SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

Zendex Finance

AUDIT

SECURITY ASSESSMENT

15. September, 2023

FOR

ZENDEX

SolidProof_io

@solidproof_io

Introduction

SolidProof.io is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Zendex Finance
Website	https://zendex.finance/
About the project	We're thrilled to introduce ZenDEX, a next-generation DEX Built on @MantaNetwork. The first fast, secure, reliable and user-friendly DEX with deep liquidity built to support Manta ecosystem.
Chain	Manta Pacific
Language	Solidity
Codebase Link	https://github.com/ZenDEXFinance/zendex-contracts/tree/zendex-contracts
Commit	a631607
Unit Tests	Provided
Forked Status	1:1 Forked from PancakeswapV3 — https://github.com/pancakeswap/pancake-v3-contracts/tree/main/projects

Social Medias

Telegram	N/A
Twitter	https://twitter.com/zendex_finance
Facebook	N/A
Instagram	N/A
Github	N/A
Reddit	N/A
Medium	N/A
Discord	https://discord.com/invite/zendex
Youtube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Changelog
v1.0	15. September 2023	• Layout Project • Automated- /Manual-Security Testing • Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it.

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
src/router/contracts/interfaces/IQuoterV2.sol	272b339467147ab0cf04fb477696353ca6a71f45
src/router/contracts/interfaces/IWETH.sol	f2a5ae84716d8bd18fc6b729fb9733a89b835c17
src/router/contracts/interfaces/IStableSwap.sol	4bf457c931e1fabf3b259019d4547add35f9f584
src/router/contracts/interfaces/IV2SwapRouter.sol	370d0336a9ebb0a96c9f2ef2dc0e6d89df83fb6b
src/router/contracts/interfaces/IMulticallExtended.sol	83e1455f6abed8cde12ff9d646ebc33bb0e07b9f
src/router/contracts/interfaces/IApproveAndCall.sol	2871a74e1cd752562cd26e329f82d5545c9d8cc0
src/router/contracts/interfaces/IStableSwapInfo.sol	695a40149776705c07c8d93fa60da75d3bb35115
src/router/contracts/interfaces/IPeripheryPaymentsWithFeeExtended.sol	07ceb588e20ab8ae2a38e024c2788980e38db675
src/router/contracts/interfaces/IImmutableState.sol	8703217c8f5b666cb0c75d21240d069812362cce
src/router/contracts/interfaces/IOracleSlippage.sol	d8c738a71ae0a7aaf786a65ee2c97805c30633b7
src/router/contracts/interfaces/IStableSwapFactory.sol	145ccb5144c42a8f43cfa3e244847d8ed76f4aae
src/router/contracts/interfaces/ISmartRouter.sol	eae62c50fc3840bc3488b9ae8b1f8ccf1c3519e7
src/router/contracts/interfaces/IStableSwapRouter.sol	50a26f4a640fb3bd046da07fd2e7379619092471
src/router/contracts/interfaces/IQuoter.sol	414c29d48a547dd7d24c1b08382b8efee92ec420

src/router/contracts/interfaces/IPeripheryPaymentsExtended.sol	bb5b0f8650a0dbf5900b0a9a33b6301c1fc3022e
src/router/contracts/interfaces/IV3SwapRouter.sol	232fad48e2d4f2e19373e4d9ff391915dd9a6f51
src/router/contracts/interfaces/ITokenValidator.sol	fb2e9d373e49e1ad500415a234e6fb1da922731f
src/router/contracts/interfaces/IMixedRouteQuoterV1.sol	812c626d116c4a3a61fdffd4ae55c2afe05341a1
src/router/contracts/SmartRouter.sol	06fddbc97986269033d5cc0e3ff5afe4815d5136
src/router/contracts/V3SwapRouter.sol	ac0bbfaf9993fc8ac4bfb7e2e0958615c4613db1
src/router/contracts/lens/MixedRouteQuoterV1.sol	09483dda2a841792e59353f015e0f41fd13790e0
src/router/contracts/base/MulticallExtended.sol	49a46cd7aa4a0ee8e7a54c57b399a62949ddebe1
src/router/contracts/base/PeripheryPaymentsExtended.sol	0f56f74c4f12ad002b37fdbefb241cbf49f4d527
src/router/contracts/base/OracleSlippage.sol	390b2a25dc494d26babd24991e1ac023767551cf
src/router/contracts/base/PeripheryPaymentsWithFeeExtended.sol	78d15cd3b49b47dbc6eae32a682eb85ec9343ef5
src/router/contracts/base/ImmutableState.sol	1a8de0e5accdefb8ec7d8c289dbe8d58ad9a07dd
src/router/contracts/base/PeripheryValidationExtended.sol	7229ae571632b113f4d9163f0455e90cda2ad51e
src/router/contracts/base/ApproveAndCall.sol	2fc29cd64c247a42348bd270728dde98c2e1e2ea
src/router/contracts/StableSwapRouter.sol	d48147988365c972a93c2a7d058cc665c1f3c892
src/router/contracts/lens/TokenValidator.sol	a21fea25b49c79a1e99514e57890bdd56c92a4b9
src/router/contracts/lens/Quoter.sol	d490768f963d83d2a84d2ba5388c66f408144f04
src/router/contracts/lens/QuoterV2.sol	9285fc1a7be016f571dc5fa8caee09d30447cbab

src/router/contracts/V2SwapRouter.sol	5cba6dc4cbdf8cbac706a3e7d13f69b3e2c651a4
src/router/contracts/libraries/PoolTicksCounter.sol	c7676aa99d5bfe1c00fffea51a355fbb30ed9f43
src/router/contracts/libraries/Constants.sol	9f5f46b3797e661deab628727277abbd1f53f676
src/router/contracts/libraries/SmartRouterHelper.sol	f3ea27c076fc4d720b81d06beac7521e14b67534
src/v3-lm-pool/contracts/interfaces/IPancakeV3LmPool.sol	46bb5a557951d9a6abfe7ce23b4913b9371fbe86
src/v3-lm-pool/contracts/interfaces/IMasterChefV3.sol	bcdefc34dfa7fb19c03beddcdadfa03445e0101f
src/v3-lm-pool/contracts/PancakeV3LmPool.sol	0e84a4f5279b28e217a1945f730213b112adacf0
src/v3-lm-pool/contracts/PancakeV3LmPoolDeployer.sol	77998427bc87333bb444f7cc52570d90c060c39b
src/v3-lm-pool/contracts/libraries/LmTick.sol	901dfb79126b58f7c42f7cd53d503b641b5fc5c5
src/v3-core/contracts/PancakeV3Pool.sol	935e984e26f7c43e2268d763a298890aac5c04c1
src/v3-core/contracts/PancakeV3Factory.sol	c6346decc119ca7344c82afaaf8a6ab40fb1d0a3
src/v3-core/contracts/interfaces/pool/IPancakeV3PoolEvents.sol	01fad64d54df0dd9f97ce5e0cc651e2ae5a5d1bd
src/v3-core/contracts/interfaces/pool/IPancakeV3PoolOwnerActions.sol	920f4b1b48e414c13db50a547c61ed38dd2a93cd
src/v3-core/contracts/interfaces/pool/IPancakeV3PoolState.sol	07746567c830094a116b99cf8fa68cdf87207bca
src/v3-core/contracts/interfaces/pool/IPancakeV3PoolDerivedState.sol	3b219a1460e44bc7ca99eadf6eabe0094c76c701
src/v3-core/contracts/interfaces/pool/IPancakeV3PoolActions.sol	5968b1517d9d7e1ec4d31d8374550cb3e8bc279b
src/v3-core/contracts/interfaces/pool/IPancakeV3PoolImmutables.sol	383146e4a8e9a7ca2148d37890195bf7c6183544
src/masterchef-v3/contracts/libraries/SafeCast.sol	0cd843e1c910d1119af2322434690839ebf09547

src/masterchef-v3/contracts/keeper/MasterChefV3KeeperV1.sol	519823ae701e03ff194f651ed3fde093be23d8d4
src/masterchef-v3/contracts/keeper/MasterChefV3KeeperV2.sol	838aae07a646929d941c7c2a4ddc0f8a6b6fa73c
src/masterchef-v3/contracts/MasterChefV3.sol	111fe17fb10fdbe36a4e03af309684ed90db0be0
src/masterchef-v3/contracts/receiver/MasterChefV3Receiver.sol	9a25efd52281cbd33a146b312be503a08b0494c1
src/masterchef-v3/contracts/utils/Multicall.sol	8137902e1c2215f98bd78d6e5a49752945133822
src/masterchef-v3/contracts/receiver/MasterChefV3ReceiverV2.sol	d7bb0661a24be6f16601380d089c46932ba9a8f9
src/masterchef-v3/contracts/Enumerable.sol	3d4bcab22971615ffb50b69501cef461608db671
src/masterchef-v3/contracts/interfaces/IReceiver.sol	49d88280ef3907a99a38f166e500a092e72a8175
src/masterchef-v3/contracts/interfaces/IWETH.sol	1ef4dc7a02ea78237d61516d4d38f17ac3e7059d
src/masterchef-v3/contracts/interfaces/INonfungiblePositionManagerStruct.sol	0dbc51143791c3bece7803f279890b447eebf90f
src/masterchef-v3/contracts/interfaces/IFarmBooster.sol	26a71a196d1e85f0a13929473d44cbc7a381d4a6
src/masterchef-v3/contracts/interfaces/ILMPoolDeployer.sol	2d57770788b244062c7d69d52013485ea9b89f98
src/v3-core/contracts/interfaces/IERC20Minimal.sol	978f86a8a5fd358b8d24493ccee7b6316d51f5f8
src/masterchef-v3/contracts/interfaces/INonfungiblePositionManager.sol	a8bae669f1f328512edaf6498207b94245a713ee
src/v3-core/contracts/interfaces/IPancakeV3Pool.sol	960f09264fcffe5e122bb0a08b608e521180fc87
src/v3-core/contracts/interfaces/IPancakeV3PoolDeployer.sol	66b17e639ed40afca3639a042519c25b3b3db71f
src/v3-core/contracts/interfaces/IPancakeV3Factory.sol	5330a26cec37c057b32a8671a70ad1d37244ee6a
src/masterchef-v3/contracts/interfaces/IPancakeV3Pool.sol	013c52a61733ae43f48effb0562a299b64d33c58

src/masterchef-v3/contracts/interfaces/IMasterChefV2.sol	04e5ad2be3a5e9e3e4bcc8f4f840be5b049b8173
src/masterchef-v3/contracts/interfaces/ILMPool.sol	dd2c78bb29cf3bb0a811163ff349fafd6cee38c8
src/masterchef-v3/contracts/interfaces/IMasterChefV3.sol	864a959be1fb257c2e82f4b6c76407dfba49f01a
src/v3-core/contracts/interfaces/callback/IPancakeV3FlashCallback.sol	5b0dea772c33771332ec7f37bb6641d930d29d94
src/v3-core/contracts/interfaces/callback/IPancakeV3MintCallback.sol	ccc783266da7d7a2718b689bae6bf2ba02a57e3e
src/v3-core/contracts/interfaces/callback/IPancakeV3SwapCallback.sol	e9d973a7d4ebb0ea6b63d0127671040b8b38dd09
src/v3-periphery/contracts/SwapRouter.sol	5dbbaba3d8542d39c02fc97a69451241210e41ff
src/v3-periphery/contracts/NonfungibleTokenPositionDescriptor.sol	9fea4b78ecf0630537d13c5f57c419b9c1ae6e04
src/v3-core/contracts/libraries/LowGasSafeMath.sol	1bee2d0f85bc054e3b63a7e92c67d237a49c650c
src/v3-core/contracts/libraries/TickMath.sol	7eee6a798a068e6eaaa63ce8f432ee193e0ff2e0
src/v3-core/contracts/libraries/Oracle.sol	49519e7e73e076479b04d0027d342468126e4cba
src/v3-core/contracts/libraries/BitMath.sol	82ee70afdc183819ee3705d274a506a42f1e278b
src/v3-core/contracts/libraries/Tick.sol	37ef664ced74a41e7a2f438cdbf99527566f1aab
src/v3-core/contracts/libraries/TickBitmap.sol	31e44d52941443c6b03ce88dd32294a3e89aa80c
src/v3-core/contracts/libraries/LiquidityMath.sol	2d440d1d862d4612b08243581f9232887b489c09
src/v3-core/contracts/libraries/Position.sol	0d6be19a8ba07321743fc90010a969b0fe26e301
src/v3-core/contracts/libraries/UnsafeMath.sol	d3e3ff1ab78e03ccec335ab6da4ea76b578cb422
src/v3-core/contracts/libraries/FixedPoint96.sol	3a3ab5c10385c523c1738b9eb9d86dcd5f59c3f4

src/v3-core/contracts/libraries/SafeCast.sol	c3b25ed7fa205de6cc2075d96e27908d43f21671
src/v3-core/contracts/libraries/FullMath.sol	0c531e95498282fc6ad5856e6273b7675b15bea0
src/v3-core/contracts/libraries/TransferHelper.sol	09f4e335c7ed41383bf2f04bf278169218994fc8
src/v3-core/contracts/libraries/SwapMath.sol	585ec272ca9a5a9b5d4645178b64fb52003e6091
src/v3-core/contracts/libraries/SqrtPriceMath.sol	0bf7a6c27c88689b4ade289bf0683adabe90a570
src/v3-core/contracts/libraries/FixedPoint128.sol	22517ba8d668bb4e86a45f3f29ed077d72fb7608
src/v3-periphery/contracts/NonfungiblePositionManager.sol	556b7cc4ba8cb507ffbd83646dd91e8645320c6e
src/v3-periphery/contracts/examples/PairFlash.sol	7ea67321c52d9496614b9e74577043ecee78db5d
src/v3-periphery/contracts/V3Migrator.sol	a82235f477837bd739c1e52261c4dc14825521ac
src/v3-periphery/contracts/NonfungibleTokenPositionDescriptorOffChainV2.sol	bc7014ad12e2989ccfde18dee202281a2aa9bad8
src/v3-periphery/contracts/NFTDescriptorEx.sol	05707ea0d848a11ba31c386f458c3e21edd5afaf
src/v3-periphery/contracts/NonfungibleTokenPositionDescriptorOffChain.sol	f6b952c11c2ed811dbdbbc02bb020f000bfd4c2f
src/v3-periphery/contracts/base/SelfPermit.sol	62cdfd2d982b595f9abcaca570c4bd39fd93faa1
src/v3-periphery/contracts/base/PeripheryValidation.sol	078495af30569dfdb02365ae8340f54d03b04c96
src/v3-periphery/contracts/base/BlockTimestamp.sol	e9433e812b02a43ae225b797863e5102e802ef27
src/v3-periphery/contracts/base/Multicall.sol	e48264609451e31ffea549e7db3e30815080505c
src/v3-periphery/contracts/base/ERC721Permit.sol	c0a49336d7af11a67d7790cf909db944041101c1

src/v3-periphery/contracts/base/PeripheryPayments.sol	4f747bd40edccc1c89f8f02bad4b9589ba55f2a7
src/v3-periphery/contracts/base/PeripheryPaymentsWithFee.sol	533939938850a044a483610175ea08f322138031
src/v3-periphery/contracts/base/PeripheryImmutableState.sol	238ba15bdc60250ead1a2f21c8307d175c9d0880
src/v3-periphery/contracts/base/PoolInitializer.sol	e3749267784816d54514b509404574e85d14ab81
src/v3-periphery/contracts/base/LiquidityManagement.sol	895c22f8dd9959cf740f7759d0bcfd7c1e20ce1f
src/v3-core/contracts/PancakeV3PoolDeployer.sol	6d4d6c7692a9090d5ce194a05431dc9c37885692
src/v3-periphery/contracts/lens/Quoter.sol	bd2f355d4f3068779ef1133cbf16f5c199ffee34
src/v3-periphery/contracts/lens/QuoterV2.sol	9fbab218809b10e1b11f94e800a04640aee977e3
src/v3-periphery/contracts/lens/PancakeInterfaceMulticall.sol	359d64d8bf14032153b0ebc863609930f8037f52
src/v3-periphery/contracts/lens/TickLens.sol	2ed3ede465ac6922898533558e102b0aa7188f55
src/v3-periphery/contracts/interfaces/IPeripheryPayments.sol	33bb73e15d6f5e842a8c2406ba6e7d538255919d
src/v3-periphery/contracts/interfaces/ISelfPermit.sol	fb8db7a56077ca32dd58a4a9bc25b54e2ad57071
src/v3-periphery/contracts/interfaces/ITickLens.sol	5bb2a6b9e8f948f1d9ffb60f7d93ed7e72eecfd3
src/v3-periphery/contracts/interfaces/external/IERC1271.sol	5560885f1e908f592046013d4df11ca12416d522
src/v3-periphery/contracts/interfaces/external/IERC20PermitAllowed.sol	0f8ae33f339095b7745444ede48774f4023f7b0e
src/v3-periphery/contracts/interfaces/external/IWETH9.sol	b6c58d4b3b77515c7dc30dd5a813bdeff6589294
src/v3-periphery/contracts/interfaces/ISwapRouter.sol	96406379b07edfb0be0f00dec1053ee4ab0552b4
src/v3-periphery/contracts/libraries/BytesLib.sol	747be1412bfe71b5c06f4bbfa7cb7b2c968bfdcc

src/v3-periphery/contracts/libraries/NFTDescriptor.sol	b04f6394336bdb4644ae135c856a4e122ca60609
src/v3-periphery/contracts/libraries/OracleLibrary.sol	d9bbb8e6078b38d3333165277cabed0530c3d6a1
src/v3-periphery/contracts/interfaces/IQuoter.sol	414c29d48a547dd7d24c1b08382b8efee92ec420
src/v3-periphery/contracts/libraries/TransferHelper.sol	f20f1d2d65b5609532e0ea83490ce6cb4a79cd38
src/v3-periphery/contracts/libraries/CallbackValidation.sol	0e7d840f3bf626b89df8f1f501230d32961b7efd
src/v3-periphery/contracts/libraries/PoolTicksCounter.sol	3c7a3ce6dd0f7ffe620ddd28813d3018bae3cd96
src/v3-periphery/contracts/interfaces/INonfungiblePositionManager.sol	ab78aada40133e958cbc0d91084ceb871879f43d
src/v3-periphery/contracts/libraries/TokenRatioSortOrder.sol	84ff0b5257a032c234bf53b3866a857edd30512b
src/v3-periphery/contracts/interfaces/IV3Migrator.sol	d5aa198c7234d0b630d71fd9ca1dc6d900bd08a2
src/v3-periphery/contracts/libraries/NFTSVG.sol	a6194b805dea4be2cb470ad3ca38d0db5d128036
src/v3-periphery/contracts/interfaces/IERC20Metadata.sol	36aad581ce20107a3ec451cb4b7c604091c028f3
src/v3-periphery/contracts/libraries/ChainId.sol	99c85fd8d764eb5b36e5ff9dc1a7723289070d85
src/v3-periphery/contracts/interfaces/IERC721Permit.sol	e331fe0555bddff85f4b515a0e10165e1d6bcb78
src/v3-periphery/contracts/libraries/PositionValue.sol	e7ea39ab08801a7c8a36a89479edd96d99d16a29
src/v3-periphery/contracts/libraries/PoolAddress.sol	1894efd76ded03e224cedfd9a4d9f319a0628c4f
src/v3-periphery/contracts/interfaces/INonfungibleTokenPositionDescriptor.sol	1b2a07a417f71dd9b40e9fd376ad0ec00660c3ad
src/v3-periphery/contracts/libraries/PositionKey.sol	6cc88dd5fd105faa25c6f048b0e7da4e50263c8b
src/v3-periphery/contracts/libraries/Path.sol	2504b1a543392240bddbe04efef9c47cecdc704b

src/v3-periphery/contracts/interfaces/IQuoterV2.sol	272b339467147ab0cf04fb477696353ca6a71f45
src/v3-periphery/contracts/libraries/HexStrings.sol	fc19854bf736b050ab6a78bb595cef7a43699b45
src/v3-periphery/contracts/interfaces/IPeripheryImmutableState.sol	820e3e0811436fffc6b6aabecea700da3f5d7e8d
src/v3-periphery/contracts/libraries/LiquidityAmounts.sol	d0e6e831938d4da61aeaf3a04bf0e8ffcc50326f
src/v3-periphery/contracts/interfaces/IPeripheryPaymentsWithFee.sol	0da1ac6c52abfdbc8171d40f3ee898e08818cb31
src/v3-periphery/contracts/libraries/SqrtPriceMathPartial.sol	57463d27a55617f9e3aea7fe0365032dac05e5b0
src/v3-periphery/contracts/interfaces/IPoolInitializer.sol	5e91f53e858852ce1ce70f623f869c8976a0fe53
src/v3-periphery/contracts/interfaces/IMulticall.sol	9e6b62357fe6d6748e7a5c4765c6ae6e1d732632

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

Dependency / Import Path	Cou nt
@openzeppelin-upgradeable/proxy/Initializable.sol	2
@openzeppelin-upgradeable/utils/StringsUpgradeable.sol	2
@oz4.8.1/contracts/access/Ownable.sol	3
@oz4.8.1/contracts/security/ReentrancyGuard.sol	1
@oz4.8.1/contracts/token/ERC20/IERC20.sol	4
@oz4.8.1/contracts/token/ERC20/utils/SafeERC20.sol	3
@oz4.8.1/contracts/token/ERC721/IERC721.sol	1
@pancakeswap/v3-core/contracts/interfaces/IPancakeV3Factory.sol	3
@pancakeswap/v3-core/contracts/interfaces/IPancakeV3Pool.sol	20
@pancakeswap/v3-core/contracts/interfaces/callback/IPancakeV3FlashCallback.sol	1
@pancakeswap/v3-core/contracts/interfaces/callback/IPancakeV3MintCallback.sol	1
@pancakeswap/v3-core/contracts/interfaces/callback/IPancakeV3SwapCallback.sol	7
@pancakeswap/v3-core/contracts/libraries/BitMath.sol	3
@pancakeswap/v3-core/contracts/libraries/FixedPoint128.sol	3
@pancakeswap/v3-core/contracts/libraries/FixedPoint96.sol	2
@pancakeswap/v3-core/contracts/libraries/FullMath.sol	7
@pancakeswap/v3-core/contracts/libraries/LiquidityMath.sol	1
@pancakeswap/v3-core/contracts/libraries/LowGasSafeMath.sol	7
@pancakeswap/v3-core/contracts/libraries/SafeCast.sol	9
@pancakeswap/v3-core/contracts/libraries/Tick.sol	1
@pancakeswap/v3-core/contracts/libraries/TickBitmap.sol	3
@pancakeswap/v3-core/contracts/libraries/TickMath.sol	13

@pancakeswap/v3-core/contracts/libraries/UnsafeMath.sol	1
@pancakeswap/v3-lm-pool/contracts/interfaces/IPancakeV3LmPool.sol	1
@pancakeswap/v3-periphery/contracts/base/BlockTimestamp.sol	1
@pancakeswap/v3-periphery/contracts/base/Multicall.sol	1
@pancakeswap/v3-periphery/contracts/base/PeripheryImmutableState.sol	6
@pancakeswap/v3-periphery/contracts/base/PeripheryPayments.sol	1
@pancakeswap/v3-periphery/contracts/base/PeripheryPaymentsWithFee.sol	1
@pancakeswap/v3-periphery/contracts/base/PeripheryValidation.sol	1
@pancakeswap/v3-periphery/contracts/base/SelfPermit.sol	1
@pancakeswap/v3-periphery/contracts/interfaces/IMulticall.sol	1
@pancakeswap/v3-periphery/contracts/interfaces/INonfungiblePositionManager.sol	2
@pancakeswap/v3-periphery/contracts/interfaces/IPeripheryPayments.sol	1
@pancakeswap/v3-periphery/contracts/interfaces/IPeripheryPaymentsWithFee.sol	1
@pancakeswap/v3-periphery/contracts/interfaces/ISelfPermit.sol	1
@pancakeswap/v3-periphery/contracts/libraries/OracleLibrary.sol	1
@pancakeswap/v3-periphery/contracts/libraries/Path.sol	5
@pancakeswap/v3-periphery/contracts/libraries/PoolAddress.sol	1
@pancakeswap/v3-periphery/contracts/libraries/TransferHelper.sol	6
@uniswap/solidity-lib/contracts/libraries/SafeERC20Namer.sol	1
@uniswap/v2-core/contracts/interfaces/IUniswapV2Callee.sol	1
@uniswap/v2-core/contracts/interfaces/IUniswapV2Pair.sol	4
base64-sol/base64.sol	3
lib/openzeppelin-contracts/contracts/access/Ownable.sol	1
lib/openzeppelin-contracts/contracts/drafts/IERC20Permit.sol	1
lib/openzeppelin-contracts/contracts/math/SafeMath.sol	2
lib/openzeppelin-contracts/contracts/math/SignedSafeMath.sol	2

lib/openzeppelin-contracts/contracts/token/ERC20/IERC20.sol	11
lib/openzeppelin-contracts/contracts/token/ERC721/ERC721.sol	1
lib/openzeppelin-contracts/contracts/token/ERC721/IERC721.sol	1
lib/openzeppelin-contracts/contracts/token/ERC721/IERC721Enumerable.sol	1
lib/openzeppelin-contracts/contracts/token/ERC721/IERC721Metadata.sol	1
lib/openzeppelin-contracts/contracts/utils/Address.sol	1
lib/openzeppelin-contracts/contracts/utils/ReentrancyGuard.sol	3
lib/openzeppelin-contracts/contracts/utils/Strings.sol	3

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit vulnerability and the impact of that event on the organization or system. The risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    a. Reviewing the specifications, sources, and instructions provided to
    SolidProof to ensure we understand the size, scope, and functionality of the
    smart contract.
    b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
    c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

2. Testing and automated analysis that includes the following:
    a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
    b. Symbolic execution, which is analysing a program to determine what inputs cause each part of a program to execute.

3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.

4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

Overall Security

Upgradeability

Contracts are not upgradeable	✅ Deployer cannot update the contracts with new functionalities
Description	The contract is not an upgradeable contract. The deployer is not able to change or add any functionalities to the contract after deploying.
Comment	Only the “NonfungibleTokenPositionDescriptorOffChainV2” contract is upgradeable which is used to setting the base Token URI

Ownership

The ownership is not renounced	❌ The owner is not renounce
Description	The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including: • Centralizations • The owner has significant control over contract's operations
Comment	N/A

Note - If the contract is not deployed then we would consider the ownership to be not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced.

Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner cannot mint new tokens	✅ **The owner cannot mint new tokens**
Description	The owner is not able to mint new tokens once the contract is deployed.
Comment	N/A

Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens	✅ **The owner cannot burn tokens**
Description	The owner is not able burn tokens without any allowances.
Comment	N/A

Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses	✅ **The owner cannot blacklist addresses**
Description	The owner is not able blacklist addresses to lock funds.
Comment	N/A

Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%	✅ **The owner cannot levy unfair taxes**
Description	The owner is not able to set the fees above 25%
Comment	N/A

Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Owner cannot lock the contracts	✅ **The owner cannot lock the contracts**
Description	The owner is not able to lock the contract by any functions or updating any variables.
Comment	The owner cannot lock the contracts directly but it is possible to halt the withdraw and harvest actions in the MasterChef contract

External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

Components

📝Contracts	📚Libraries	🔍Interfaces	🎨Abstract
26	37	61	21

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

🌐Public	💰Payable
366	100

External	Internal	Private	Pure	View
306	356	63	124	137

StateVariables

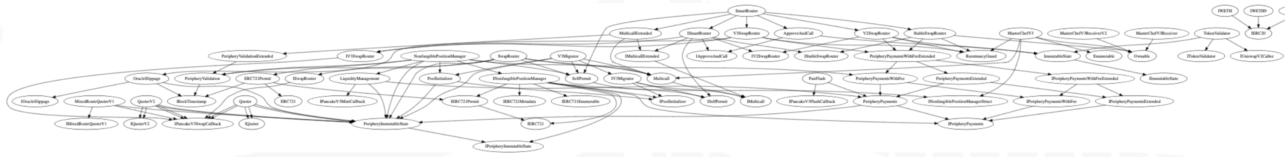
Total	🌐Public
152	80

Capabilities

Solidity Versions observed	📤 Transfers ETH	💰 Can Receive Funds	🖥 Uses Assembly	👥 DelegateCall
>=0.7.5 >=0.5.0 =0.7.6 >=0.6.0 >=0.5.0 <0.8.0 ^0.8.10 ^0.8.0 >=0.7.0 >=0.4.0 >=0.4.0 <0.8.0 >=0.7.6 ^0.7.0 >=0.6.8 <0.8.0	Yes	Yes	Yes	Yes

Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.



Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.

In the project, there are authorities that have access to the following functions:

File	Privileges
MasterChefV3.sol	• onlyOwner • Enable/Disable Emergency • Set Receiver and LM Pool Deployer address • Add a new pool • Update pool's allocation point • Update Reward for the liquidity Mining Pool • Set Period Duration • Update Farm Boost Contract
PancakeV3LmPool.sol	• onlyOwner or Masterchef • Accumulate Reward • Cross Lm Tick • Update Position
NFTDescriptorEx.sol	• onlyOwner • Set Owner • Update NFT domain and Switch back and forth from Http link

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness of privileged operations

- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

#1 | Missing Zero Address Validation

File	Severity	Location	Status
MasterChefV3	Low	L193	Open

Description - Make sure to validate that the address passed in the function parameters is “non-zero”.

#2 | Missing Events

File	Severity	Location	Status
PancakeV3LmPool	Low	L50—94	Open

Description - Make sure to emit events for all the critical parameter changes in the contract to ensure the transparency and trackability of all the state variable changes.

#3 | Old Compiler version

File	Severity	Location	Status
All	Low	N/A	Open

Description - The contracts use outdated compiler versions, which are not recommended for deployment as they may be susceptible to known vulnerabilities.

Remediation - Use a newer pragma version. At least use the 0.8.18 version.

Informational issues

#1 | NatSpec documentation missing

File	Severity	Location	Status
PancakeV3LmPool	Informational	N/A	Open

Description - If you started to comment on your code, comment on all other functions, variables etc.

#2 | Floating Pragma

File	Severity	Location	Status
All	Informational	N/A	Open

Description - The contracts should be deployed with the same compiler version and flag that they have been tested thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using other versions.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.

Solid Proofed

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY