Revoluzion Audit

Audit Report

Name	: CFTBET
Symbol	: CFT
Decimals	: 18
Address	: 0xA11bb08906cA57F802f24F7b5AB3f4286CCcaBDa
Owner	: 0x4a34cfbF0A40ab7363Ae2d32344Ce8E395893dD3
Network	: Binance Smart Chain (Mainnet)
Type	: BEP20
Audited on	: 2 November 2022

Contents

Project Overview

Name	CFTBET
Symbol	CFT
Decimals	18
Total Supply	1,000,000,000
Tax	Buy 2% | Sell 5% — (Fixed Tax)
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	Yes with 200 runs
License Type	Unlicensed
Explorer Link	https://bscscan.com/address/0xA11bb08906cA57F802f24F7b5AB3f4286CCcaBDa
Create Tx	0x8e210285e9f7d87d3d20a3915f730f3a21bcc33962a4e87882955fdde7385cfe
Creator	0x4a34cfbf0a40ab7363ae2d32344ce8e395893dd3
Featured Wallet	Marketing Wallet — 0x42aa3c96e642E618b69324C3C53E35b362769b97 Burned Wallet — 0x42aa3c96e642E618b69324C3C53E35b362769b97
GitHub Link	https://github.com/cftbet/Smart-Contract
Website	https://cftbet.com

Project Description

According to their website and Medium article

CFTBET makes peer-to-peer trading on sporting events fairer using the BSC Network. They hope to bring cryptocurrency and smart contract-based protocols to the mainstream and become a market standard for betting operators worldwide. With industry-low fees, fun tournaments, and unique non-custodial exchange technology, users can set their own odds and trade against others with confidence. Sports betting should be priced like a commodity, because it is one. This mean CFTBET will always an open platform designed for maximum versatility, fully welcoming third-party application and service providers.

Release Date	: TBA
Category	: Utility Token

CFTBET
You only compete against other players.
All bets are recorded in the blockchain which proves that we are provably fair and that we do not manipulate the results.

Online Presence

About Website

Registrar	: https://www.netearthone.com
Domain Expiration	: 2023-09-19
SSL Certificate	: Issued by Let's Encrypt

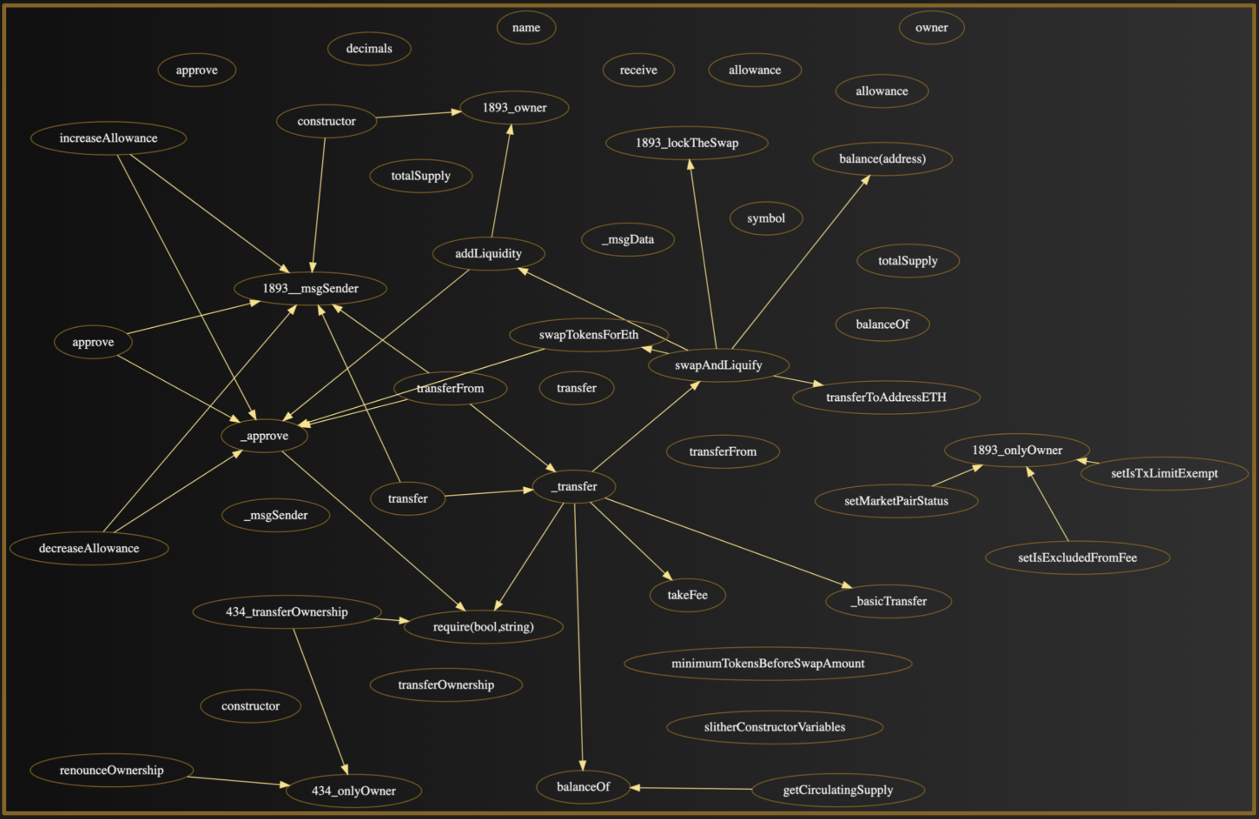
Official Links

Website	https://cftbet.com
YouTube	https://youtube.com/channel/UC3jEK53ncrnLLOvBmlnDp9w
Twitter	https://twitter.com/CFTBET
GitHub	https://github.com/cftbet
Reddit	https://reddit.com/user/cftbet
Medium	https://medium.com/@CFTBET
Telegram Channel	https://t.me/cftbetnews
Telegram Group	https://t.me/CFTBET

The Team

About	We from Revoluzion discovered that the team has privately doxxed to Expelee by completing the tasks as listed below.
KYC Issuer	Expelee
Member's KYC'd	N/A
KYC Date	23 October 2022
Certificate Link	**https://github.com/expelee-co/KYCs/blob/main/CFTBET%20KYC%20Certificate.pdf**
Task Completed	Project details — **Completed** ID verification — **Completed** Video statement — **Completed** Video interview with devs — **Completed**

Contract Functions Interaction



Audit Overview

Threat Level

When conducting audit on smart contract(s), we first look for known vulnerabilities and issues within the code because any exploitation on such vulnerabilities and issues by malicious actors could potentially result in serious financial damage to the projects. All the issues and vulnerabilities will be categorized into the categories as provided below.

Critical

This category provides issues and vulnerabilities that are critical to the performance/functionality of the smart contract and should be fixed by project creator before moving to a live environment.

Medium

This category provides issues and vulnerabilities that are not that critical to the performance/functionality of the smart contract but is recommended to be fixed by project creator before moving to a live environment.

Minor

This category provides issues and vulnerabilities that are minor to the performance/functionality of the smart contract and can remain unfixed by project creator before moving to a live environment.

Informational

This category provides issues and vulnerability that have insignificant effect on the performance/functionality of the smart contract and can remain unfixed by project creator before moving to a live environment. However, fixing them can further improve the efficacy or security for features with a risk-free factor.

Notable Information

- Contract Owner cannot stop or pause transactions.
- Contract Owner cannot transfer tokens from specific address.
- Contract Owner cannot increase the distribution of liquidity taken more than 5%.
- Contract Owner cannot mint new tokens after deploying smart contract.
- Contract Owner cannot burn tokens from specific wallet.
- Contract Owner cannot blacklist wallets from selling.
- Fixed buy and sell fees hardcoded as 2% and 5% respectively.
- There are no compiler warnings when compiling the smart contracts.
- Contract is using safe Zeppelin modules.

Caution

- Burned wallet is set to be a wallet address which is the exact same one as the marketing wallet. It is possible that the team will be doing a manual burn but there's also a risk where the funds will not be used for buyback and burn.

- Contract Owner can no longer change/update the router in the future should there is any issue arise since there is no function to so.

- Contract Owner can no longer change/update the marketing and burned wallet address in the future should there is any issue arise since there is no function to so.

Contract Diagnostic

Link for initial smart contract commit being audited on GitHub:

https://github.com/cftbet/Smart-Contract/commit/5cb813fdae220e7f6f423b986f4ef1aa290bc05f

CODE	SEVERITY	DESCRIPTION
SWC-103	Minor	A floating pragma is set.
SWC-108	Minor	State variable visibility is not set.
SWC-120	Minor	Potential use of "block.number" as source of randomness.
SS	Informational	Function state shadowing other function.
UR	Informational	Unused return value(s).
FIS	Informational	Function init states.
DC	Informational	Dead code.
NC	Informational	Naming convention.
SN	Informational	Similar name.
CS	Informational	State variable that can be declared as constant.

SWC-103 — A floating pragma is set

SEVERITY	Minor
LOCATION(S)	CFTBET.sol#L10
DESCRIPTION	The current pragma Solidity directive is set as ""^0.8.4"".
RECOMMENDATIONS	Project creator is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. It is important if the project rely on bytecode-level verification of the code.
STATUS	**N/A**

SWC-108 — State variable visibility is not set

SEVERITY	Minor
LOCATION(S)	CFTBET.sol#L262, 293
DESCRIPTION	It is best practice to set the visibility of state variables explicitly. The default visibility for "_balances", "_saleKeepFee" and "inSwapAndLiquify" are internal. Other possible visibility settings are public and private.
RECOMMENDATIONS	Project creator is recommended to set the visibility for "_balances ", "_saleKeepFee" and "inSwapAndLiquify" parameters under CFTBET.sol even if they are supposed to be internal.
STATUS	**N/A**

SWC-120 — Potential use of "block.number" as source of randomness

SEVERITY	Minor
LOCATION(S)	CFTBET.sol#451, 483
DESCRIPTION	The environment variable "block.number" looks like it might be used as a source of randomness to trigger a function.
RECOMMENDATIONS	We would recommend project owner to not use any of the environment variables like coinbase, gaslimit, block number and timestamp as sources of randomness since they are predictable and be aware that such usage could introduces a certain level of trust into miners. Keep in mind that malicious miner can manipulate the value of those variables and that any attackers could also predetermine the hashes of earlier blocks. However, based on our analysis, there's nothing to be done by project owner since in each of the "block.number" value was used as a means to keep track of time/epoch that relates to the trigger of a specific function.
STATUS	**N/A**

SS — Function state shadowing other function

SEVERITY	Informational — Medium
LOCATION(S)	CFTBET.sol#L521, 523, 926, 927
DESCRIPTION	[CFTBET._approve] (#L392) has “owner” parameter that shadows [Ownable.owner()] (#L122-124) [CFTBET.allowance] (#L369) “owner” parameter that shadows [Ownable.owner()] (#L122-124)
RECOMMENDATIONS	Project creator can choose to either rename the parameters to something else or completely ignore them.
STATUS	**N/A**

UR — Unused return value(s)

SEVERITY	Informational — Minor
LOCATION(S)	CFTBET.sol#L1177-1211
DESCRIPTION	[CFTBET.addLiquidity()] (#L539-551) ignores the return value at [uniswapV2Router.addLiquidityETH()] (#L543-550)
RECOMMENDATIONS	Based on our analysis, project creator doesn't need to do anything for this issue since it will be redundant.
STATUS	**N/A**

FIS — Function init states

SEVERITY	Informational — High
LOCATION(S)	CFTBET.sol#L277, 278, 279, 285, 286
DESCRIPTION	[CFTBET._liquidityShare] (#L277) is set pre-construction with a non-constant function or state variable: _sellLiquidityFee [CFTBET._marketingShare] (#L278) is set pre-construction with a non-constant function or state variable: _sellMarketingFee [CFTBET._BurnedShare] (#L279) is set pre-construction with a non-constant function or state variable: _sellBurnedFee [CFTBET._totalSupply] (#L285) is set pre-construction with a non-constant function or state variable: 10 * 10 ** 8 * 10 ** _decimals [CFTBET.minimumTokensBeforeSwap] (#L286) is set pre-construction with a non-constant function or state variable: 1 * 10 ** _decimals
RECOMMENDATIONS	We would recommend project owner to set these states as constant.
STATUS	**N/A**

DC — Dead code

SEVERITY	Informational — Medium
LOCATION(S)	CFTBET.sol#L19-22, 80-82, 84-87, 92-98, 100-106
DESCRIPTION	[Context._msgData()] (#L19-22) is never used and should be removed. [SafeMath.mod()] (#L80-82) is never used and should be removed. [SafeMath.mod()] (#L84-87) is never used and should be removed. [Address.isContract()] (#L92-98) is never used and should be removed [Address.sendValue()] (#L100-106) is never used and should be removed
RECOMMENDATIONS	Based on our analysis, the Address, Context and SafeMath smart contracts is the standard that is a direct fork from Open Zeppelin and were used within the contract itself. However, it is recommended for project creator to remove those functions to further optimize the smart contract since they are not used anywhere at all. Doing so will reduce the amount gas required when deploying the smart contract.
STATUS	**N/A**

NC — Naming convention

SEVERITY	Informational — Minor
LOCATION(S)	CFTBET.sol#L156, 259, 262, 270, 271, 272, 273, 274, 275, 277, 278, 279, 281, 282, 283, 293
DESCRIPTION	[IUniswapV2Router01.WETH()] (#L156) is not in mixedCase. [CFTBET.BurnedWalletAddress] (#L259) is not in mixedCase. [CFTBET._balances] (#L262) is not in mixedCase. [CFTBET._buyLiquidityFee] (#L270) is not in mixedCase. [CFTBET._buyMarketingFee] (#L271) is not in mixedCase. [CFTBET._buyBurnedFee] (#L272) is not in mixedCase. [CFTBET._sellLiquidityFee] (#L273) is not in mixedCase. [CFTBET._sellMarketingFee] (#L274) is not in mixedCase. [CFTBET._sellBurnedFee] (#L275) is not in mixedCase. [CFTBET._liquidityShare] (#L277) is not in mixedCase. [CFTBET._marketingShare] (#L278) is not in mixedCase. [CFTBET._BurnedShare] (#L279) is not in mixedCase. [CFTBET._totalTaxIfBuying] (#L281) is not in mixedCase. [CFTBET._totalTaxIfSelling] (#L282) is not in mixedCase. [CFTBET._totalDistributionShares] (#L283) is not in mixedCase. [CFTBET._saleKeepFee] (#L293) is not in mixedCase.
RECOMMENDATIONS	Based on our analysis, the IUniswapV2Router smart contract is a direct fork from Uniswap. Although the name doesn't conform to the standard convention, it's still okay to leave it be to avoid from potentially breaking any external function.

	However, for CFTBET smart contract, it is okay for project creator to update the name of the parameters in those functions so that they conform to the standard naming convention.
STATUS	**N/A**

SN — Similar name

SEVERITY	Informational — Minor
LOCATION(S)	CFTBET.sol#L161-162
DESCRIPTION	[IUniswapV2Router01.addLiquidity()] (#L161-162) has two parameters names that are too similar.
RECOMMENDATIONS	Based on our analysis, the IUniswapV2Router smart contract is a direct fork from Uniswap. Although their names are too similar, it's still okay to leave them be for the purpose of following the standard parameter declaration that is widely used as reference.
STATUS	**N/A**

CS — State variable that can be declared as constant

SEVERITY	Informational — Minor
LOCATION(S)	CFTBET.sol#L254, 255, 256, 258, 259, 270, 271, 272, 273, 274, 275, 292, 293
DESCRIPTION	[CFTBET._name] (#L254) should be constant. [CFTBET._symbol] (#L255) should be constant. [CFTBET._decimals] (#L256) should be constant. [CFTBET.marketingWalletAddress] (#L258) should be constant. [CFTBET.BurnedWalletAddress] (#L259) should be constant. [CFTBET._buyLiquidityFee] (#L270) should be constant. [CFTBET._buyMarketingFee] (#L271) should be constant. [CFTBET._buyBurnedFee] (#L272) should be constant. [CFTBET._sellLiquidityFee] (#L273) should be constant. [CFTBET._sellMarketingFee] (#L274) should be constant. [CFTBET._sellBurnedFee] (#L275) should be constant. [CFTBET.coolBlock] (#L292) should be constant. [CFTBET._saleKeepFee] (#L293) should be constant.
RECOMMENDATIONS	Based on our analysis, these variables should be declared as constant since they don't change throughout smart contract.
STATUS	**N/A**

Disclaimer

This report only shows findings based on our limited project analysis according to the good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall online presence and team transparency details of which are set out in this report. To get a full view of our analysis, **it is important for you to read the full report.** Under no circumstances did Revoluzion Audit receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. **Our team provides no guarantees against the sale of team tokens or the removal of liquidity by the project** audited in this document.

While **we have done our best to conduct thorough analysis to produce this report**, it is crucial to note that you should not rely solely on this report and use the content provided in this document as financial advice or a reason to buy any investment. The Our team disclaims any liability against us for the resulting losses based on the you decision made by relying on the content of this report. **You must conduct your own independent investigations before making any decisions** to protect yourselves from being scammed. We go into more detail on this in the disclaimer clause in the next page — please make sure to read it in full.

Full Disclaimer Clause

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy all copies of this report downloaded and/or printed by you. This report is provided for information purposes only, on a non-reliance basis and does not constitute to any investment advice.

No one shall have any right to rely on the report or its contents, and Revoluzion Audit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (collectively known as Revoluzion) owe no duty of care towards you or any other person, nor do we make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Revoluzion hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report.

Except and only to the extent that it is prohibited by law, Revoluzion hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Revoluzion, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts, website, social media, and team.