DEX Finance audit by Raiders of DeFi

Objects of review: audit the following contracts of DEX Finance and compare them to original Tomb Finance and other major algorithmic protocols contracts. Explore potential vulnerability vectors by difference checks, such as non-renounced contracts, exploitable parameters, or malicious inserted code.

Peg Token (USDEX) 📝 0x829c09fCc46D9fd31967272ABA245BEF9f727F93

✅ ERC20 compliant, 18-decimal token.

✅ Compliant with other algorithmic protocols' peg token.

ℹ️ Tokenomics: 600 002 tokens airdropped (-> 243 000 presale, 301 467 airdrop to gnosis safe, 55 535 others), 1 token for DEX, 1 token for genesis pool, 1 token for initial liquidity. Devs control 50% of tokens at inception.

⚠️ Owner not renounced. The team may mint, on their discretion, arbitrary amount of tokens, and drain all liquidity.

Share Token (dexSHARE) 📝 0xf4914E6D97a75f014AcFcF4072f11be5CfFc4cA6

✅ ERC20 compliant, 18-decimal token.

✅ Compliant with other algorithmic protocols' share token.

ℹ️ Tokenomics: 65 250 tokens airdropped (-> 59 500 farming pools, 1 254 presale, 4 263 airdrop to gnosis safe, 233 others), 31 250 shares for community fund, 5000 shares for developer and team fund, 1 share for initial liquidity.

✅ Share vesting: community fund and developer funds vest over 365 days, starting along with liquidity pool share farming.

ℹ️ As community funds, developer funds, and gnosis safe airdrop are all governed by the project owners, developers control 40% of all shares. *Developer commentary: "The reason for the large amount of shares to community fund is because we will be using this in order to fund the bonding mechanism ie; USDC, BNB, ETC in exchange for vested dexSHARE at a discount."*

⚠️ Ownership same as in peg token.

Share Reward Pool Contract

📝 **0xCC180BfA5d2C3Ac191758B721C9bBbB263b3fd1C**

✅ Compliant with other algorithmic protocols' reward pools.

✅ Rewards run from Wednesday, May 11, 2022 2:00:00 AM UTC for 370 days.

✅ governanceRecoverUnsupported (no tamper) can drain tokens 90 days after pool end (industry standard, but make sure to withdraw !).

ℹ️ Operator not renounced. They can change pool allocations (including deactivating pools) or add new pools (including "ghost pools", i.e. boosted pools for themselves only). This is however typical in most forks to allow incentive tweaks in response to changing market conditions over the whole project lifetime.

Treasury Contract 📝 0x1DF93D98EE398C3cCAE4AA5e3580C583Fb16403A

Masonry Contract 📝 0xA649987E48F89Ef11981c9A794DF2C7D3fa3AeB3

ℹ️ Compliant with other algorithmic protocols' contracts, but with significant functionality change:

▶️ All rewards are routed to "Peg Regulation address", which is a 2/3 gnosis safe proxy under developer's complete control. *As per official developer communication about the innovations of their project: The peg regulation address has been updated to the gnosis safe and gelato resolvers are used to calculate the conversion to ETF tokens and redistribution to the regulation pool (ETF rewards).*

Wrapped wDEX-SHARE 📝 0x05220A11566a954d449dCB72d241277668b8cF9E

ℹ️ Custom contract, governing distribution of the rewards for wrapped share tokens.

✅ Results of the wrap are governed by Ratio Manager (📝 0x9d84a0bbd352ed9b8044a2d852c2e3dc908e02a8), while rewards by Reward Manager (📝 0xe27d6d13589c7aef73c834617b01be0388df69bd). Both are automated.

⚠️ As with other contracts, ownership is not renounced. Owners may pause rewards, disable unwrapping, and more.

Verdict: ⚠️

Summary: We have not found any rug or scam code in the DEX Finance contracts listed. Nonetheless, many contracts remain in complete ownership of the team to enable them maintain the innovative functionalities and react to market demands. However, this means all liquidity can be drained. Investing requires trust in the project team. Contracts not listed here have not been audited.

@Filip | Tomb Raider#6283 | Audit based on status at 14.5.2022 6:00 UTC, fixes of several points based on status at 19.5. 6:00 UTC, published 19.5.2022 10:00 UTC.

Levels of findings: ✅ Correct > ℹ️ Informational > ⚠️ Warning > ❌ Major vulnerability
Warning: **Always check that contracts you are signing match contracts mentioned in this audit. We have no control over website UI the project provides!**

Disclaimer: This review is for informational purposes only. Although done by paid professionals, we cannot ensure code safety, only assess vulnerability to some of the known vulnerability vectors. Furthermore, the review only concerns itself with security and hard rug code. Do not take the review as an indication of the likelihood of making money with this project. For example, we have no control over project teams selling their own investments or abandoning the project. NFA, DYOR.

* * *

Link to Official Raiders of DeFi Discord server:
https://discord.gg/mGRePw9Uzn