INVARIANT AUDITING
SOLUTIONS

PEPE Token Smart Contract Audit

Executive Summary

PEPE Token, an ERC20-compliant token on the Ethereum blockchain, is deployed at the location https://etherscan.io/address/0x6982508145454ce325ddbe47a25d4ec3d2311933.

The token's smart contract includes administrative functions exclusive to privileged users, which will be thoroughly reviewed in the ensuing sections.

The total token supply of PEPE is fixed at an upper limit of 420,690,000,000,000 tokens. There has been a marginal reduction in the token supply owing to an insignificant degree of token burn activity.

Initially, the token presented issues related to centralization of administrative authority. However, these issues have been mitigated subsequent to the renouncement of ownership by the token deployer.

The token transfers performed by the PEPE token deployer matches the allocation described on its website and whitepaper.

Methodology

Tools used

1. Static analysis: mythril, slither
2. Manual inspection: code and unit tests
3. Invariant violation testing: echidna fuzzing

Token Information

Chain	Ethereum
Token Address	0x6982508145454ce325ddbe47a25d4ec3d2311933
Name	Pepe
Symbol	PEPE
Decimals	18

Vulnerability Checklist

Reentrancy Vulnerability	No
Arithmetic Overflow Underflow	No
Dead-code	No
Upgradeable Contract	No
Arbitrary Contract Call	No
Arbitrary Storage Write	No
Delegate Call to Arbitrary Contract	No
Low-level Calls	No
Dependence on Predictable Variables	No
Signature Verification	No
Unbounded Loops	No
Improper Events	No
Improper Authorization Design	No
Oracle Issues	No
Logical Issues	No
Centralization Issues	No

Centralization Issues

Does the contract contain admin-only functions?	Yes
Are the admin-only functions standard?	No
Does the token contain a black or block list?	Yes
Does the token allocation match the whitepaper?	Yes

Exclusive Admin-only Functions

The PEPE token was launched by the address **0xfbfeaf0da0f2fde5c66df570133ae35f3eb58c9a**, which will henceforth be referred to as the 'PEPE deployer'.

The PEPE token contract adheres to the standard specifications of an ERC20 contract.

However, it also integrates non-standard administrative-exclusive functions, namely **'setRule'** and **'blacklist'**.

'setRule' Function Description

The **'setRule'** function governs the transferability of initial liquidity from the UniswapV2 PEPE-ETH pool to any potential PEPE token holder.

The stages of liquidity and transfer restrictions for PEPE have evolved as follows:

1. Initially, PEPE could only be transferred to and from the token owner account.
2. Subsequently, the deployer set a rule where users buying PEPE from the initial liquidity in the UniswapV2 PEPE-ETH pool must hold between 84 billion and 252 billion PEPE tokens. Apart from this condition, tokens could be transferred without restrictions.
3. Ultimately, the deployer lifted all restrictions on PEPE purchase and transfer.

Immediately following the deployment of the PEPE token and before the first invocation of **'setRule'**, all transfers not involving the token owner were blocked.

During the Ethereum blocks 17047544 through 17047929, the liquidity in the UniswapV2 PEPE-ETH pool was in a "limited" state. Buyers were required to hold a minimum of 84 billion PEPE and a maximum of 252 billion PEPE tokens.

All restrictions were removed by the PEPE deployer in Ethereum block 17047929.

On-chain setRule calls

setRule(bool _limited, address _uniswapV2Pair, uint256 _maxHodlingAmount, uint256 _minHoldingAmount)	
Time and TxHash	**Call**

Apr-14-2023 07:46:47 PM +UTC	setRule(_limited=true, _uniswapV2Pair=0xa43fe16908251ee70ef74718545e4fe6c5ccec9f, _maxHodlingAmount=252414000000000000000000000000, _minHoldingAmount=841380000000000000000000000000)
0x23e6f40d4a2c973e53d3e2a282225c630f64f23746c8295de710f578d240c699	
Apr-14-2023 09:07:59 PM +UTC	setRule(_limited=false, _uniswapV2Pair=0xa43fe16908251ee70ef74718545e4fe6c5ccec9f, _maxHodlingAmount=0, _minHoldingAmount=0)
0x6a1dea2dccb315a6bab936b2b173ac871e0aa0fc095f9893572430a775b80eb1	

'blacklist' Function Description

The administrative-exclusive **'blacklist'** function has the ability to regulate the transfer of PEPE tokens to and from a specified address.

It is noteworthy that this function was invoked only once prior to the PEPE deployer relinquishing ownership of the contract. The address subjected to the blacklist operation is **0xaf2358e98683265cbd3a48509123d390ddf54534**.

On-chain blacklist calls

blacklist(address _address, bool _isBlacklisting)	
Time and TxHash	**Call**
Apr-14-2023 07:54:11 PM +UTC	blacklist(_address=0xaf2358e98683265cbd3a48509123d390ddf54534, _isBlacklisting=true)
0xb162f87a3f4eb22f06573049967187fedbcd33a34a99c740dd98c261ce207e21	

Transfer of Ownership

As previously discussed, the PEPE contract includes functions that are solely accessible by the administrator. These functions can only be invoked by the contract owner, which at any given point can only be a single address.

From Ethereum block 17046105 until block 17047934, the PEPE token contract was under the ownership of the PEPE deployer. Subsequently, the PEPE deployer relinquished their ownership, rendering the administrative-exclusive functions uncallable by any party.

On-chain renounceOwnership calls

renounceOwnership()	
Time and TxHash	**Call**
Apr-14-2023 09:08:59 PM +UTC	renounceOwnership()
0x91c9a6caf8e7b5419a7e597982a0cf9b4fc01413279ab840bb57a2e9c528f252	

ERC20 Implementation

The core ERC20 functionality of the PEPE token utilizes code from the OpenZeppelin library version 4.4.0, specifically the **'ERC20.sol'** and **'Ownable.sol'** modules. Consequently, its core implementation is based on well-reviewed and extensively tested code.

Accordingly, the manual review was primarily concentrated on the custom logic encapsulated within **'PepeToken.sol'**, as detailed earlier in this report.

Token Supply and Liquidity Provisioning

The PEPE token generated its entire supply within the transaction where it was deployed. The recipient of all these minted tokens was the PEPE deployer.

It is important to note that the supply of PEPE tokens cannot increase post-deployment, because no mechanism to mint new tokens is present in the token contract.

During the deployment of the token, the PEPE token minted its full potential supply, amounting to 420,690,000,000,000 tokens, which were credited to the PEPE deployer. This happened on April 14, 2023, 02:51:35 PM +UTC, in transaction https://etherscan.io/tx/0x2afae7763487e60b893cb57803694810e6d3d136186a6de6719921afd7ca304a.

Subsequently, the PEPE Deployer provided liquidity to the UniswapV2 PEPE-ETH pool by committing 93.1% of the tokens and 2 ETH. This action resulted in a return of 27,987,939.902750970427665813 Liquidity Provider (LP) tokens. This happened on April 14, 2023, 05:21:11 PM +UTC in transaction https://etherscan.io/tx/0x273894b35d8c30d32e1ffa22ee6aa320cc9f55f2adbba0583594ed47c031f6f6

The LP tokens were then transferred to the PEPE token contract by the PEPE deployer on Apr 14, 2023 05:21:11 PM +UTC in transaction https://etherscan.io/tx/0x4b950490c13cee92d8fadb8280c6220dc414f5cc23835e9295ec4a836fe23c86

The PEPE token contract does not contain any code that would allow the transfer or withdrawal of ERC20 tokens held at the token address. This effectively renders the UniswapV2 LP tokens inoperative.

Missing Desirable Features

The PEPE token lacks support for ERC-2612: Permit Extension for EIP-20 Signed Approvals specification. Thus it does not support gasless transactions using signed messages from the token holder, unlike e.g. USDC and DAI.