



Cyberscope

Audit Report

BabyMona

April 2024

Network SOL

Type SPL-Token

Address BGJGRESuGgZNy6z3e2wiK2E5hdVfkWhCTQCoJuaJonFA

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

Analysis	1
Diagnostics	2
Table of Contents	3
Review	4
Audit Updates	4
Source Files	4
Overview	5
Metadata	6
Findings Breakdown	10
UA - Update Authority	11
Description	11
Recommendation	11
ITA - Initial Token Allocation	12
Description	12
Recommendation	12
Summary	13
Disclaimer	14
About Cyberscope	15

Review

Network	SOL
Explorer	https://solscan.io/token/BGJGRESuGgZNy6z3e2wiK2E5hdVfkWhCTQCoJuaJonFA
Fixed Supply	1,000,000,000.00
Token Address	BGJGRESuGgZNy6z3e2wiK2E5hdVfkWhCTQCoJuaJonFA
Token name	Baby Mona (BYMONA)
Owner Program	Token Program
Decimals	6
MintTokens Authority	Revoked
FreezeAccount Authority	Revoked
Metadata File Type	JSON
Badge Eligibility	Yes

Audit Updates

Initial Audit	03 Apr 2024
---------------	-------------

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/BGJGRESuGgZNy6z3e2wiK2E5hdVfkWhCTQCoJuaJonFA#metadata

Overview

The **Baby Mona** token symbolized as **BYMONA**, is a distinguished SPL (Solana Program Library) token initialized using the **TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA** Token Program on the Solana blockchain, with 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 URL <https://ipfs.io/ipfs/QmcvDdbYWdt4TyHbef2PJGL5GdnECTLruWXXVDb54dU7EKk>, which points to a decentralized storage service while the <https://ipfs.io/ipfs/QmZLhfdawbV6B6umm55Wpzc8CnakjEYaTqSDhnJAQyEmZ9> 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.

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

<https://solscan.io/tx/5Nu9jFN3jXZUbhni5CziZgTLywjU2g7ECyspiPy5K8As6iGeD2Z9XFiwprWzPYRkNB4cCGNxyvmpwEaSocoLv8AD>

Metadata

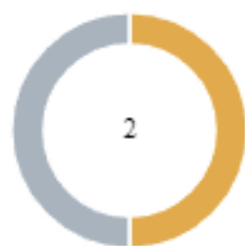
The Metaplex Metadata provides details of the characteristics of the **Baby Mona** token, a distinctive digital asset on the Solana blockchain tailored for utilizing the Metaplex Metadata. This metadata includes crucial information necessary for the asset's seamless integration and operation within the Solana ecosystem. Specifically, the update authority attribute specifies the account **8nsHARAGuPavaHWveGzJ9pqRZ73MgptkRH3UXkkbKwuV** authorized to modify the metadata. The mint attribute specifies the account **BGJGRESuGgZNy6z3e2wiK2E5hdVfkWhCTQCoJuaJonFA** 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 **Baby Mona** key features and its operational framework within the Metaplex ecosystem on Solana.

```
{
  "key": 4,
  "updateAuthority": "8nsHARAGuPavaHWveGzJ9pqRZ73MgptkRH3UXkkbKwuV",
  "mint": "BGJGRESuGgZNy6z3e2wiK2E5hdVfkWhCTQCoJuaJonFA",
  "data": {
    "name": "Baby Mona ",
    "symbol": "BYMONA",
    "uri":
      "https://ipfs.io/ipfs/QmcvDdbYWdt4TyHbef2PJGL5GdnECTLruWXXVDb54dU7EK",
    "sellerFeeBasisPoints": 0
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 254,
  "tokenStandard": 2,
  "name": "Baby Mona ",
  "symbol": "BYMONA",
  "description": "Baby Mona is the Memefied Version of MonaCoin (aka
  Japanese Dogecoin). It was Derived From The Most Promising ASCII art
  character \"Mona\". $BYMONA is The Most Memeable Memecoin in Existence.
  #BYMONAARMY Rocks !!!!!",
  "image":
    "https://ipfs.io/ipfs/QmZLhfdawbV6B6umm55Wpzc8CnakjEYaTqSDhnJAQyEmZ9",
  "extensions": {
    "website": "https://babymona.vip/",
    "twitter": "https://twitter.com/BabyMonaCoin",
    "telegram": "https://t.me/BabyMonaCoin",
    "discord": ""
  },
  "creator": {
    "name": "DepLoySolXYZ Development Tools",
    "site": "https://www.deploysol.xyz/"
  }
}
```


Field	Value	Description
key	4	Account discriminator that identifies the type of metadata account
updateAuthority	8nsHARAGuPavaHWveGzJ9pq RZ73MgptkRH3UXkkbKwuV	The public key that is allowed to update this account
mint	BGJGRESuGgZNY6z3e2wiK2E 5hdVfkWhCTQCoJuaJonFA	The public key of the Mint Account it derives from
name	Baby Mona	The on-chain name of the token
symbol	BYMONA	The on-chain symbol of the token
uri	https://ipfs.io/ipfs/QmcvDdbYWdt4TyHbef2PJGL5GdnECTLruWXXVDb54dU7EK	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
description	Baby Mona is the Memefied Version of MonaCoin (aka Japanese DogeCoin). It was Derived From The Most Promising ASCII art character "Mona". \$BYMONA is The Most Memeable Memecoin in Existence. #BYMONAARMY Rocks !!!!!	The description of the asset
image	https://ipfs.io/ipfs/QmZLhfdawbV6B6umm55Wpzc8CnakiEYaTqSDhnJAQyEmZ9	URL pointing to the asset's logo
extensions	website, twitter, telegram, discord	Extensions of the asset
creator	name, site	Creator of the asset

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 `8nsHARAGuPavaHWveGzJ9pqRZ73MgptkRH3UXkbbKwuV`, 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-immutable-solana-programs#remove-the-update-authority-of-a-solana-program>

ITA - Initial Token Allocation

Criticality	Minor / Informative
Status	Unresolved

Description

The token account `vzHdWgQbPeng1VU8GyXA5hiwrJj9MtajfRvZG58DHLA`, holds a large portion of total supply. Consequently, at the time of the report, this address owns 70.0000% of the entire token supply, amounting to 700,000,001 `BYMONA`. This concentration of almost 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
<code>vzHdWgQbPeng1VU8GyXA5hiwrJj9MtajfRvZG58DHLA</code>	700,000,001	70.0000%

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 "BabyMona" 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 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>