

SKELETON ECOSYSTEM

SMART CONTRACT AUDIT



OFFICIAL SCAM COIN
SCAM
SOL

J8wM2nDdDCAbU5ubuCeBdBJrk7strxtfcjhTHMtmpump



Table of Contents

Table of Contents	1
Disclaimer	2
Overview	3
Creation/Audit Date	3
Verified Socials	3
Contract Functions Analysis	4
Details of Findings	6
Metaplex Metadata Informations	8
URI Metadata Informations	7
Detected Vulnerabilities	9
Audit Scope	12

Global Disclaimer

This document serves as a disclaimer for the crypto smart contract audit conducted by Skeleton Ecosystem. The purpose of the audit was to review the codebase of the smart contracts for potential vulnerabilities and issues. It is important to note the following:

Limited Scope: The audit is based on the code and information available up to the audit completion date. It does not cover external factors, system interactions, or changes made after the audit. The audit itself can not guarantee 100% safety and can not detect common scam methods like farming and developer sell-out.

No Guarantee of Security: While we have taken reasonable steps to identify vulnerabilities, it is impossible to guarantee the complete absence of security risks or issues. The audit report provides an assessment of the contract's security as of the audit date.

Continued Development: Smart contracts and blockchain technology are evolving fields. Updates, forks, or changes to the contract post-audit may introduce new risks that were not present during the audit.

Third-party Code: If the smart contract relies on third-party libraries or code, those components were not thoroughly audited unless explicitly stated. Security of these dependencies is the responsibility of their respective developers.

Non-Exhaustive Testing: The audit involved automated analysis, manual review, and testing under controlled conditions. It is possible that certain vulnerabilities or issues may not have been identified.

Risk Evaluation: The audit report includes a risk assessment for identified vulnerabilities. It is recommended that the development team carefully reviews and addresses these risks to mitigate potential exploits.

Not Financial Advice: This audit report is not intended as financial or investment advice. Decisions regarding the use, deployment, or investment in the smart contract should be made based on a comprehensive assessment of the associated risks.

By accessing and using this audit report, you acknowledge and agree to the limitations outlined above. Skeleton Ecosystem and its auditors shall not be held liable for any direct or indirect damages resulting from the use of the audit report or the smart contract itself.

Please consult with legal, technical, and financial professionals before making any decisions related to the smart contract.

Overview

Contract Name	Official Scam Coin
Ticker/Symbol	SCAM
Blockchain	Solana
Contract Address	J8wM2nDdDCAbU5ubuCeBdBJrk7strxtfcjhTHMtmpump
Creator Address	2cPeiD5utGcgfL4CZcfBGrZixZ14gvYeL2Yi6hTVq46k
Update Authority	TSLvdd1pWpHVjahSpsvCXUbgwsL3JAcvokwaKt1eokM
Total Supply	1.000.000.000 SCAM
Current Supply	998,972,574.77 SCAM
Decimals	6




Creation/Audit




Contract Deployed	22.01.2025
Audit Created	28.01.2025
Audit Update	V 1.0

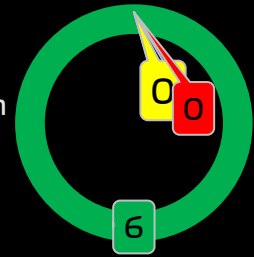
Verified Socials

Website	https://officialscamcoin.com
Telegram	https://t.me/theofficialscamcoin
Twitter (X)	https://x.com/scamcoinofc

Contract Function Analysis

 Pass
  Attention Item
  Risky Item

 Pass
 Attention
 Risk



Contract Ownership	Renounced	
Buy Tax	0 %	
Sell Tax	0 %	
Liquidity Status		100% of the Added SPL Tokens are Burned
Firts LP Added		29% % of Total supply
Freeze Authority	 Revoked	Authorised owner can "freeze" the tokens inside a wallet. So the owner of the tokens would not be able to move/transfer/sell them to a different wallet.
Metadata Update Authority	 Revoked	The metadata of the token like Name, logo, website, socials can be changed. Doesn't mean the token is a scam but can be confusing to rebrand a token like it were a new one.
Mint authority	 Revoked	Mint functions may increase the amount of tokens in circulation and effect the price of the token. Owner can mint new tokens for any account and sell.

 **Passed:** All possible issues regarding this function are fixed.

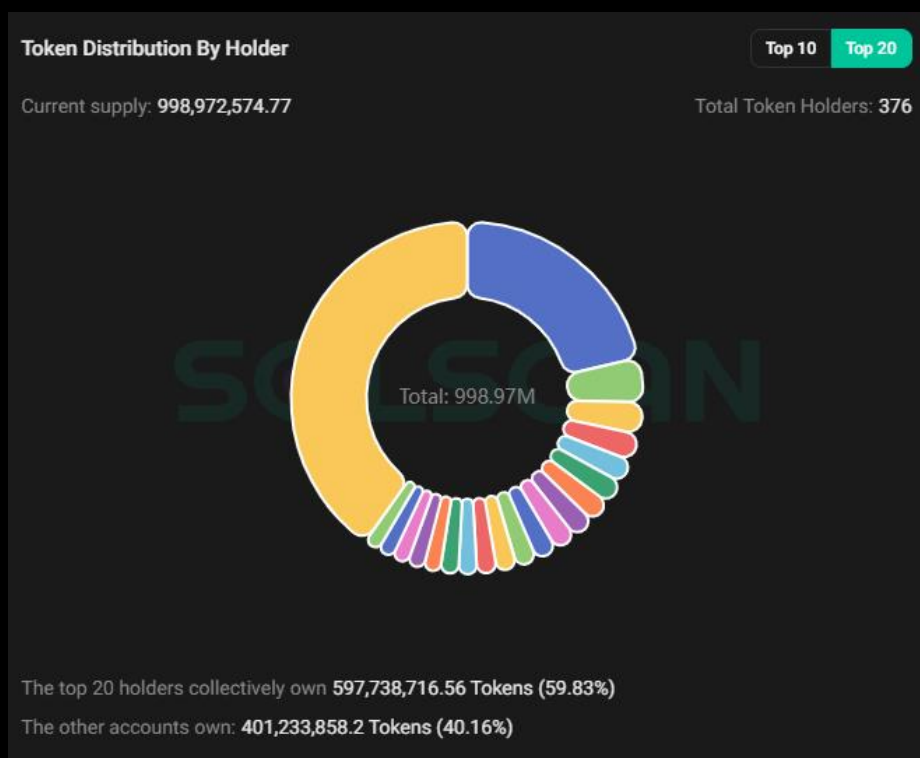
⚠ **Attention Item:** Can cause problems or may result in manipulation

⚠ **Risky Item:** High possibility of manipulation, asset loss.

Details of Risk - Attention Items

No Items

Holder distribution on 28.01.2025



Metaplex Metadata Informations

The Token Metadata program is one of the most important programs when dealing with NFTs on the Solana blockchain. Its main goal is to attach additional data to Fungible or Non-Fungible Tokens on Solana.

To learn more: <https://developers.metaplex.com/token-metadata>

Key	6	
Update Authority	TSLvdd1pWpHVjahSpsvCXUbgwsL3JAcvokwaKt1eokM	The public key that has permissions to update this account
Mint	J8wM2nDdDCAbU5ubuCeBdBJrk7stxrtfcjhTHMtmpump	The public key of the Mint Account
Name	Official Scam coin	The on-chain name of this token
Symbol	SCAM	The on-chain symbol of this token
URI	https://ipfs.io/ipfs/QmNSVTko5bfjY5RUPLHGyCrGDBpuznK4Dom2dQLQSs7VLo	Key of external metadata. Points to an off chain JSON file contains additional data
Seller Basis Points	0	
Primary Sale Happened	0	Indicator shows the token were sold or not. 0 = false 1= true (bool)
IsMutable	0	Indicator shows the metadata can be updated or not. 0 = false 1= true (bool)
EditionNonce	255	Identifier
Tokenstandard	2	The token standard

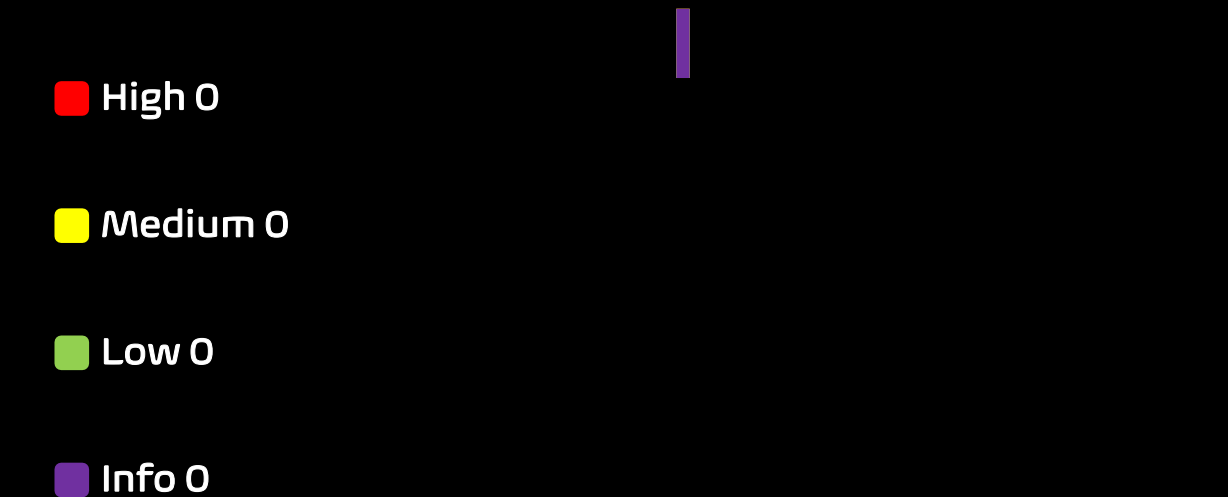
```
{ 8 items
  key: 4
  updateAuthority: "TSLvdd1pWpHVjah5psvCXUbgwL3JAcvolwaktleokM"
  mint: "J8wM2nDdDCAbU5ubuCeBdBJrk7strxtfcjhTHttmpump"
  data: { 4 items
    name: "Official Scam Coin"
    symbol: "SCAM"
    uri: "https://ipfs.io/ipfs/QmNSVTko5bfjY5RUPLHGyCrGDBpuznK4Dom2dQLQs7VLo"
    sellerFeeBasisPoints: 0
  }
  primarySaleHappened: 0
  isMutable: 0
  editionNonce: 255
  tokenStandard: 2
}
```

URI Metadata Informations

<https://ipfs.io/ipfs/QmNSVTko5bfjY5RUPLHGyCrGDBpuznK4Dom2dQLQs7VLo>

```
{
  "name": "Official Scam Coin",
  "symbol": "SCAM",
  "description": "The Official Scam Coin.\r\nLet's celebrate crypro scammers together!",
  "image": "https://ipfs.io/ipfs/QmTNzYifUMvxEvFa5kwatnzZQHPnFv2QeRoMyvuVkf1uKe",
  "showName": true,
  "createdOn": "https://pump.fun",
  "twitter": "https://x.com/scamcoinofc",
  "telegram": "https://t.me/theofficialscamcoin",
  "website": "https://officialscamcoin.com"
}
```


Detected Vulnerabilities



High Severity Issues: High possibility to cause problems, need to be resolved.

Medium Severity Issue: Will likely cause problems, recommended to resolve.


Low Severity Issues: Won't cause problems, but for improvement purposes could be adjusted.

Informational Severity Issues: Not harmful in any way, information for the developer team.


 **High severity Issues: (0)**

 **Medium severity issues: (0)**


 **Low severity issues: (0)**

 **Informational severity issues: (0)**

Detected High and Medium Severity Vulnerability Description

 None

Audit Result

 Passed

Audit Scope

Audit Method.

Our smart contract audit is an extensive methodical examination and analysis of the smart contract's code that is used to interact with the blockchain. Goal: discover errors, issues and security vulnerabilities in the code. Findings getting reported and improvements getting suggested.

Automatic and Manual Review

We are using automated tools to scan functions and weaknesses of the contract. Transfers, integer over-undeflow checks such as all CWE events.

Tools we use:

Solscan
CWE
SWC
Solidity Scan
SVD

In manual code review our auditor looking at source code and performing line by line examination. This method helps to clarify developer's coding decisions and business logic.

Skeleton Ecosystem

<https://skeletonecosystem.com>

<https://github.com/SkeletonEcosystem/Audits>

