NOTE AND RECOMMENDATION

1. In the current contract version the owner(deployer) of the contract address and the default referrer address are the same. Recommended to separate these addresses for security reasons. This does not influence the contract business logic and other investors' risks.

2. There is a retrieve ERC-20 tokens logic method present in the contract. This does not influence the contract business logic and other investors' risks as contract logic doesn't depend on ERC-20 tokens balance on the contract.

WARNING AND DICREPANCY WITH PECIFICATION

In the final contract was not found:

- Backdoors for the money withdrawal by project administrators.
- Bugs allow stealing money or block deposits/withdrawals by investors.

OPTIMIZATION POSSIBILITIES

Possibilities to decrease cost of transactions and data storage of SmartContracts.

NOTE AND RECOMMENDATION

Tips and tricks, all other issues and recommendations, as well as errors that do not
affect the functionality of the Smart-Contract

DICREPANCY WITH PECIFICATION

Sensitive warnings and discrepancy with project technical specification.

CRITICAL ISSUES

Bugs and vulnerabilities that enable theft of funds, lock access to funds without
possibility to restore it, or lead to any other loss of funds to be transferred to any party;
high priority unacceptable bugs for deployment at mainnet; critical warnings for owners,
customers or investors.

ERRORS AND BUGS

Bugs that can trigger a contract failure, with further recovery only possible through
manual modification of the contract state or contract replacement altogether; lack of
necessary security precautions; other warnings.

OUR CONTRACT REVIEW PROCESS

The contract review process pays special attention to the following:
Testing the smart contracts against both common and uncommon vulnerabilities
Assessing the codebase to ensure compliance with current best practices and industry standards.
Ensuring contract logic meets the specifications and intentions of the client.
Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
Thorough line-by-line manual review of the entire codebase by industry experts

Blockchain security tools used:
- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

LIQUIDEX

Symbol - N/A

Contract Address - 0x90a3eaf71f734edb6eacc20537bf8836235dd291

Network - Binance Smart Chain

Language - Solidity

Deployment Date - Sep-14-2023 08:05:04 PM +UTC

Verified? - Yes

Total Supply - N/A,

Status - Launched

LIQUIDEX

PROJECT DESCRIPTION

The staking platform not only offers the security of smart contracts and attractive earning options such as staking rewards and a referral program but also generates revenue through the liquidity of tokens.

The funds received on the platform are invested in these tokens, generating profits that are distributed among the platform's users. This innovative approach ensures that users can not only earn from their staking activities but also benefit from the platform's investment activities, further enhancing their overall returns.

By leveraging the potential of token liquidity, the platform creates an additional avenue for users to maximize their earnings and participate in the growth of the ecosystem

OVERVIEW

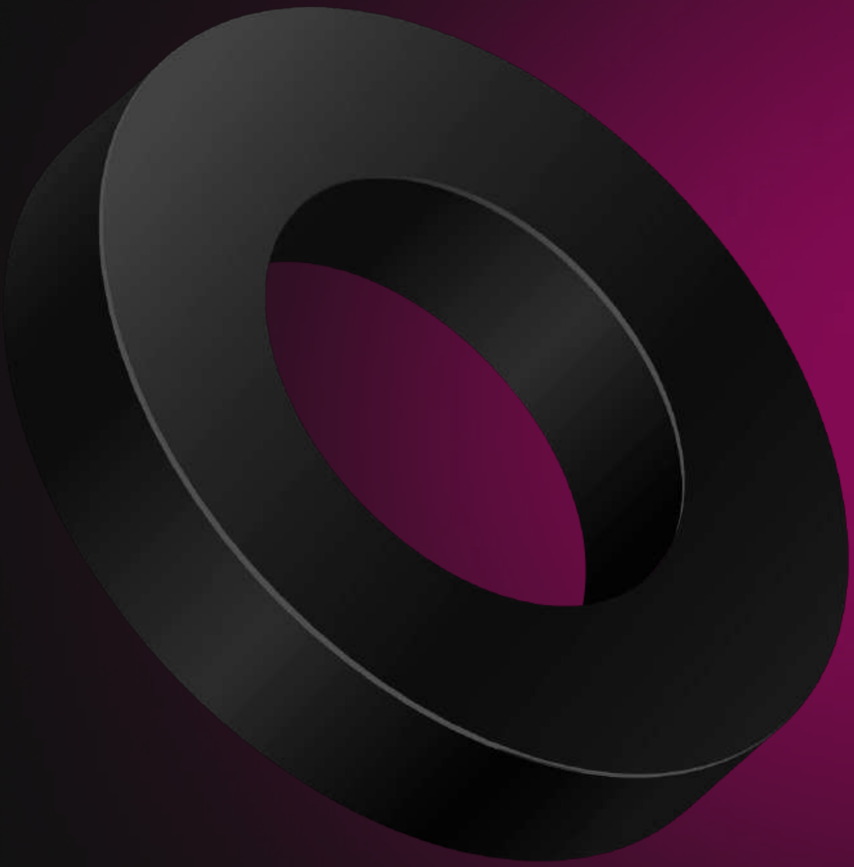
This audit has been prepared **for LiquiDex Platform** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- Contract's source code
- Owners' wallets
- Tokenomics
- Team transparency and goals
- Website's age, code, security and UX
- Whitepaper and roadmap
- Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

Smart Patrol



Security Audit

of LIQUIDEX Smart Contracts

by SmartPatrol