership
20. updateBuyFees *
21. updateClaimWait
22. updateGasForProcessing
23. updateMaxAmount
24. updateMaxWalletAmount
25. updateSellFees *
26. updateSwapEnabler
27. updateMarketingWallet
28. withdrawStuckEth
29. withdrawTokens

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 —> Righ-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

PFX EST. 2021 AUDIT

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

The Big Experiment 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.