Cyberscope

Audit Report
Bee On Sol

April 2024

Network	SOL
Type	SPL-Token
Address	42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz
Audited by	© cyberscope

Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor / Informative

Severity	Code	Description	Status
🟠	UA	Update Authority	Unresolved
⚪	ITA	Initial Token Allocation	Unresolved

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz
Fixed Supply	420,000,000
Token Address	42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz
Token name	Bee On Sol (BOS)
Owner Program	Token Program
Decimals	9
MintTokens Authority	Revoked
FreezeAccount Authority	None
Metadata File Type	JSON
Badge Eligibility	Yes

Audit Updates

Initial Audit	06 Apr 2024

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz#metadata

Overview

The `Bee On Sol` token symbolized as `BOS`, is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain, with a fixed supply of `420,000,000` tokens since the mint has been disabled. This ensures a stable and unchangeable total supply, enhancing its value proposition within the ecosystem. The token uses the URL https://bafkreicarfldzfpk5qqtnsjyxmnbleuq354rfesrphnd5glyesa7sgyc3i.ipfs.nftstorage.link, which points to a decentralized storage service while the https://bafkreichwkruvqwjtfcezjawq5smcrw4lvloopp6jyl4o2oi6epkxna4wu.ipfs.nftstorage.link image is used for visual identification of the token across various platforms and marketplaces. Overall, the project is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

the contract's mint authority have been renounced. The information regarding the transaction can be accessed through the following link: https://solscan.io/tx/3mCexr53yBjLc65Brs3Ho4mssfQ9amPaSZy1SphjU4ppHu6f4TaPY4Z6boybve1uhHxdwVtqxicnLCBJ4eKdKrvH

Metadata

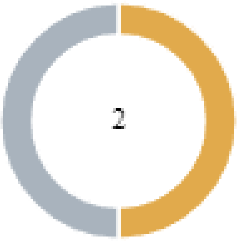
The Metaplex Metadata provides details of the characteristics of the `Bee On Sol` token, a distinctive digital asset on the Solana blockchain tailored for utilizing the Metaplex Metadata. This metadata includes crucial information necessary for the asset's seamless integration and operation within the Solana ecosystem. Specifically, the update authority attribute specifies the account `GiYQjaygcYS3JvM7PQcFs3QGQ4ZbfibnWCW57hNTVCcX` authorized to modify the metadata. The mint attribute specifies the account `42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz` authorized for the initial token mint. The asset imposes a seller fee of 0 basis points, indicating no transaction fee for trading was set in the deploying phase. The metadata indicates that the asset has not yet undergone its primary sale (`primarySaleHappened` : 0) and is marked as mutable (`isMutable` : 1), allowing for future changes to the metadata. An `editionNonce` of 254 denotes a unique edition, and the asset conforms to a specific token standard within the Solana network (`tokenStandard` : 2), ensuring its compatibility and standardization across the platform. This detailed metadata structure offers a comprehensive overview of `Bee On Sol` key features and its operational framework within the Metaplex ecosystem on Solana.

```json
{
  "key": 4,
  "updateAuthority": "GiYQjaygcYS3JvM7PQcFs3QGQ4ZbfibnWCW57hNTVCcX",
  "mint": "42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz",
  "data": {
    "name": "Bee On Sol",
    "symbol": "BOS",
    "uri":
"https://bafkreicarfldzfpk5qqtnsjyxmnbleuq354rfesrphnd5glyesa7sgyc3i.ipfs.nftstorage.link",
    "sellerFeeBasisPoints": 0
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 254,
  "tokenStandard": 2
}
```

Field	Value	Description
key	4	Account discriminator that identifies the type of metadata account
updateAuthority	GiYQjaygcYS3JvM7PQcFs3QGQ4ZbfibnWCW57hNTVCcX	The public key that is allowed to update this account
mint	42awNZ2DgW3T7G2TbwLuEyq5ujG9bpcMHpm3cAHEP6Pz	The public key of the Mint Account it derives from
name	Bee On Sol	The on-chain name of the token
symbol	BOS	The on-chain symbol of the token
uri	https://bafkreicarfldzfpk5qgtnsjyxmnbleuq354rfesrphnd5glyesa7sgyc3i.ipfs.nftstorage.link	The URI to the external metadata. This URI points to an off-chain JSON file that contains additional data following a certain standard
sellerFeeBasisPoints	0	The royalties shared by the creators in basis points — This field is used by most NFT marketplaces, it is not enforced by the Token Metadata program itself
primarySaleHappened	0	A boolean indicating if the token has already been sold at least once. Once flipped to True, it cannot ever be False again. This field can affect the way royalties are distributed
isMutable	1	A boolean indicating if the metadata account can be updated. Once flipped to False, it cannot ever be True again
editionNonce	254	Unique identifier for this edition

tokenStandard	2	The standard of the token

Findings Breakdown



●	Critical	0
●	Medium	1
●	Minor / Informative	1

	Severity	Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	1	0	0	0
●	Minor / Informative	1	0	0	0

UA - Update Authority

Criticality	Medium
Status	Unresolved

Description

The contract is set up in a way that grants the update authority, with the address `GiYQjaygcYS3JvM7PQcFs3QGQ4ZbfibnWCW57hNTVCcX` , continued access to alter key metadata fields. This situation leaves the token exposed to potential hazards, as this address has the power to adjust critical attributes such as the token's name, symbol, and image. Without revoking these privileges from the update authority, there's a risk of unauthorized or harmful changes that could undermine the token's integrity and its intended use.

Recommendation

It is recommended to revoke the update authority privileges. This action would ensure a consistent security posture across the contract's operational aspects, eliminating the discrepancy that currently allows for undue modification privileges. Implementing this recommendation would align the contract's security measures, providing a more robust defense against unauthorized changes and enhancing the overall security of the contract's operational environment.

How to revoke the Update Authority:
https://www.quicknode.com/guides/solana-development/anchor/how-to-make-immutible-solana-programs#remove-the-update-authority-of-a-solana-program

ITA - Initial Token Allocation

Criticality	Minor / Informative
Status	Unresolved

Description

The account `51h33NEqfF9oWDfYN17RGkbTRevZ7ZTBY2ZCx8u22vbU` holds a large portion of the total supply. This concentration of a huge supply in one address raises significant concerns about centralization within the token's ecosystem. Such a scenario creates a risk of market manipulation and could lead to other adverse effects, potentially undermining the token's decentralized nature and the overall health of its ecosystem.

Account	Token Account	Quantity	Percentage
51h33NEqfF9oWDfYN17RGkbTRevZ7ZTBY2ZCx8u22vbU	deSpfS65gCQcZZj9QoNcjuUAhhnPrLWKdDpew6r2Hfz	374,094,000	89.07%

Recommendation

It is recommended to distribute the tokens more broadly to achieve a more decentralized token holding structure. This can mitigate the risks associated with centralization and ensure a more stable and secure ecosystem for all participants. If the new address consists of a team's wallet address, then the team should carefully manage the private keys of that account. We strongly recommend implementing a robust security mechanism to prevent a single user from accessing the contract admin functions, such as a multi-sign wallet so that many addresses will confirm the action.

Summary

The "Bee On Sol" token, built on the Solana network, implements a robust smart contract structure that was initialized using the Token program, with analysis revealing 1 medium and 1 minor/informative issue.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io