Cyberscope

Audit Report

BlahBlahCoin

March 2024

Network	SOL
Type	SPL-Token
Address	2T9q21zS1vkgwbbwgcWaNna9gd7TPboXU96msNaBjbsZ
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

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/2T9q21zS1vkgwbbwgcWaNna9gd7TPboXU96msNaBjbsZ
Fixed Supply	10,000,000,000
Token name	BlahBlahCoin (BLAHBLAH)
Token address	2T9q21zS1vkgwbbwgcWaNna9gd7TPboXU96msNaBjbsZ
Owner Program	Token Program
Decimals	9
Signature	2zaVjhGWc9DL3j5hPKXzKG8q6ZAnyMmsmo8Re9qTSSZLciwfNRb76EjwRuqyFFHdUfi3pY6w6sXnpU9xW9TxqzL8
Block	# 254876253
Deploy Time	March 18, 2024 08:27:32 Eastern European Standard Time
Instructions	Compute-Budget-Set-Compute-Unit-Price,Compute-Budget-Set-Compute-Unit-Limit,Create,Mint
By	EZ4giR4cPhHzMZ9fyaaA6vsAynHiWb7ADBc4aXDMJ3J3
MintTokens Authority	Revoked
FreezeAccount Authority	Revoked
Metadata File Type	JSON
Name	BlahBlahCoin
Symbol	BLAHBLAH

Image	https://cloudflare-ipfs.com/ipfs/QmQr7KsccwVRMpmYYfg8ZBeFsCNSToHhraiRuzWeGAg4kB
Total Transfers (At the time of the report)	7
Total Transactions (At the time of the report)	10
Total Holders (At the time of the report)	7

Audit Updates

Initial Audit	24 Mar 2024

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/2T9q21zS1vkgwbbwgcWaNna9gd7TPboXU96msNaBjbsZ#metadata

Overview

The `BlahBlahCoin` token symbolized as `BLAHBLAH` , is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain. The `BlahBlahCoin` token has a fixed supply of `10,000,000,000` 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://cloudflare-ipfs.com/ipfs/QmRKR2VDeX1zhZ42p6vjikDXLuDGZpcoFiTvdiBk4foUF8" , which points to a decentralized storage service while the "https://cloudflare-ipfs.com/ipfs/QmQr7KsccwVRMpmYYfg8ZBeFsCNSToHhraiRuzWeGAg4kB" image is used for visual identification of the token across various platforms and marketplaces. Overall, the `BlahBlahCoin` token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Transfers

At the time of this report, the Transfers of the BlahBlahCoin token are as follows:

Signature	Time (UTC)	Type	From	To	Amount
22VgoZcC2izfqe bQYgzDePm4yzs 7osS6PWDvQM9 cuUgjwWQtGhSV W67v51dz85vwA wXWRaCPeiLSh NK2v58TVqws	03-23-2024 18:00:04	Spl-Transfer	EZ4giR... DMJ3J3	5ypcmX... Gaoh3b	1,500,000,000
3tkaCnBV5Kc55 gfjQK7PbHNnFZ bETkkzz1EWvKB MW167xuCDip2 uEKcaS2ea5dY4 LXDc4zsopipRrc qMeGewwX3g	03-23-2024 13:48:47	Spl-Transfer	BaMUpq.. .KpmEAW	3tod4e...B etWjM	2,000,000,000
5VVZ54R8YBkH DkgrBypxi2c5fQ Si6LEaPiWcvpzp xEu4Bze8wnPNT qSuZNihPAQwTe 4ArPvsktsWDac EggRZTPRs	03-23-2024 12:50:38	Spl-Transfer	EZ4giR... DMJ3J3	8uzTmw... wkRegS	500,000,000
uwFRrEZwPRVuy Qk6LSLqCHcgAR tT27vxEBpFDzLA	03-23-2024 12:49:30	Spl-Transfer	EZ4giR... DMJ3J3	8rcqxx...e9 fBgA	1,000,000,000

M6n4F7Zu9yT5K TWSAmJJvSJAa ioKckzoXLQCWA C4nk3FLGD					
4BdjD1Lxp8LYAR izYxH9tdcbEVWx wzVmnAVZhgRy T3UzLim6JPgT6 6mjiKMEmiUyvt HHpien7sYbyo6F tK81LP3k	03-23-2024 12:48:17	Spl-Transfer	EZ4giR... DMJ3J3	BPaFkB... AEZqcH	1,000,000,000
vvh9oKdnZ9BY6 1fXCFFMm9FgX yehPWoy2AJL3s Dvq2dSwD3BGY 8khDDRGe7Yr1Q 4XYL1Kzxndeow 6jXHuRyEtUu	03-23-2024 12:46:48	Spl-Transfer	EZ4giR... DMJ3J3	B9qack...g 7pzCU	2,000,000,000
41CDPueGfnUx7 H2aR76V3aMm5 k49gBfhrMbiDCS 5brSxg6x3xAEJ mpES8nJVA8cC FTZ8z9EFvcmpr FLXnuQg69X4	03-23-2024 12:45:18	Spl-Transfer	EZ4giR... DMJ3J3	BaMUpq... KpmEAW	2,000,000,000

Transactions

At the time of this report, the last 5 transactions of the BlahBlahCoin token are as follows:

Signature	Block	Time	Instructions	By	Fee (SOL)
22VgoZcC2izfqebQYgzDePm4yzs7osS6PWDvQM9cuUgjwWQtGhSVW67v51dz85vwAwXWRaCPeiLShNK2v58TVqws	#255994952	03-23-2024 18:00:04	Compute-Budget-Set-Compute-Unit-Price (4+)	EZ4giR...DMJ3J3	0.000025
3tkaCnBV5Kc55gfjQK7PbHNnFZbETkkzz1EWvKBMW167xuCDip2uEKcaS2ea5dY4LXDc4zsopipRrcqMeGewwX3g	#255960184	03-23-2024 13:48:47	Compute-Budget-Set-Compute-Unit-Price (2+)	BaMUpq...KpmEAW	0.00003
5VVZ54R8YBkHDkgrBypxi2c5fQSi6LEaPiWcvpzpxEu4Bze8wnPNTqSuZNihPAQwTe4ArPvsktsWDacEggRZTPRs	#255952346	03-23-2024 12:50:38	Compute-Budget-Set-Compute-Unit-Price (4+)	EZ4giR...DMJ3J3	0.000025
uwFRrEZwPRVuyQk6LSLqCHcgARtT27vxEBpFDzLAM6n4F7Zu9yT5KTWSAmJJvSJAaioKckzoXLQCWAC4nk3FLGD	#255952195	03-23-2024 12:49:30	Compute-Budget-Set-Compute-Unit-Price (4+)	EZ4giR...DMJ3J3	0.000025
4BdjD1Lxp8LYARizYxH9tdcbEVWxwzVmnAVZhgRyT3UzLim6JPgT66mjiKMEmiUyvtHHpien7sYbyo6FtK81LP3k	#255952024	03-23-2024 12:48:17	Compute-Budget-Set-Compute-Unit-Price (4+)	EZ4giR...DMJ3J3	0.000025

Holders

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

#	Token Account	Account	Quantity	Percentage
1	9bchZW...Chp3Hv	EZ4giR...DMJ3J3	2,000,000,000	20.0000%
2	CYYkFA...cmQ2ss	B9qack...g7pzCU	2,000,000,000	20.0000%
3	A1k7ST...DRhfyw	3tod4e...BetWjM	2,000,000,000	20.0000%
4	9kRRFL...WL2mFs	5ypcmX...Gaoh3b	1,500,000,000	15.0000%
5	2DBxFD...Cxbp8e	BPaFkB...AEZqcH	1,000,000,000	10.0000%
6	FUNnST...NNEGaK	8rcqxx...e9fBgA	1,000,000,000	10.0000%
7	5ZEPjQ...xjJ8a8	8uzTmw...wkRegS	500,000,000	5.0000%

Metadata

MetaplexMetadata

The Metaplex Metadata provides details of the characteristics of the `BlahBlahCoin`
token which uses the `BLAHBLAH` 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
`EZ4giR4cPhHzMZ9fyaaA6vsAynHiWb7ADBc4aXDMJ3J3.` Furthermore, the mint
attribute specifies the account
`2T9q21zS1vkgwbbwgcWaNna9gd7TPboXU96msNaBjbsZ` authorized for the initial
token mint.

```
{
  "key": 4,
  "updateAuthority": "EZ4giR4cPhHzMZ9fyaaA6vsAynHiWb7ADBc4aXDMJ3J3",
  "mint": "2T9q21zS1vkgwbbwgcWaNna9gd7TPboXU96msNaBjbsZ",
  "data": {
    "name": "BlahBlahCoin",
    "symbol": "BLAHBLAH",
    "uri":
"https://cloudflare-ipfs.com/ipfs/QmRKR2VDeX1zhZ42p6vjikDXLuDGZpcoFiTvd
iBk4foUF8",
    "sellerFeeBasisPoints": 0,
    "creators": [
      {
        "address": "EZ4giR4cPhHzMZ9fyaaA6vsAynHiWb7ADBc4aXDMJ3J3",
        "verified": 1,
        "share": 100
      }
    ]
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 254,
  "tokenStandard": 2,
  "name": "BlahBlahCoin",
  "symbol": "BLAHBLAH",
  "description": "Blah Blah Coin has been created for public. Telegram
: https://t.me/BlahBlahCoin, X : https://twitter.com/BlahBlahCoin,
Website: https://blahblahcoin.org",
  "image":
"https://cloudflare-ipfs.com/ipfs/QmQr7KsccwVRMpmYYfg8ZBeFsCNSToHhraiRu
zWeGAg4kB",
  "creator": "TrustSwap - Team Finance",
  "site": "https://solana.team.finance"
}
```

Metadata description

The data section within the metadata discloses the asset's name as `BlahBlahCoin` , its trading symbol as `BLAHBLAH`, and an image URI pointing to "https://cloudflare-ipfs.com/ipfs/QmQr7KsccwVRMpmYYfg8ZBeFsCNSToHhraiRuzWeGAg 4kB". 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 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 `BlahBlahCoin` 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	EZ4giR4cPhHzMZ9fyaaA6vsAy nHiWb7ADBc4aXDMJ3J3	The public key that is allowed to update this account
mint	2T9q21zS1vkgwbbwgcWaNna 9gd7TPboXU96msNaBjbsZ	The public key of the Mint Account it derives from
Name	BlahBlahCoin	The on-chain name of the token
Symbol	BLAHBLAH	The on-chain symbol of the token
Uri	https://cloudflare-ipfs.com/ipfs /QmRKR2VDeX1zhZ42p6vjikD XLuDGZpcoFiTvdiBk4foUF8	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	Blah Blah Coin has been created for public. Telegram : https://t.me/BlahBlahCoin, X : https://twitter.com/BlahBlahCoin, Website: https://blahblahcoin.org	Description of the asset
image	https://cloudflare-ipfs.com/ipfs/QmQr7KsccwVRMpmYYfg8ZBeFsCNSToHhraiRuzWeGAg4kB	URI pointing to the asset's logo
creator	TrustSwap - Team Finance	The creator of the asset
site	https://solana.team.finance	The site of the asset

Findings Breakdown
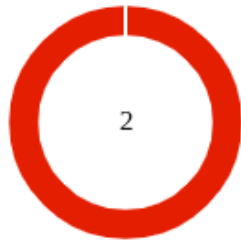
	Critical	2
	Medium	0
	Minor / Informative	0

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

ELFM - Exceeds Fees Limit

Criticality	Critical
Location	BlahBlahCoin
Status	Unresolved

Description

The current metadata configuration of the token has the `isMutable` field set to `1`, which allows for future changes to the metadata. This enables the update authority to modify the `setTaxFeePercent` field, thereby adjusting the fee structure as desired. Consequently, the update authority may take advantage of it by setting the `setTaxFeePercent` variable to a high percentage value.

Recommendation

It is recommended to revoke the update authority's privileges. This action will prevent any future modifications to the metadata, including updates on fees, thereby ensuring that the `setTaxFeePercent` variable cannot be set to a disproportionately high value. Revoking these privileges effectively disables the ability to change the fees. One method to accomplish this is by adhering to the instructions provided in the guide available at Remove the Update Authority of a Solana Program

UA - Update Authority

Criticality	Critical
Location	BlahBlahCoin
Status	Unresolved

Description

The contract is set up in a way that grants the update authority, with the address `EZ4giR4cPhHzMZ9fyaaA6vsAynHiWb7ADBc4aXDMJ3J3`, 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.

Summary

The BlahBlahCoin 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/5Fgs39eEdQe46mxBb3zkJTXLLpsmrt2pcbnRmNduNFNXNacQf6yMRgzYSyaoMtLxHAm9nYePgVtexyGNC7hkJH7Q.

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

https://solscan.io/tx/R4yDEXqXFedrvMYx8dCRJa45iTdsXoBRteFzhcLUbbDvrLSMHtV4gEkJYwHUtMKWMNte7nLxtCSgm7G1Grb6FyS

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