SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

Galador Exchange

AUDIT

SECURITY ASSESSMENT

25. January, 2024

FOR

Introduction 3
Disclaimer 3
Project Overview 4
Summary 4
Social Medias 6
Audit Summary 7
File Overview 8
Imported packages 16
Components 17
Exposed Functions 17
Capabilities 18
Inheritance Graph 19
Audit Information 20
Vulnerability & Risk Level 20
Auditing Strategy and Techniques Applied 21
Methodology 21
Overall Security 22
Upgradeability 22
Ownership 23
Ownership Privileges 24
Minting tokens 24
Burning tokens 25
Blacklist addresses 26
Fees and Tax 27
Lock User Funds 28
Centralization Privileges 29
Audit results 31

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	Galador Exchange
Website	https://www.galador.io/
About the project	Galador has been built as a highly-efficient and customizable protocol, allowing both builders and users to leverage our custom infrastructure for deep sustainable, and adaptable liquidity. We move beyond the traditional design of DEXs to focus on offering a tailored approach that prioritizes composability.
Chain	TBA
Language	Solidity
Codebase	https://github.com/galadorexchange/contracts
Forked Status	This Project is forked from Uniswap and Pancakeswap, So the issues that will be present in these contracts will not be part of the audit scope and we are not responsible for any issues related to them. The contracts can be found in the links below: Swapv2: https://github.com/Uniswap/v2-core/tree/master/contracts https://github.com/Uniswap/v2-periphery/tree/master/contracts Swapv3: https://github.com/pancakeswap/pancake-v3-contracts
Deployed Contracts	GaladorFactory:https://www.teloscan.io/address/0x0773c452f0EeDB7643ac5375E9c23BCE4FEB71b0#contract GaladorRouter02:https://www.teloscan.io/address/0xefC73FbB3D33C05a032901043d5840e6445598fc#contract Multicall2:https://www.teloscan.io/address/0x83Cd32eC8807852e2Ef659515b6c3C64ca1850AD#contract Multicall3:https://www.teloscan.io/address/0x4E06d6ec4a3A90790edee253C8BF098bbb4F51E5#contract GaladorV3PoolDeployer:https://www.teloscan.io/address/0x1fea636a57Ef81A5D83f12f95b6f3013fAA1896c#contract GaladorV3Factory:https://www.teloscan.io/address/0x177D6eA09b3b02b57e21642A9A8997F9D979132E#contract SwapRouter:https://www.teloscan.io/address/0xb33096C90D1D60B08af8DC168A30F2cB04E4947e#contract NonfungibleTokenPositionDescriptorOffChain:https://www.teloscan.io/address/0xb7E99aF568E1d1f86E2B6e963

	B2374Fe45A7beC6#contract NonfungiblePositionManager:https://www.teloscan.io/address/0x00c57EE7ba3e384168FF863950D8810B85001DDA#contract GaladorInterfaceMulticall:https://www.teloscan.io/address/0xbD45C86ac01ceba66Ebe6439072029Df8e405C6E#contract V3Migrator:https://www.teloscan.io/address/0xaB0A1069676e93f78Da22Dff731F0daAbFc011bE#contract TickLens:https://www.teloscan.io/address/0xBb53DeAABe48f35926C6f5B1583FE63A033B19d6#contract QuoterV2:https://www.teloscan.io/address/0x057Ce605df6867E9da743080148B225633b483d5#contract SmartRouterHelper:https://www.teloscan.io/address/0xEdED9825f986eF1237F4Ef5A6165382Cc8b90BBC#contract SmartRouter:https://www.teloscan.io/address/0xb8C06b7193565d105A256Bf0C0f116156826ae39#contract MixedRouteQuoterV1:https://www.teloscan.io/address/0xB052Bb0ed23F57975a9B3843300CFa2fd9BBB7f2#contract QuoterV2:https://www.teloscan.io/address/0x1E6Ed1Ce1fBF8463438C3Dc8958B573cAf7b7cC4#contract TokenValidator:https://www.teloscan.io/address/0x4D1b7b6942FF1a569900e53C979FB98B2d0d192C#contract
Commit	https://github.com/galadorexchange/contracts/commit/6505c377c0a3e05279951336198584bcba585fc1
Unit Tests	Provided

Social Medias

Telegram	https://t.me/galadorfi
Twitter	https://twitter.com/galadorfi
Facebook	N/A
Instagram	N/A
GitHub	https://github.com/galadorexchange
Reddit	N/A
Medium	N/A
Discord	https://discord.gg/xTRcEFRAJ6
YouTube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Change Log
v1.0	13. January 2024	· Layout Project · Automated/ Manual-Security Testing · Summary
v1.2	25. January 2024	· Reaudit

Note – The following audit report presents a comprehensive security analysis of the smart contract utilized in the project that includes outside manipulation of the contract's functions in a malicious way. 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. This includes internal calculations in the formulae used in the contract. Also, some of the contracts isn't verified on the mainnet so we cannot check that the code which is provided to us is same as the code provided in the repository so we cannot guarantee the code in the contract is same.

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
swapV3/router/interfaces/IOracleSlippage.sol	d8c738a71ae0a7aaf786a65ee2c97805c30633b7
swapV3/router/interfaces/IStableSwapFactory.sol	6d5dda813f8192b8267aa4a82eb88af88d4713d0
swapV3/router/interfaces/ISmartRouter.sol	1e1f2358b41c8e9a5c1a88a0689283517bef4793
swapV3/router/interfaces/IStableSwapRouter.sol	9b2c2e7850ce72dd043aa1c2f4249fc41f76609b
swapV3/router/interfaces/IQuoter.sol	b27b93ebb11a4fc136d7f7d91cb93f2e12133789
swapV3/router/interfaces/IPeripheryPaymentsExtended.sol	9d2a1071a0793004c05095182b130859acca7878
swapV3/router/interfaces/IV3SwapRouter.sol	cdf03c97208b2c2a49012b419c9ea5a199036603
swapV3/router/interfaces/ITokenValidator.sol	2b19ac97a5aad121162a9f4edb6b2af073df7a6d
swapV3/router/interfaces/IMixedRouteQuoterV1.sol	a1b4a6265fa603f970863d90935b977f4f94dbbb
swapV3/router/interfaces/IV2SwapRouter.sol	d4d868da259463bcd9cbe4ff5c754b9704cbcaa2
swapV3/router/interfaces/IWETH.sol	f2a5ae84716d8bd18fc6b729fb9733a89b835c17
swapV3/router/interfaces/IStableSwap.sol	4bf457c931e1fabf3b259019d4547add35f9f584
swapV3/router/interfaces/IMulticallExtended.sol	8cc450e5bb919dc1798a3fcaf0908e17fb4db737
swapV3/router/interfaces/IQuoterV2.sol	1ab5cc793a60fc32965e01a770272e3d06bcbda9
swapV3/router/interfaces/IApproveAndCall.sol	f902d77a4b094960369190800821dc5f6ee0fb9c
swapV3/router/interfaces/IStableSwapInfo.sol	695a40149776705c07c8d93fa60da75d3bb35115
swapV3/router/interfaces/IPeripheryPaymentsWithFeeExtended.sol	1de2bc24e36dc880ac40a228b8d7258d827fa198

File Name	SHA-1 Hash
swapV3/router/interfaces/IImmutableState.sol	15326ac11c38f23364859a03976302609dc16258
swapV3/router/base/MulticallExtended.sol	af5ed64fb40a8a8cd039ff80c23ba4c638a67d03
swapV3/router/base/PeripheryPaymentsExtended.sol	81474cfbd0eed3b2fa7cf3399389de90acf614fb
swapV3/router/base/OracleSlippage.sol	4ee83528c7cc4999a2185624c301d6ddbeb46762
swapV3/router/base/PeripheryPaymentsWithFeeExtended.sol	00a7ae7e66c5b2c481c683e486317596ad7fa346
swapV3/router/base/ImmutableState.sol	765e870e30dcced3f15a45aca53e5150efa992d7
swapV3/router/base/PeripheryValidationExtended.sol	c442f86064f29f8adab4a6ba498ab6d7e1ef5c53
swapV3/router/base/ApproveAndCall.sol	804efd6203600df631a2b2c20c95586b0f1a636a
swapV3/router/SmartRouter.sol	0b49b545caaa1a4be9936326fc0556114a320bca
swapV3/router/V3SwapRouter.sol	0dee1c20a83a3e73fa3611e650bb73723c7958dc
swapV3/router/lens/TokenValidator.sol	2dc332d081a8ba312cffd043f8ab0272d5341b05
swapV3/router/lens/Quoter.sol	993b1245f9f5b1016c525e956b9e45adbf6f4f66
swapV3/router/lens/QuoterV2.sol	80d733c38038e50d6fab50df1f80707172ae9257
swapV3/router/lens/MixedRouteQuoterV1.sol	38400f46266fe8af3c76b59213a6292607b6006f
swapV3/router/StableSwapRouter.sol	64c17c00eff7361c5c8e5975647222bacb148522
swapV3/router/libraries/PoolTicksCounter.sol	eaaec134ed5bf7b982b21230bf33c40f8010e77f
swapV3/router/libraries/Constants.sol	9f5f46b3797e661deab628727277abbd1f53f676
swapV3/router/libraries/SmartRouterHelper.sol	d8f2b707abe2cc3d60bba9514db14146b7b96065
swapV3/router/V2SwapRouter.sol	014fc21840700c49ee90b2aa2ec65d18b78ddcb8
swapV3/openzeppelin/contracts-	6e787c3994e602a05cdcc45ace2e5f7a5a

File Name	SHA-1 Hash
upgradeable/utils/AddressUpgradeable.sol	37d698
swapV3/openzeppelin/contracts-upgradeable/utils/StringsUpgradeable.sol	034362686b931958e6077ad96b7a2e078e3213b4
swapV3/openzeppelin/contracts-upgradeable/proxy/ClonesUpgradeable.sol	3748ba60f335469619c8a79ecca1ac1a9024f063
swapV3/openzeppelin/contracts-upgradeable/proxy/Initializable.sol	8b29874aea561b809494b08ab07307406b9ae646
swapV3/v2/interfaces/IGaladorPair.sol	1f6b5cfb16401357d0a9c407f2dfb48a3c601d36
swapV3/v2/interfaces/IGaladorCallee.sol	99199fba19ad7cab30b810ba348848a49c4c72e9
swapV3/periphery/interfaces/ISelfPermit.sol	fb8db7a56077ca32dd58a4a9bc25b54e2ad57071
swapV3/periphery/interfaces/ITickLens.sol	a4637d80b53ec4df6e856a5a6037b6727e573f72
swapV3/periphery/interfaces/IPeripheryPayments.sol	62c96883d26e41281afc84329898533832ad70cd
swapV3/periphery/interfaces/external/IERC1271.sol	b4294b6fc22368771e4e6837ce9866193749 94cd
swapV3/periphery/interfaces/external/IERC20PermitAllowed.sol	0f8ae33f339095b7745444ede48774f4023f7b0e
swapV3/periphery/interfaces/external/IWETH9.sol	af992260b11f057e0dbef946918641161c7fa647
swapV3/periphery/interfaces/ISwapRouter.sol	637e37472813eeeca5c145ab26cce6fc70623693
swapV3/periphery/interfaces/IQuoter.sol	b27b93ebb11a4fc136d7f7d91cb93f2e12133789
swapV3/periphery/interfaces/INonfungiblePositionManager.sol	e3620f3a70d6a691578a197b3cc87dcb35300c31
swapV3/periphery/interfaces/IV3Migrator.sol	fdff53d27638162a767bb646a3375fab3a992f82
swapV3/periphery/interfaces/IERC20Metadata.sol	900b0d273c3eaa64a27bf12858bec097622db779
swapV3/periphery/interfaces/IERC721Permit.sol	345454f72b32464cc1bf65d6f2f24eeda6907e1f
swapV3/periphery/interfaces/INonfungibleTokenPositionDescriptor.sol	88b743f0928423a36f1b4775bd51e575dd75dc2a
swapV3/periphery/interfaces/IQuoterV2.sol	1ab5cc793a60fc32965e01a770272e3d06bcbda9

File Name	SHA-1 Hash
swapV3/periphery/interfaces/IPeripheryImmutableState.sol	91b4523620c102d5c0401c2a4d1fec98dd73bdbd
swapV3/periphery/interfaces/IPeripheryPaymentsWithFee.sol	04c3d15451802e33b303e55e742e1857176a3511
swapV3/periphery/interfaces/IPoolInitializer.sol	5e91f53e858852ce1ce70f623f869c8976a0fe53
swapV3/periphery/interfaces/IMulticall.sol	00fcedd2582ff5029973ea594189379b58597420
swapV3/periphery/base/PeripheryValidation.sol	5fa09566b7c1b99b07812bd2bf55c571e3c99e1a
swapV3/periphery/base/BlockTimestamp.sol	e9433e812b02a43ae225b797863e5102e802ef27
swapV3/periphery/base/Multicall.sol	1d0669d0505b3cdf5ef5438f9c9e3dec85488069
swapV3/periphery/base/ERC721Permit.sol	856e843f2e42813fcf1076a6ebec71c0c75bff53
swapV3/periphery/base/PeripheryPayments.sol	c067d1abb844e8dbea49237df083c75552bded45
swapV3/periphery/base/PeripheryPaymentsWithFee.sol	60af03904e4a5f8770aa5aca475d463d892dd6b4
swapV3/periphery/base/PeripheryImmutableState.sol	b36c4b4deec277e5a63fde0c72a2ebf6a5d7c711
swapV3/periphery/base/PoolInitializer.sol	4e432d269c032b36408b5a0bdf66816fba6a856d
swapV3/periphery/base/LiquidityManagement.sol	3de414c5cb36fa2ef310ffdee499f6320532b618
swapV3/periphery/base/SelfPermit.sol	5eedf89252b3b3386e0bb7cf0b9dd38dc70c7f48
swapV3/periphery/NonfungibleTokenPositionDescriptor.sol	8df47e3548610a82ab1f76e1fea76b61bf185b01
swapV3/periphery/examples/PairFlash.sol	ade744cc4e2118d236ea05d7d6103d7620438faf
swapV3/periphery/NonfungiblePositionManager.sol	080d32413053f9560cf3ee959e2b6ecc79464b7d
swapV3/periphery/lens/Quoter.sol	411f9265a3d8882972b5e2629dd920967a80519f
swapV3/periphery/lens/QuoterV2.sol	371797a020224432898f5d283685da90bb94ed63
swapV3/periphery/lens/TickLens.sol	8abe98e9b2def2836e0aa88c774bf1c300

File Name	SHA-1 Hash
	6fa3fc
swapV3/periphery/lens/GaladorInterfaceMulticall.sol	d9542d8ac215ebbd4b202a05250220006773e882
swapV3/periphery/SwapRouter.sol	f3c8f51a31c4916810673449 19fd5b69242e4185
swapV3/periphery/libraries/BytesLib.sol	39cf60af450748c4151c486f0a960416b358209b
swapV3/periphery/libraries/NFTDescriptor.sol	948697ffd127a53f71d0f6cb04dfbc8090e5d428
swapV3/periphery/libraries/OracleLibrary.sol	fb9a02651611b8d429e498d111ee967e60dcf8fb
swapV3/periphery/libraries/TransferHelper.sol	95d871188c962e1d077c630615cc9ada4395fc9a
swapV3/periphery/libraries/CallbackValidation.sol	946bd3cea59465804c56537cc5cab5bfe3b0bb59
swapV3/periphery/libraries/PoolTicksCounter.sol	eaaec134ed5bf7b982b21230bf33c40f8010e77f
swapV3/periphery/libraries/TokenRatioSortOrder.sol	84ff0b5257a032c234bf53b3866a857edd30512b
swapV3/periphery/libraries/NFTSVG.sol	b5d3f2da13c7cbaf68844f249b30b81e04b5496c
swapV3/periphery/libraries/ChainId.sol	15296b77054cea2965c9a8485e693f0bbd71eacb
swapV3/periphery/libraries/PositionValue.sol	66e245709f004b0dff78f94cbb9cc853880bdb9a
swapV3/periphery/libraries/PoolAddress.sol	5f22b151028c7a8788ef5741c6f104be1372ee4e
swapV3/periphery/libraries/PositionKey.sol	6cc88dd5fd105faa25c6f048b0e7da4e50263c8b
swapV3/periphery/libraries/Path.sol	97106557f4ffebeb12d34de1c0952c735cbf172b
swapV3/periphery/libraries/HexStrings.sol	daa636926a289980331546019 44b8812b1390ad9
swapV3/periphery/libraries/LiquidityAmounts.sol	95bf67f7c4998efb569a703babaeb3d2a549ced4
swapV3/periphery/libraries/AddressStringUtil.sol	6c3ee345b3b2468b90519cd1c76acfbdb197decb
swapV3/periphery/libraries/SafeERC20Namer.sol	8f97fa28cbf48bba10fc30ee4faa9385a31a7d6c

File Name	SHA-1 Hash
swapV3/periphery/libraries/SqrtPriceMathPartial.sol	52a8dc684664478cd74757a0c73d350b71212ea3
swapV3/periphery/V3Migrator.sol	c041e86b22d94274a65e9281be7bfef34e5c7c4e
swapV3/periphery/NonfungibleTokenPositionDescriptorOffChainV2.sol	622255ec83b9f3dec55e12b273de5b7984d539ec
swapV3/periphery/NFTDescriptorEx.sol	e94df60d4ceb780a87479f05c3c0bcfdad4b21bc
swapV3/periphery/NonfungibleTokenPositionDescriptorOffChain.sol	e0815fc28d44c1e2d0caf1dc4949314b37552c00
swapV3/base64-sol/Base64.sol	a7fff24e244962c0ca88281f9facbd43357aea78
swapV3/core/interfaces/IGaladorV3Factory.sol	71cdcc90859fd64c4e36f984cbe364b2612e97b2
swapV3/core/interfaces/pool/IGaladorV3PoolState.sol	79b4c33efa15452096e98028f3534690958f91f4
swapV3/core/interfaces/pool/IGaladorV3PoolEvents.sol	c249808fb7afe2b4b6241b95b6ea6d6ef4670bda
swapV3/core/interfaces/pool/IGaladorV3PoolActions.sol	a2c245e2b7932d83889e96e0e57f3f85a7cfe29b
swapV3/core/interfaces/pool/IGaladorV3PoolOwnerActions.sol	8740e7c7ddadfb7f037f827e55aef032373a50e2
swapV3/core/interfaces/pool/IGaladorV3PoolImmutables.sol	8d98f094d3a625db771393029775518e301b20b3b
swapV3/core/interfaces/pool/IGaladorV3PoolDerivedState.sol	66a0cd631a86b35f3d20f96f90df06a610c6c8c9
swapV3/core/interfaces/callback/IGaladorV3FlashCallback.sol	cfcc83c94a0ac9725c8a55ee83fbdc75aefb5ac9
swapV3/core/interfaces/callback/IGaladorV3MintCallback.sol	19878d4220c6c0e0e7c81814afd8259604af4ae7
swapV3/core/interfaces/callback/IGaladorV3SwapCallback.sol	4dae25c63c985d31a556fcefd6ee564f7dab8a7a
swapV3/core/interfaces/IERC20Minimal.sol	1fc7227b35a04b1a8476c94797dc8cdb08dada2a
swapV3/core/interfaces/IGaladorV3PoolDeployer.sol	e393d593012c2f9f3083167adbd4c0ba221171e9
swapV3/core/interfaces/IGaladorV3Pool.sol	23113139fc16104e8d5ecc6fcae3ba1d519876ba
swapV3/core/libraries/SwapMath.sol	528f7da05da7370af193175c4b5b80b3c00

File Name	SHA-1 Hash
	6024a
swapV3/core/libraries/UnsafeMath.sol	97311ad71761a6b4d623cc540db3ad37f77ee0e2
swapV3/core/libraries/FixedPoint96.sol	3a3ab5c10385c523c1738b9eb9d86dcd5f59c3f4
swapV3/core/libraries/SafeCast.sol	bd0887ff5fe3e9b695bd373d64d83d8b66e12d5b
swapV3/core/libraries/FullMath.sol	c325c22a1ca0b5400ca8b4caa3cb02a3bd000bb1
swapV3/core/libraries/TransferHelper.sol	97e1a0d6107b804c2b2676a7a013156a65314fed
swapV3/core/libraries/SqrtPriceMath.sol	8034a05c6659186f7515cbbe4efc250a30a9ed95
swapV3/core/libraries/FixedPoint128.sol	22517ba8d668bb4e86a45f3f29ed077d72fb7608
swapV3/core/libraries/TickMath.sol	881ac7bb18df4fe4f5d52857075189933538 9cf3
swapV3/core/libraries/Oracle.sol	ffac8ff584d1ff603223cc7f1a5dfa5adc646991
swapV3/core/libraries/LowGasSafeMath.sol	1bee2d0f85bc054e3b63a7e92c67d237a49c650c
swapV3/core/libraries/BitMath.sol	82ee70afdc183819ee3705d274a506a42f1e278b
swapV3/core/libraries/Tick.sol	a1d5d58fe4e940deb5e8ce6ab541030bd238d236
swapV3/core/libraries/TickBitmap.sol	af4ca00937898b49c5017924afc2d28c4b03d07e
swapV3/core/libraries/LiquidityMath.sol	796fe68a3c92976f392b047a80ab4f0f9a634f55
swapV3/core/libraries/Position.sol	96c95d591b929ffd5541149e5ec334c4a86ff83e
swapV3/core/GaladorV3Factory.sol	adc12ce8043ff585fcda7e104911459bf2c8468d
swapV3/core/GaladorV3PoolDeployer.sol	3fc596c6a55cc591bf2b567bc4a0afb7bc8c62db
swapV3/core/GaladorV3Pool.sol	9fb8560212d8ff45059707fe621cccc64899d2d9
swapV3/openzeppelin-3.4.2/math/Math.sol	4de1b0181035f2a9088a2556a7f6ff45abc36295

File Name	SHA-1 Hash
swapV3/openzeppelin-3.4.2/math/SignedSafeMath.sol	38401e89465215367d124fa34c44d2b04f18a0f7
swapV3/openzeppelin-3.4.2/math/SafeMath.sol	875f257c172b5e3dfcbf2b8c74ca666576d22cb5
swapV3/openzeppelin-3.4.2/introspection/IERC165.sol	6e098caf450b72f2462ec65c27988f8fc94d112a
swapV3/openzeppelin-3.4.2/introspection/ERC165.sol	497d6bdb651781b9481b286072d2faea1506ba4a
swapV3/openzeppelin-3.4.2/utils/SafeCast.sol	1ce0607efd38c3cb14ebb5e0d687f51355436279
swapV3/openzeppelin-3.4.2/utils/Strings.sol	f8929c3d8703fd0c806eec8a976412ea3bbb9912
swapV3/openzeppelin-3.4.2/utils/Context.sol	db2960443dd005ba75dc9e5cd56bd028b316621c
swapV3/openzeppelin-3.4.2/utils/Create2.sol	4af51465535c6346b64bc013aeab1dfc19e02071
swapV3/openzeppelin-3.4.2/utils/EnumerableSet.sol	21d64e5e1c28db4337e204200f5de80bef2b5734
swapV3/openzeppelin-3.4.2/utils/Address.sol	ccee81fc8ce99727846b1179319fa89f989e98a4
swapV3/openzeppelin-3.4.2/utils/Arrays.sol	05fe11718d3cd3b39c27382e43b6b3f73e32d0c4
swapV3/openzeppelin-3.4.2/utils/EnumerableMap.sol	dce67367d345acc5f6a27703b77ab0742f48c977
swapV3/openzeppelin-3.4.2/utils/Counters.sol	1ba483c0befd61df8598e1d9b51d669459801deb
swapV3/openzeppelin-3.4.2/utils/Pausable.sol	ac0845b9cf5ff98be1c420124ba491c758a73da7
swapV3/openzeppelin-3.4.2/utils/ReentrancyGuard.sol	67047504a8ca237b572108ef5c32383429f1ad66
swapV3/openzeppelin-3.4.2/access/Ownable.sol	58cfbd567ff53153a462b441614118cf6459aea2
swapV3/openzeppelin-3.4.2/token/ERC721/ERC721Burnable.sol	40828fc8aa692c7b06ec3dadab436960ba7e2f58
swapV3/openzeppelin-3.4.2/token/ERC721/ERC721Holder.sol	0902afe7e6646897c2030b8fdbfd1e746c2160e1
swapV3/openzeppelin-3.4.2/token/ERC721/IERC721.sol	06ee0a7db2e8f3b62b564e1611f9347390d4c1c0
swapV3/openzeppelin-3.4.2/token/ERC721/ERC721.sol	6e9f5fd2ed7217b0f532cb163c5163f5bf2a21

File Name	SHA-1 Hash
	d2
swapV3/openzeppelin-3.4.2/token/ERC721/ERC721Pausable.sol	d199b3ddec231ba3da044d6de808f2436fe30fd0
swapV3/openzeppelin-3.4.2/token/ERC721/IERC721Receiver.sol	cf6006c2ecb41a0d51572978dca60e5207738c0f
swapV3/openzeppelin-3.4.2/token/ERC721/IERC721Metadata.sol	257a6ae6f1408c02fc767c2ea5278daa6c081111
swapV3/openzeppelin-3.4.2/token/ERC721/IERC721Enumerable.sol	f88487b9aa6334f1684fcb2de599a70df0c6e572
swapV3/openzeppelin-3.4.2/token/ERC20/IERC20PermitOzep342.sol	0286e162ac37454892b1298c14d057b5d41f03fb
swapV3/openzeppelin-3.4.2/token/ERC20/IERC20Ozep342.sol	f85f2ac4650ff7872b261a919e58c4ec4dfab6a5
helpers/Multicall2.sol	d48cde323fa6641fd8459a01e16ff5ed15640bf0
helpers/Multicall3.sol	797243fbddef00a2e9a8e024efee89ed26353e8f
helpers/Timelock.sol	d3107b6f6bba85b75dc7fbb15030025f81df3d07
helpers/SwapV2Multicall.sol	55da956437b034c774fe29101830985aad2c2ffd
swapV2/interfaces/IGaladorLP.sol	0ae49229f8e41a1887a467b21a7e6a9f114aa295
swapV2/interfaces/IGaladorPair.sol	941a7749c447a1fa08ee7795c139434bba074c9c
swapV2/interfaces/IGaladorRouter02.sol	40d7c63f6cb9e58efc1a9ab25951f80ea177cdc0
swapV2/interfaces/IGaladorFactory.sol	0c2628c601e9272d2086b24bff68883508d27dbf
swapV2/interfaces/IGaladorRouter01.sol	c312593ed55823af0a4522ae6cc01a3506599c69
swapV2/interfaces/IGaladorCallee.sol	58ea0ae9829968fd5a70d0282e07a1f6e529f7ad
swapV2/interfaces/IWETH.sol	6d60a5b42e70d54bd6d02ec86065d892db80b14b
swapV2/GaladorPair.sol	bf9c9ad370a6f75efd11470002802a05f71f0300
swapV2/GaladorLP.sol	3ceaef922561b8f91497941b8f5292d8af33c839

File Name	SHA-1 Hash
swapV2/GaladorRouter02.sol	7892785ff980e1a96e09c7c101df7c4eeabbba66
swapV2/GaladorFactory.sol	23ddd22310ca18881af01f5958a0d32a8bc337fc
swapV2/libraries/GaladorLibrary.sol	cc1e3919969634dcd4104b847db12b3d591922c3
swapV2/libraries/SafeMathGalador.sol	1c23987232aa5aaa12c18eee7e834f2f0b1c1c66
swapV2/libraries/TransferHelper.sol	4cf2dfbb0a8a3417a5e3519b23f6ae47b359a750
swapV2/libraries/Math.sol	77ab89000dde3dc7732b701263e95871c44fc74c
swapV2/libraries/UQ112x112.sol	3279c729db6bc799ac24f8e466f3a4ba819a4193
libraries/IBoringERC20.sol	1804f9471ad4e5127b48c96b54a2f26f5ac65909
libraries/BoringERC20.sol	6b606ef5ff367a7e169ee79ad865c2fc372eb8c9

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. These are the above SHA is of the contracts which was in the mentioned repository in the above section.

Imported packages.

Used code from other Frameworks/Smart Contracts.

N/A

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. Also, the project is 1:1 forked with Uniswap and pancake swap but due to compatibility issues, the project owner has made some changes in the 'SmartRouterHelper' library within the main contract itself (V2SwapRouter and V3SwapRouter). As a fix, they removed the external call entirely by including the source implementation within the main 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'sstate. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be needed within visibility modifier, such as public, private or internal, which determines the access level of the variable.

Components

📝 Contracts	📚 Libraries	🔍 Interfaces	🎨 Abstract
30	58	70	28

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
537	110

External	Internal	Private	Pure	View
411	591	89	203	269

StateVariables

Total	🌐 Public
173	76

Capabilities

Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
>=0.7.5 =0.7.6 >=0.5.0 >=0.6.2 <=0.8.0 >=0.6.0 <=0.8.0 >=0.4.24 <=0.8.0 >=0.7.0 >=0.5.0 <=0.8.0 >=0.6.0 >=0.6.8 <=0.8.0 >=0.4.0 <=0.8.0 ^0.7.0 0.8.12 =0.8.2 =0.6.12 ^0.8.7	ABIEncoderV2	Yes	yes (64 asm blocks)	----------

Transfers ETH	Low-Level Calls	Delegate Call	Uses Hash Functions	ECRecover	New/Create/Create2
yes		yes	yes	yes	yes ⟶ AssemblyCall:Name:create ⟶ AssemblyCall:Name:create2

TryCatch	Σ Unchecked
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 methodsfrom another class. It shows the relationships between different contracts and how they are related to each other through inheritance.

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit the 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 executingthe 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 andsmart 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

Contract is an upgradable	✗ Deployer can update the contract with new functionalities.
Description	The contract is an upgradeable contract. The Deployer is able to change or add any functionalities to the contract after deploying.
Comment	It is recommended to make sure to check all the upgradable functionalities.

File/Line(s): L955-957

Codebase: NonFungibleTokenPositionDescriptorOffChain.sol

```
ftrace | funcSig
function initialize(string calldata baseTokenURI↑) external initializer {
    _baseTokenURI = baseTokenURI↑;
}
```

Ownership

Contract ownership is not renounced.	❌ **The ownership is not renounced.**
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 – *The contract cannot be considered as renounced till it is not deployed or having some functionality that can change the state of the contract.*

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. Although, the contract contains the functionalities where the NFT can be minted.
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 wallets.**
Description	The owner cannot blacklist addresses for transferring of tokens.
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 indeveloping and maintaining the contract.

Contract owner cannot set fees more than 25%.	✅ **The owner cannot set fees more than 25%.**

Description	The owner cannot set fees more than 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 token 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.

Contract owner cannot lock functions.	✅ **The owner cannot lock the contract.**
Description	The owner cannot be able to lock the contract.
Comment	N/A

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
Timelock.sol	➢ The pending admin can change admin. ➢ The admin can update new admin in the contract. ➢ The admin can queue, cancel, and execute transactions.
GaladorFactory.sol	➢ The FeeToSetter address can change the fee wallet address. ➢ The FeeToSetter address can update the migrator address. ➢ The FeeToSetter can update the FeeToSetter address.
NFTDescriptorEx.sol	➢ The owner can update the owner address. ➢ The owner can toggle Http link and NFT domain in the contract.
StableSwapRouter.sol	➢ The owner can update the stable swap factory and info address in the contract.

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 Result

Critical Issues

No critical issues

High Issues

No high issues

Medium Issue

No medium issues

Low Issue

#1 | Floating pragma solidity version.

File	Severity	Location	Status
All	Low	--	ACK

Description – Adding the constant latest version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

#2 | Missing zero address validation.

File	Severity	Location	Status
GaladorFactory	Low	--	ACK
NFTDescriptorEx	Low	--	ACK

Description – It is recommended to check that the address cannot be set to zero or a dead address.

#3 | Missing events.

File	Severity	Location	Status
GaladorFactory	Low	--	ACK

Description – Emit all the critical parameter changes.

#4 | Remove safemath library.

File	Severity	Location	Status
All	Low	--	ACK

Description – The compiler version above 0.8.0 has the ability to control arithmetic overflow/underflow, it is recommended to remove the unwanted code in order to avoid high gas fees.

Informational Issue

#1 | NatSpec Documentation missing.

File	Severity	Location	Status
All	Informational	--	ACK

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

#2 | Contract doesn't import npm packages from source (like OpenZeppelin etc.)

File	Severity	Location	Status
All	Informational	--	ACK

Description – We recommend importing all packages from npm directly without flattening the contracts. Functions could be modified or can be susceptible to vulnerabilities.

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.

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY