GORDIAN AGENCY

SMART CONTRACT SECURITY AUDIT

May 19th, 2022

Professional Auditing Agency

Website https://gordian.agency/

AUDIT DETAILS

GORDIAN AGENCY

Project

DEX Finance

Deployer Address

0x0785b464316abE29Ad9b3555218FCaD27769FA0d

Client Contacts

@dexCEO

Blockchain

Binance Smart Chain

Project Website

https://www.dexfinance.com/

BACKGROUND

GORDIAN AGENCY

Gordian Agency was commissioned by Dex finance to perform an audit of smart contracts:

Controller	0xFDF0aa7A94af4eb26e8A80DCC1645b68E2CcB342
PoolFactory	0xD7c2a4C6c013538701500E43D24c924A5B37bd65
PoolInitializer	0x0D6ee0928386FCfEF121e30Ff094b1b099Fb8b3C
IndexPool	0x60EBfD605Cb25C7796F729c78a4453ACeCb1CE03
DexETFUniswapRouterMinter	0xbc070418aDf5d5dfDe4f1C272eCca0326033Ee00
DexETFUniswapRouterBurner	0x0D673c2b9e9523e71868dA0915316Ef175E19c57
ProxyAccessControl	0xA5FA1f5363D6667A4E3B4739F2AB390f90650dC9
ProxyManager	0x548F14453c27388799bB9c3d85fc3910aCB25157
DexETFUniswapV2Oracle	0x3B186d534c714679cf9d0504D1FBFD56c2339E7C

The information in this report should be used to understand the risk exposure of the smart contracts, and as a guide to improve the security posture of the smart contracts by remediating the issues that were identified.

SUMMARY

GORDIAN AGENCY

DEX finance is building an innovative platform to easily build, deploy, and maintain Index Funds comprised of various tokens in a secure and decentralized manner.

Audit Findings Summary:

- No security issues from outside attackers were identified.
- The project team should exercise caution to avoid adding fee-on-transfer tokens as an asset in any Index Pool which can lead to errors during balance calculations.
- Investing requires placing trust in the project team as they have substantial power in the ecosystem.
- IndexPool contract does not contain the logic related to swapping and flash-borrowing funds in the pool.

The information in this report should be used to understand the risk exposure of the smart contracts, and as a guide to improve the security posture of the smart contracts by remediating the issues that were identified.

CONTRACT DETAILS

Dex finance contract details

Controller::

- *This contract contract provides the owner a few permissions across the platform.*
- *The owner can use this contract to configure and deploy an Index Pool.*
- *The system uses time-weighted averages to determine the pricing of each token involved in the Index Pool.*
- *Once an Index Pool is deployed, the PoolInitializer must finish preparing the pool by calculating the weights for each token in the Pool.*
- *Anyone is able to use the contract to evaluate and update data including denormalized weights for an Index Pool that has reached it's minimum balance requirements at any time.*
- *Anyone is able to reindex any initialized Index Pool at any time, as long as it is due for a reindex; reindexing recalculates and updates the minimum required balances and the denormalized weights for each token in the Index Pool.*
- *Anyone is able to reweigh any initialized Index Pool at any time, as long as it is due for a reweigh; reweighing recalculates the denormalized weights for the desired tokens in the Index Pool, as well as the top tokens in the category of interest.*
- *The owner is able to set the maximum number of different tokens any initialized Index Pool can be comprised of at any time.*
- *The owner is able to set the exit fee receiver address on any initialized Index Pool at any time.*

CONTRACT DETAILS

Dex finance contract details

PoolFactory and PoolAccessControl:

- *Approved addresses can use this contract to deploy a new Index Pool using a many-to-one proxy, meaning there can be multiple addresses for the same implementation code; this is used in order to create multiple Index Pools at will.*
- *The owner of the PoolFactory contract is intended to be the PoolAccessControl contract.*
- *The owner is able to use the PoolAccessControl contract to transfer the ownership of the PoolFactory contract to any address at any time.*
- *The owner is able to grant or revoke Admin access from any address at any time.*
- *The owner or any address with the Admin role is able to grant the ability for any address to deploy pools via the Pool Factory contract at any time; only the owner can revoke this permission.*

CONTRACT DETAILS

Dex finance contract details

PoolInitializer:

- *The project team can use the PoolInitializer contract to initialize an IndexPool via the Controller contract.*
- *The Index Pool is not considered to have finished initialization until it has met the minimum contribution amounts for each of the desired tokens; the minimum contribution amounts are based on the weights of each token.*
- *Users can contribute tokens to the Index Pool in order to meet the balance requirements; the system will assign the users "credits" based on the current ETH value of the tokens being deposited.*
- *Before contributing, users can issue a call to fetch the latest time-weighted average token prices to ensure the most up-to-date pricing.*
- *Once the Index Pool has met the target contribution amounts for each token in its composition, the initialization is marked as finished, and the Controller contract calculates the denormalized weights for each token based on the current ETH value of the balance of each token.*
- *Once the initialization of the Index Pool is completed, users will be able to claim a portion of the Index Pool shares based on the ETH value of their tokens at contribution time.*

CONTRACT DETAILS

Dex finance contract details

IndexPool:

- *In order to join the Pool, a user must deposit an amount of each asset token the Pool is comprised of proportional to the amount of shares the user wishes to purchase; users will be able to join as long as the Pool has not yet reached its capacity.*
- *Upon exiting the Pool, users pay a portion of their shares to the exit fee recipients determined by the project team. The remaining shares are liquified and an amount of each asset token proportional to the amount of shares being burned is delivered to the user.*
- *The Controller contract is able to set the maximum pool shares cap to any value at any time.*
- *The Controller contract is able to set both exit fee recipient addresses to any address at any time.*
- *The Controller contract is able to set the minimum balance required for a token in the pool as long as the token is bound and not in Ready status.*

DexETFUniswapRouterMinter/Burner:

- *Anyone can use the DexETFUniswapRouterMinter contract to invest in the Index Pool using a single asset; the tokens or ETH deposited are swapped for the asset tokens of the Index Pool and the user receives shares representing their ownership of the Index Pool in exchange.*
- *Anyone can use the DexETFUniswapRouterBurner contract to divest from the Index Pool and receive a single asset token or ETH in return. An amount of each asset token the Index Pool is comprised of proportional to the amount of shares the user wishes to burn is swapped for the desired output token and delivered to the user.*

THREAT ASSESSMENT

GORDIAN AGENCY

EXTERNAL THREAT RESULTS

Vulnerability Category	Notes	Result
Arbitrary Storage Write	N/A	PASS
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Integer Over/Underflow	N/A	PASS
Multiple Sends	N/A	PASS
Suicide	N/A	PASS
State Change External Calls	N/A	PASS
Unchecked Retval	N/A	PASS
User Supplied Assertion	N/A	PASS
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety	N/A	PASS

NOTES

General notes

- Excellent structuring of logic to prevent reentrancy attacks and to optimize gas usage.
- The platform uses Uniswap to calculate time-weighted averages for pricing data; price data points consulted in the average are at least 30 minutes apart.
- The Index Pool and BMath libraries used throughout the platform are based on code pioneered by Balancer Finance.
- The BMath libaries also serve to protect transactions from overflows.
- The contracts utilize 112x112 fixed point number representation for arithmetic operations, which promotes gas efficiency in calculations, but sacrifies range and precision that the standard floating point number representation offers.

CONCLUSION

The audited contract contains no issues and is safe to deploy.

NOTES:

Please check the disclaimer below and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is solely provided for the contracts mentioned in the report and does not include any other potential contracts deployed by the Owner.

DISCLAIMER

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: 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 any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Gordian and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Gordian) owe no duty of care towards you or any other person, nor does Gordian 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 Gordian 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, Gordian hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Gordian, 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 alone. No applications or operations were reviewed for security. No product code has been reviewed.