Audit Report for NZT48 Smart Contract

Overview

The NZT48 smart contract is a decentralized token built on the Polygon blockchain, following the ERC20 standard. It integrates transaction fee mechanisms, staking functionality, a governance voting system, and dividend distribution features. This audit aims to assess the code for security vulnerabilities, best practices compliance, and overall functionality.

Contract Details

Contract Address: 0x5062629D8D97dAb7817405e160BA2Ff9BF6A1D96

Token Name: NZT48 Token

Token Symbol: NZT48

Total Supply: 1,000,000,000 NZT48 (18 decimals)

Buy Fee: 5%

Sell Fee: 5%

Staking Lock Period: 30 days

Max Staking Reward: 50,000 NZT48

Key Features

Fee Distribution:

10% to Marketing Wallet

60% to Liquidity Wallet

20% to Dividend Wallet

10% Burned

Staking: Users can stake their tokens with a 30-day lock period to earn rewards.

Voting Mechanism: Token holders can create and vote on proposals related to fee changes and governance.

Dividend Distribution: Eligible holders receive dividends based on their token holdings.

Emergency Withdrawals: The contract owner can withdraw ETH from the contract.

Security Analysis

Reentrancy Protection: The contract uses OpenZeppelin's ReentrancyGuard to secure functions like withdrawStakedTokens and withdrawDividends.

Access Control: Critical functions are restricted to the contract owner to prevent unauthorized access.

Voting Limits: There are restrictions on vote frequency and total votes per address to ensure fair governance.

Fee Adjustment Cooldown: Prevents frequent fee changes to avoid malicious behavior.

Safe Math: Uses Solidity 0.8.x, which has built-in overflow and underflow protection.

Gas Optimization: Efficient use of mappings and arrays, though dividend logic could be further optimized.

Error Handling: Clear require statements ensure smooth operations and transparency.

Recommendations

Weighted Voting: Consider implementing a system where voting power is proportional to token holdings.

Dynamic Fee Structure: Allow fee adjustments based on market conditions or token performance.

Regular Security Audits: Engage external security firms to maintain contract security.

Conclusion

The NZT48 smart contract is well-structured, incorporating key features that enhance functionality and security. While the contract provides a solid foundation, implementing the recommended improvements will further strengthen its robustness and user trust. Continuous monitoring and updates will be essential to maintain security and adapt to evolving standards in the DeFi space.

Appendix

Version: Solidity 0.8.28

Libraries Used: OpenZeppelin Contracts (ERC20, ReentrancyGuard, Ownable)

Audit Date: October 13, 2024

Auditor: CERTIFY

www.certify.services