Cyberscope

Audit Report

DigiCask

February 2024

Network	SOL
Type	SPL-Token
Address	64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW
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	Unresolved
●	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
●	CR	Centralization Risk	Unresolved

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW
Fixed Supply	1,000,000,000
Token name	DigiCask Token (DCASK)
Token address	64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW
Owner Program	Token Program
Decimals	9
Signature	e3q7Abz6woA7Zu1ErcSRofqz18p8yoipETCZmkDCpPudRAfLwZfibVTZAEs2yPdBcyCScFm4XFnZktTVvLXJKDV
Block	#249563757
Deploy Time	February 21, 2024 16:12:09 Eastern European Standard Time
Instructions	Create Account, Mint
By	4chffxTvaMJMSscFaTFMUPE7dnwgVHbnq9ompm1hnqmH
MintTokens Authority	None
FreezeAccount Authority	None
Metadata File Type	JSON
Name	DigiCask Token
Symbol	DCASK
Description	Offcial token of the DigiCask tokenization platform.

Image	https://quicknode.quicknode-ipfs.com/ipfs/QmVzeq9bq1v3u29JRbcG8iJssfhfayvWJ47F7CoHDBhpY6
Total Transfers (At the time of the report)	0
Total Transactions (At the time of the report)	3
Total Holders (At the time of the report)	1

Audit Updates

Initial Audit	26 Feb 2024

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW#metadata

Overview

The DigiCask Token, symbolized as DCASK, is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain. The DigiCask Token token has a fixed supply of 1,000,000,000 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 image URL https://quicknode.quicknode-ipfs.com/ipfs/QmVzeq9bq1v3u29JRbcG8iJssfhfayvWJ47F7CoHDBhpY6, which points to an image hosted on Quicknode, a decentralized storage service. This image is used for visual identification of the token across various platforms and marketplaces. Overall, the DigiCask Token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Transactions

At the time of this report, the transactions of the DigiCask Token token are as follows:

Signature	Block	Time	Instructions	By	Fee (SOL)
552AFdwA8NM4GNzdAqhkuALkrmeuKacwt38ADGUS3RN2XV92UTao2Ezoidv7LzYwCr4JBPFFX4XExkFXcdnSfnxT	#249565111	02-21-2024 16:21:30	SetAuthority	dcask-...er.sol	0.000005
2PNjXjf8Rqh1K5Nec3C6QvAgXXJvfUzCMMu8NcmDe18gA6XLFETpQcKGVzEkLDNNZB1hcvVkLi3fPhpP3cTYSs1f	#249565049	02-21-2024 16:21:05	SetAuthority	dcask-...er.sol	0.000005
e3q7Abz6woA7Zu1ErcSRofqz18p8yoipETCZmkDCpPudRAfLwZfibVTZAEs2yPdBcyCScFm4XFnZktTVvLXJKDV	#249563757	02-21-2024 16:12:09	Create, Mint	dcask-...er.sol	0.00001

Holders

At the time of this report, the distribution of DigiCask Token token holders is as follows:

#	Token Account	Quantity	Percentage
1	GVr3VBtMa9Lq3MVDRqDmAy3MjUdJKaegkLJ6n3PyShZz	1,000,000,000	100%

Metadata

MetaplexMetadata

The Metaplex Metadata provides details of the characteristics of the `DigiCask Token` token which uses the `DCASK` symbol, 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. The `updateAuthority` field is designated to the account capable of modifying this metadata, identified by the public key `4chffxTvaMJMSscFaTFMUPE7dnwgVHbnq9ompm1hnqmH`. Furthermore, the mint attribute specifies the account `64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW` authorized for the initial token mint.

```
{
  "key": 4,
  "updateAuthority": "4chffxTvaMJMSscFaTFMUPE7dnwgVHbnq9ompm1hnqmH",
  "mint": "64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW",
  "data": {
    "name": "DigiCask Token",
    "symbol": "DCASK",
    "uri":
"https://quicknode.quicknode-ipfs.com/ipfs/QmWTU5BC5AocSFNJPNhsyoRpkRnD
Aut1KLTuyS3wYQvcP2",
    "sellerFeeBasisPoints": 0,
    "creators": [
      {
        "address": "4chffxTvaMJMSscFaTFMUPE7dnwgVHbnq9ompm1hnqmH",
        "verified": 1,
        "share": 100
      }
    ]
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 255,
  "tokenStandard": 2,
  "name": "DigiCask Token",
  "symbol": "DCASK",
  "description": "Offcial token of the DigiCask tokenization
platform.",
  "image":
"https://quicknode.quicknode-ipfs.com/ipfs/QmVzeq9bq1v3u29JRbcG8iJssfhf
ayvWJ47F7CoHDBhpY6"
}
```


Metadata description

The `data` section within the metadata discloses the asset's name as "DigiCask Token", its trading symbol as "DCASK", and a URI pointing to "https://quicknode.quicknode-ipfs.com/ipfs/QmWTU5BC5AocSFNJPNhsyoRpkRnDAut1KLTuyS3wYQvcP2". Notably, 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 `255` 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 "DigiCask Token's" key features and its operational framework within the Metaplex ecosystem on Solana.

Field	Value	Description
key	4	Account discriminator that identifies the type of metadata account
updateAuthority	4chffxTvaMJMSscFaTFMUPE7dnwgVHbnq9ompm1hnqmH	The public key that is allowed to update this account
mint	64sad4VPVkoSARy9juUw1stfpGg5TkRCm4TpRRLb4WEW	The public key of the Mint Account it derives from
Name	DigiCask Token	The on-chain name of the token
Symbol	DCASK	The on-chain symbol of the token
Uri	https://quicknode.quicknode-ipfs.com/ipfs/QmWTU5BC5AocSFNJPNhsyoRpkRnDAut1KLTuyS3wYQvcP2	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	255	Unique identifier for this edition
tokenStandard	2	The standard of the token
description	Offcial token of the DigiCask tokenization platform.	Description of the asset
image	https://quicknode.quicknode-ipfs.com/ipfs/QmVzeq9bq1v3u29JRbcG8iJssfhfayvWJ47F7CoHDBhpY6	URI pointing to the asset's logo

Findings Breakdown

Critical	2
Medium	0
Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	2	0	0	0
Medium	0	0	0	0
Minor / Informative	1	0	0	0

ELFM - Exceeds Fees Limit

Criticality	Critical
Location	DigiCask Token
Status	Unresolved

Description

The update authority has the ability to increase the fees over the allowed limit of 25%. The update authority may take advantage of it by setting the `sellerFeeBasisPoints` variable to a high percentage value.

Recommendation

The contract could embody a check for the maximum acceptable value. The team should carefully manage the private keys of the update authority's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract's features.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a multi-signature wallet so that many addresses will confirm the action.

Permanent Solution:

- Revoke the update authority, which will eliminate the threats but it is non-reversible.

UA - Update Authority

Criticality	Critical
Location	DigiCask Token
Status	Unresolved

Description

The contract is currently configured in a manner that allows the update authority, identified by the address `4chffxTvaMJMSscFaTFMUPE7dnwgVHbnq9ompm1hnqmH`, to retain privileges that enable the modification of crucial metadata fields. This situation arises despite the revocation of authorities related to Mint and Freeze functionalities, which was done to enhance security and reduce the risk of unauthorized alterations. However, the failure to revoke the `update` authority in a similar manner leaves the token vulnerable to potential risks, as the designated address retains the capability to make changes to the metadata. This oversight could lead to unauthorized or malicious modifications that might compromise the integrity and intended functionality of the token.

Recommendation

It is recommended to revoke the `update` authority privileges in the same manner as the authority was revoked for the `Mint` and `Freeze` authorities. 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.

CR - Centralization Risk

Criticality	Minor / Informative
Location	DigiCask Token
Status	Unresolved

Description

The token account `GVr3VBtMa9Lq3MVDRqDmAy3MjUdJKaegkLJ6n3PyShZz` , holds the entire supply of the DCASK token. Following the deployment, all tokens were transferred to this single account. Consequently, this address now owns the entire token supply, amounting to 1,000,000,000 `DCASK` . This concentration of the entire token 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.

Token Account	Quantity	Percentage
GVr3VBtMa9Lq3MVDRqDmAy3MjUdJKaegkLJ6n3PyShZz	1,000,000,000	100%

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 "DigiCask Token" token, built on the Solana network, implements a robust smart contract structure that was initialized using the Token program, with analysis revealing 2 critical issues.

The contract's mint authority has been renounced. The information regarding the transaction can be accessed through the following link:

https://solscan.io/tx/2PNjXjf8Rqh1K5Nec3C6QvAgXXJvfUzCMMu8NcmDe18gA6XLFETpQcKGVzEkLDNNZB1hcvVkLi3fPhpP3cTYSs1f.

The contract's freeze authority has also been renounced. The information regarding the transaction can be accessed through the following link:

https://solscan.io/tx/552AFdwA8NM4GNzdAqhkuALkrmeuKacwt38ADGUS3RN2XV92UTao2Ezoidv7LzYwCr4JBPFFX4XExkFXcdnSfnxT.

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