PapaExchange

Not just a bunch of Dads

PapaExchange Audit for

Bear Cub Token

Audit Details

Prepared for: Bear Cub Token

Blockchain: Binance Smart Chain

Project website:
https://www.thebeartoken.com

Authors: PapaExchange Audit team

Date: 05/09/2022

Disclaimer

PapaExchange LLP 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.

PapaExchange LLP does not provide any warranty on its released reports.

PapaExchange LLP should not be used as a decision to invest into an audited project please do your own research. PapaExchange LLP 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.

PapaExchange LLP presence is to analyze, audit and assess the client's smart contract's code.

Each company or project shall be liable for its own security flaws and functionalities.

Scope of Work & Background

The main scope 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.

Bear CubToken team agreed and provided us with the files that needed to be tested (Through Github, Bscscan, files, etc.). PapaExchange 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

PapaExchange was commissioned by The Bear Cub Token to perform an audit of smart contract:

● Contract Address 0x7D0254D6226DeB51Af649A96D1F23754C18fcb75

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.

Token Description from Dev's

The Bear Cub Token is a Binance Smart Chain rewards and utility token and is the child token of The Bear Token.

Social Media Links

Telegram: https://t.me/thebeartoken

Twitter: https://twitter.com/TheBearToken

Facebook: N/A

Discord: N/A

Contracts details

Token contract details for 05/09/2022

Contract/Project name: Bear Cub

Description Utility and Reward Token

Compiler version: 0.7.6

Contract address: 0x7D0254D6226DeB51Af649A96D1F23754C18fcb75

Total supply: 2,000,000

Token ticker: CUB

Decimals: 9

Token holders at time of report: 235

Transactions count at time of report: 3,231

Top 100 holders dominance: 89.75%

Contract deployer address: 0xAe1465f22362738423869315c893D5AF9e73A3a9

Contract’s current owner address: 0xAe1465f22362738423869315c893D5AF9e73A3a9

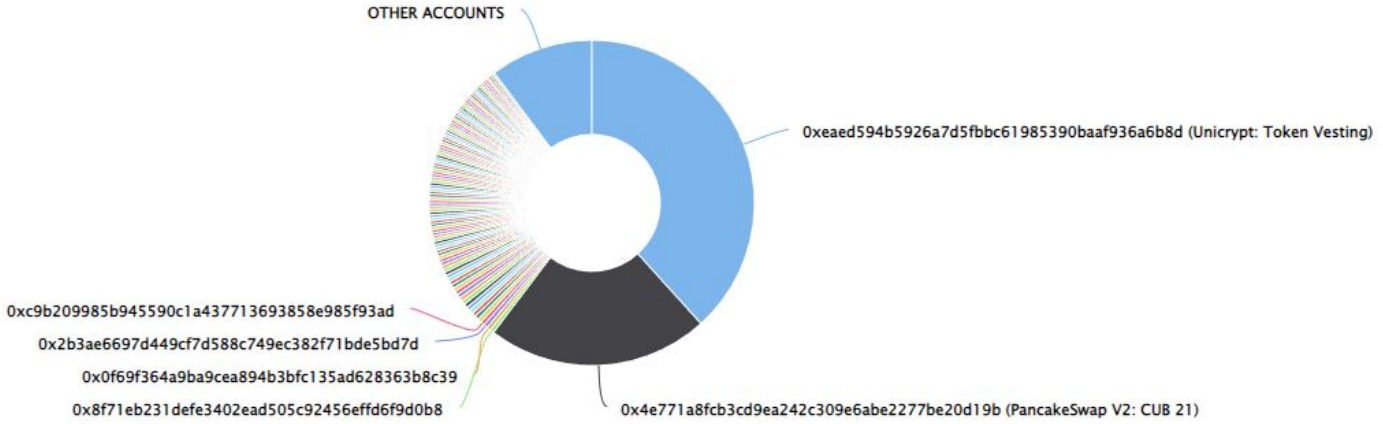
LP LOCK Mudra 1 month

Dev’s KYC Yes Fuddox (through previous projects)

Launch Type Fair launch

Bear Cub Top 100 Token Holders

Source: BscScan.com



(A total of 1,794,994.94 tokens held by the top 100 accounts from the total supply of 2,000,000.00 token)

Token name LP token holder

1. 0xae7e6cabad8d80f0b4e1c4dde2a5db7201ef1252 100% (Mudra Locked)

Contract write functions details

Owner privileges:

Ownership has not been renounced, although some privileges may be disabled in the fuyure, the owner has privileges, and has authority to make any changes now. Owner is entitled to Blacklist.

Current Fees: • Buy: 12% • Sell: 12% • Owner can not change fees above 33% (25% isPapa's recommended maximum and 50% would be a maximum for a satisfactory assessment).

All Write Functions of Contract that can be adjusted after the contract is deployed.

1. approve
2. approveMax
3. authorize
4. clearStuckBalance
5. clearStuckBalance_Sender
6. cooldownEnabled
7. enable_blacklist
8. manage_blacklist
9. multiTransfer
10. multiTransfer_fixed
11. removeFromBlacklist
12. renounceBlacklistAbility
13. setDistributionCriteria
14. setDistributorSettings
15. setFeeRecievers
16. setFees
17. setIsDividendExempt
18. setIsFeeExempt
19. setIsTimelockExempt
20. setIsTxLimitExempt
21. setMaxTxPercent_base1000
22. setMaxWalletPercent_base1000
23. setSwapBackSettings
24. setTargetLiquidity
25. setTxLimit
26. set_sell_multiplier
27. transfer
28. transferFrom
29. transferOwnership
30. unauthorize

SWC Registry: Smart Contract Weakness/Vulnerabilities

SWC-136	Unencrypted Private Data On-Chain	PASSED
SWC-135	Code With No Effects	PASSED
SWC-134	Message call with hardcoded gas amount	PASSED
SWC-133	Hash Collisions with Multiple Variable Length Arguments	PASSED
SWC-132	Unexpected Ether balance	PASSED
SWC-131	Presence of unused variables	PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	PASSED
SWC-129	Typographical Error	PASSED

SWC-128	DoS With Block Gas Limit	PASSED
SWC-127	Arbitrary Jump with Function Type Variable	PASSED
SWC-126	Insufficient Gas Griefing	PASSED
SWC-125	Incorrect Inheritance Order	PASSED
SWC-124	Write to Arbitrary Storage Location	PASSED
SWC-123	Requirement Violation	PASSED
SWC-122	Lack of Proper Signature Verification	PASSED
SWC-119	Shadowing State Variables	PASSED

SWC-118	Incorrect Constructor Name	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	PASSED
SWC-117	Signature Malleability	PASSED
SWC-116	Block values as a proxy for time	PASSED
SWC-115	Authorization through tx.origin	PASSED
SWC-114	Transaction Order Dependence	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	PASSED
SWC-113	DoS with Failed Call	LOW ISSUE

SWC-112	Delegatecall to Untrusted Callee	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED
SWC-110	Assert Violation	PASSED
SWC-109	Uninitialized Storage Pointer	PASSED
SWC-108	State Variable Default Visibility	PASSED
SWC-107	Reentrancy	LOW ISSUE
SWC-106	Unprotected SELFDESTRUCT Instruction	PASSED
SWC-105	Unprotected Ether Withdrawal	PASSED

SWC-104	Unchecked Call Return Value	PASSED
SWC-103	Floating Pragma	LOW ISSUE
SWC-102	Outdated Compiler Version	PASSED
SWC-101	Integer Overflow and Underflow	PASSED

Issue Checking

Manual code review is satisfactory.

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 always 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.

OVERALL ASSESSMENT

SATISFACTORY