Cyberscope

Audit Report
Catwifhat

June 2024

Network	SOL
Type	Token 2022
Address	7atgF8KQo4wJrD5ATGX7t1V2zVvykPJbFfNeVf1icFv1
Audited by	© cyberscope

Analysis

● Critical   ● Medium   ● Minor / Informative   ● Pass

Severity	Code	Description	Status
●	STPMTA	Mint Authority	Passed
●	STPFRA	Freeze Authority	Passed
●	STPUPA	Update Authority	Passed
●	RWWA	Renounced Withdraw Withheld Authority	Acknowledged

Table of Contents

Review

Network	Solana
Address	7atgF8KQo4wJrD5ATGX7t1V2zVvykPJbFfNeVf1icFv1
Explorer	https://solscan.io/address/7atgF8KQo4wJrD5ATGX7t1V2zVvykPJbFfNeVf1icFv1
Name	catwifhat
Symbol	$CWIF
Decimals	2
Total Supply	34,978,158,080,924.04
Metadata File Type	JSON
Owner Program	https://solscan.io/account/TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb
Badge Eligibility	Yes

Audit Updates

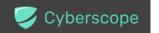| Initial Audit	20 Jun 2024

Overview

The catwifhat token symbolized as $CWIF, is a distinguished SPL (Solana Program Library) token initialized using the `TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb` Token 2022 Program on the Solana blockchain, with a supply of 34,978,158,080,924.04 tokens. The token uses the URL https://bafkreib5jykd5ehlvmi7f253jdjzzknj6eqlnqhzenfmdc6okrwksqfu6a.ipfs.nftstorage.link, which points to a decentralized storage service, while the https://bafkreigmg552j5o5qv5ra6hvg4by4qzjjichzsyaljhmyvwe5qkjphgxoi.ipfs.nftstorage.link image is used for visual identification of the token across various platforms and marketplaces. Overall, the solana token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Field	Value	Description
updateAuthority	7kpmtHX9Nr29687jeMcLZ JMpAewUbAWBeqeQhDh HJ3Kn	The public key that is allowed to update this account
mint	7atgF8KQo4wJrD5ATGX7t 1V2zVvykPJbFfNeVf1icFv1	The public key of the Mint Account it derives from
name	catwifhat	The on-chain name of the token
symbol	$CWIF	The on-chain symbol of the token
uri	https://bafkreib5jykd5ehlv mi7f253jdjzzknj6eqlnqhzen fmdc6okrwksqfu6a.ipfs.nft storage.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	400	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	false	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	false	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

Metadata

The Metaplex Metadata provides details of the characteristics of the `catwifhat` , 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 asset imposes `sellerFeeBasisPoints` of 400 basis points, indicating a 4% transaction fee for trading is set. The metadata indicates that the asset has not yet undergone its primary sale as indicated by the `primarySaleHappened` value set to 0, and it is marked as immutable since `isMutable` is 0, not allowing for future changes to the metadata. The `editionNonce` of 254 signifies a unique edition, while the `tokenStandard` of 2, aligns with a specified token standard within the Solana blockchain, ensuring its compatibility and standardization across the network. This detailed metadata structure offers a comprehensive overview of the token's key features and its operational framework within the Metaplex ecosystem on Solana.

```
{
  "key": 4,
  "updateAuthority": "7kpmtHX9Nr29687jeMcLZJMpAewUbAWBeqeQhDhHJ3Kn",
  "mint": "7atgF8KQo4wJrD5ATGX7t1V2zVvykPJbFfNeVf1icFv1",
  "data": {
    "name": "catwifhat",
    "symbol": "$CWIF",
    "uri":
"https://bafkreib5jykd5ehlvmi7f253jdjzzknj6eqlnqhzenfmdc6okrwksqfu6a.ipfs
.nftstorage.link",
    "sellerFeeBasisPoints": 400
  },
  "primarySaleHappened": 0,
  "isMutable": 0,
  "editionNonce": 254,
  "tokenStandard": 2
}
```

Extensions

Additionally to Metaplex Metadata, the token has extensions. Specifically, the asset imposes `400` basis points for transfer fee calculation (`transferFeeBasisPoints` : 400), which means that the transfer fee is 4%. Furthermore, the `maximumFee` is set to `9999999999999900` , which is the maximum fee per transfer. The `transferFeeConfigAuthority` has been renounced and as a result, the fees configuration cannot change.

```
[
  {
    "extension": "transferFeeConfig",
    "state": {
      "newerTransferFee": {
        "epoch": 551,
        "maximumFee": 9999999999999900,
        "transferFeeBasisPoints": 400
      },
      "olderTransferFee": {
        "epoch": 551,
        "maximumFee": 9999999999999900,
        "transferFeeBasisPoints": 400
      },
      "transferFeeConfigAuthority": null,
      "withdrawWithheldAuthority": null,
      "withheldAmount": 46131793921809890
    }
  }
]
```

Findings Breakdown

● Critical	0
● Medium	0
● Minor / Informative	1

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

STPMTA - Mint Authority

Criticality	Passed
Status	Resolved

Description

The token has a fixed supply of tokens, as the mint authority has been revoked, ensuring a stable and unchangeable total supply. This key characteristic enhances its value proposition within the ecosystem by eliminating the possibility of future inflation of the token value through additional minting. This creates a predictable environment for investors and users, contributing to a perception of increased trustworthiness and security. This decision aligns with the best practices aiming to preserve the token's integrity and value, fostering a more sustainable and confident market presence.

STPFRA - Freeze Authority

Criticality	Passed
Status	Resolved

Description

The freeze authority of the token has been revoked, permanently disabling the ability to freeze and thaw accounts. This action signals a definitive stance on account management within the token's ecosystem, emphasizing the permanence of account statuses. Removing the possibility of altering account states, establishes a more secure environment for token holders, reinforcing the network's commitment to stability and reliability. This decision reflects adherence to best security practices, aiming to solidify investor confidence and enhance the token's value by ensuring consistent operational integrity.

RWWA - Renounced Withdraw Withheld Authority

Criticality	Minor / Informative
Status	Acknowledged

Description

The `TransferFeeConfig` extension is designed to facilitate the collection of fees, where every token transfer incurs a fee. The `transferFeeConfigAuthority` has been renounced, meaning that the configuration of fees cannot change. However, the `withdrawWithheldAuthority` has been renounced. The renouncement of the `withdrawWithheldAuthority` effectively nullifies the ability to withdraw any accumulated transfer fees. The lack of an authority to manage fee withdrawals could imply that, the fees accumulated would remain perpetually locked within the system. This configuration could inadvertently undermine the intended utility of the transfer fees.

```
[
  {
    "extension": "transferFeeConfig",
    "state": {
      "newerTransferFee": {
        "epoch": 551,
        "maximumFee": 9999999999999900,
        "transferFeeBasisPoints": 400
      },
      "olderTransferFee": {
        "epoch": 551,
        "maximumFee": 9999999999999900,
        "transferFeeBasisPoints": 400
      },
      "transferFeeConfigAuthority": null,
      "withdrawWithheldAuthority": null,
      "withheldAmount": 46131793921809890
    }
  }
]
```

Recommendation

It is recommended to reassess the token's economic models to ensure they align with the intended utility and long-term viability of the token, that revolves around the renouncement of the `withdrawWithheldAuthority` .

Team Update

The team has acknowledged that this is not a security issue but an intended functionality and states:

The purpose of the transfer fees in the $CWIF token system is to act as a deflationary burn mechanism. Specifically, a 4% fee is deducted from every transaction involving $CWIF tokens. This fee is automatically subtracted and withheld in the recipient's token account, effectively removing it from circulation permanently. This mechanism is designed to gradually reduce the total supply of $CWIF tokens, potentially increasing their value over time. https://docs.cwifwiki.com/token-extensions/transfer-fee-extension

Summary

The Catwifhat token, built on the Solana network, leverages a solid architecture initiated via the Token 2022 program. This audit rigorously evaluates its performance, security, and compliance with best practices. The investigation aims to identify and address any operational vulnerabilities, performance bottlenecks, and areas for optimization, ensuring the token's robustness and reliability in the Solana ecosystem. The token program analysis reported no compiler errors or critical issues.

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