Cyberscope

Audit Report

Onyx Arches

June 2024

Network	SOL
Address	CubzXgS7oXWwyDsGovSpR4KhswQz5nQi3NV1FbTAz2RK
Audited by	© cyberscope

Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	STPMTA	Mint Authority	Unresolved
●	STPFRA	Freeze Authority	Unresolved
●	STPUPA	Update Authority	Unresolved

Table of Contents

Review

Network	Solana
Address	CubzXgS7oXWwyDsGovSpR4KhswQz5nQi3NV1FbTAz2RK
Explorer	https://solscan.io/address/CubzXgS7oXWwyDsGovSpR4KhswQz5nQi3NV1FbTAz2RK
Name	Onyx Arches
Symbol	OXA
Decimals	9
Total Supply	1,000,000,000
Metadata File Type	JSON
Owner Program	https://solscan.io/address/TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
Badge Eligibility	Must Fix Criticals

Audit Updates

Initial Audit	19 Jun 2024

Overview

The Onyx Arches token symbolized as OXA, is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain, with a supply of 1,000,000,000 tokens. The token uses the URL https://bafkreig7bf3n3yomwhnmotwel6imdq3i7fm7dzcnakhc4g3mb3hgpecjpi.ipfs.nftstorage.link/, which points to a decentralized storage service for the uri. However, this link points to an image and not the metadata of the token. 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	78E7iNoy9LW8j4yP889w7ptHiF7p2penMejScPfGKGP3	The public key that is allowed to update this account
mint	CubzXgS7oXWwyDsGovSpR4KhswQz5nQi3NV1FbTAz2RK	The public key of the Mint Account it derives from
name	Onyx Arches	The on-chain name of the token
symbol	OXA	The on-chain symbol of the token
uri	https://bafkreig7bf3n3yomwhnmotwel6imdq3i7fm7dzcnakhc4g3mb3hgpecjpi.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

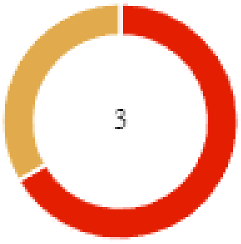
primarySaleHappened	false	A boolean indicating if the token has already been sold at least once. Once flipped to True, it cannot ever be False again. This field can affect the way royalties are distributed
isMutable	true	A boolean indicating if the metadata account can be updated. Once flipped to False, it cannot ever be True again
editionNonce	251	Unique identifier for this edition
tokenStandard	2	The standard of the token

Metadata

The Metaplex Metadata provides details of the characteristics of the `Onyx Arches 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.

The asset imposes `sellerFeeBasisPoints` of 0 basis points, indicating no 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 mutable since `isMutable` is true, allowing future changes to the metadata. The `editionNonce` of 251 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.

Findings Breakdown



●	Critical	2
●	Medium	1
●	Minor / Informative	0

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

STPMTA - Mint Authority

Criticality	Critical
Status	Unresolved

Description

The token is currently configured in a manner that grants the account `78E7iNoy9LW8j4yP889w7ptHiF7p2penMejScPfGKGP3` the exclusive capability to mint new tokens at will. This unrestricted minting authority poses a significant risk of token inflation for the token. If the minting capability is exercised without stringent controls or limitations, it could lead to a scenario where the supply of tokens is significantly increased in a short period. Such an action would dilute the value of existing tokens, potentially leading to a loss of trust among investors and users, and ultimately, a decrease in the token's market value. This highlights a critical vulnerability in the token's economic model, where the potential for unchecked token creation could result in a highly inflated token supply, undermining the asset's stability and value proposition.

Recommendation

It is recommended to revoke the mint authority to mitigate the risk of unchecked token inflation. Implementing a fixed supply model could significantly enhance the token's economic security and investor confidence. By removing or significantly restricting the ability to mint new tokens, the token can maintain a stable supply, preserving its value and ensuring a fair and predictable market for all stakeholders.

STPFRA - Freeze Authority

Criticality	Critical
Status	Unresolved

Description

The token configuration currently empowers the account `78E7iNoy9LW8j4yP889w7ptHiF7p2penMejScPfGKGP3` with the freeze authority, allowing it to unilaterally freeze and thaw token accounts. This authority grants significant control over the token's liquidity and could potentially be misused to manipulate market conditions or target specific token holders unfavorably. The ability to freeze accounts without checks poses a risk to the token's operational integrity and could erode trust among its community. Furthermore, if the freeze authority is revoked without careful consideration, accounts frozen at that time would remain in a perpetual state of immobilization, disrupting the intended fluidity of the token's ecosystem. This condition introduces a rigid constraint on the token's market dynamics and could impact its overall utility and value negatively.

Recommendation

It is recommended to revoke the freeze authority to mitigate the risk of arbitrary account access control. By disabling the ability to freeze and thaw accounts, the token ensures a consistent and uninterrupted user experience, enhancing trust among its holders. Establishing a permanent and immutable operational model would solidify the token's reputation for reliability and fairness, preserving its market value and supporting a stable ecosystem for all participants.

STPUPA - Update Authority

Criticality	Medium
Status	Unresolved

Description

The contract is set up in a way that grants the update authority, with the address `78E7iNoy9LW8j4yP889w7ptHiF7p2penMejScPfGKGP3` , 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

Summary

The Onyx Arches token, built on the Solana network, leverages a solid architecture initiated via the Token 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 that the mint, freeze, and update authorities of the token have not yet been revoked. This situation leaves the token's operations regarding minting, freezing, and updating actions, open to modifications. Consequently, these critical operations remain exposed to potential adjustments by the owner.

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