Cyberscope

Audit Report

Gatsby

March 2024

Network	SOL
Type	SPL-Token
Address	28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkyqX
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	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Unresolved

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	UA	Update Authority	Unresolved

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkyqX
Current Supply	8,888,888,888,888
Token name	Gatsby (GATSBY)
Token address	28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkyqX
Owner Program	Token Program
Authority	FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM
Decimals	6
Signature	https://solscan.io/tx/44P88vV7uA9miEeZYrf1gkduYFqvCdDyERjvB2M4Jf9PuWobpZD86PEZZEQ8bGVyjUWcVyGffZnmKekk8gYh32eG
Block	#255133125
Deploy Time	March 19, 2024 14:19:42 Eastern European Standard Time
Instructions	Compute-Budget-Set-Compute-Unit-Limit, Compute-Budget-Set-Compute-Unit-Limit, CreateAccount, InitializeMint, Unknown, Create, MintTo
By	FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM
MintTokens Authority	FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM
FreezeAccount Authority	FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM
Metadata File Type	JSON

Name	Gatsby
Symbol	GATSBY
Image	https://bafkreiaendowxbqr4x4i3cmka7b5mmqtvtaplhwnzoeh33xoulo6ikkafi.ipfs.nftstorage.link
Total Transfers (At the time of the report)	3
Total Transactions (At the time of the report)	4
Total Holders (At the time of the report)	4

Audit Updates

Initial Audit	16 Mar 2024 https://github.com/cyberscope-io/audits/blob/main/gatsbytoken/v1/audit.pdf
Corrected Phase 2	19 Mar 2023

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkyqX#metadata

Overview

The `Gatsby` token, represented by the symbol `GATSBY`, is a notable SPL (Solana Program Library) token created under the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain. The minting and freezing authorities for the Gatsby token have not been renounced and are held by the same entity, identified as `FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM`. This allows for potential adjustments to the token's supply and state, offering a level of control over its distribution and security.

The Gatsby token boasts a unique identifier mint of `28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkyqX` and has updated its visual representation with the image URL: https://bafkreidx6eluhgkjiuynlm62zzjcsw3ydtxzn2bv7cuckvj2c5vrk3rlpm.ipfs.nftstorage.link. This image serves as the token's visual identity across various platforms and marketplaces, enhancing its recognition within the ecosystem. Overall, the `Gatsby` 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 "Gatsby" token are as follows:

Signature	Time	Type	From	To	Amount
3yuK64FXjH9N3M9eunyh	03-19-2024 13:55:05	Spl-Transfer	FoazeP...JYiWaM	3tod4e...BetWjM	479,999,999,999.95
5xgArQM9Hn2xsdPguZw	03-19-2024 13:48:16	Spl-Transfer	FoazeP...JYiWaM	3tod4e...BetWjM	799,999,999,999.92
67n6BtvGwrpopRUaQJwk	03-19-2024 13:36:26	Spl-Transfer	FoazeP...JYiWaM	3tod4e...BetWjM	1,066,666,666,666.56

Transactions

At the time of this report, the transactions of "Gatsby" token are as follows:

Signature	Block	Time (UTC)	Instructions	By	Fee (SOL)
3yuK64FXjH9N3M9eunyh9gXqpSNNq5	#255146840	03-19-2024 13:55:05	Compute-Budget-Set-Compute-Unit-Price (2+)	FoazeP...JYiWaM	0.00003
5xgArQM9Hn2xsdPguZwaf4KeevWETZ	#255145846	03-19-2024 13:48:16	Compute-Budget-Set-Compute-Unit-Price (2+)	FoazeP...JYiWaM	0.00003
67n6BtvGwrpopRUaQJwk5ZKjrDuybVRP	#255144156	03-19-2024 13:36:26	Compute-Budget-Set-Compute-Unit-Price (2+)	FoazeP...JYiWaM	0.00003
44P88vV7uA9miEeZYrf1gkduYFqvCdD...	#255133125	03-19-2024 12:19:42	Compute-Budget-Set-Compute-Unit-Limit, Compute-Budget-Set-Compute-Unit-LimitCreateAccount, InitializeMint, Unknown, Create, MintTo	FoazeP...JYiWaM	0.00011

Holders

At the time of this report, the holders of "Gatsby" token are as follows:

#	Token Account	Quantity	Percentage
1	HuPwBi...sfFeJJ	6,542,222,222,221.568	73.6000%
2	3GZAZE...h76soE	1,066,666,666,666.56	12.0000%
3	EsnjCS...f8ayfY	799,999,999,999.92	9.0000%
4	HyvRvX...UHcNWE	479,999,999,999.952	5.3999%

Metadata

MetaplexMetadata

The Metaplex Metadata for the `Gatsby` token, symbolized as `GATSBY`, enriches the Solana blockchain with a unique digital asset, meticulously designed for integration with the Metaplex protocol. This metadata is pivotal for the asset's functionality within the ecosystem, detailing essential attributes that facilitate its recognition and utility. The `updateAuthority` for Gatsby is vested in the account with the public key `FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM`, empowering it with the authority to change the metadata as necessary. The mint attribute specifies the account `2pzuQMLnssLFweUXDqZ1pXW3qXCTo1bgWF3mFzzE8dC2` authorized for the initial token mint.


```
{
  "key": 4,
  "updateAuthority": "FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM",
  "mint": "28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkyqX",
  "data": {
    "name": "Gatsby",
    "symbol": "GATSBY",
    "uri":
"https://bafkreidx6eluhgkjiuynlm62zzjcsw3ydtxzn2bv7cuckvj2c5vrk3rlpm.ipfs
.nftstorage.link",
    "sellerFeeBasisPoints": 0
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 255,
  "tokenStandard": 2,
  "name": "Gatsby",
  "symbol": "GATSBY",
  "description": "WEB: gatsbytoken.io, TG: t.me/GATSBYcommunity, X:
x.com/GatsbyToken",
  "image":
"https://bafkreiaendowxbgr4x4i3cmka7b5mmqtvtaplhwnzoeh33xoulo6ikkafi.ipfs
.nftstorage.link"
}
```

Metadata description

The `data` section within the metadata discloses the asset's name as "Gatsby" , its trading symbol as "GATSBY", and a URI pointing to "https://bafkreidx6eluhgkjiuynlm62zzjcsw3ydtxzn2bv7cuckvj2c5vrk3rlpm.ipfs.nftstorage.link". 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 `251` 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 "Gatsby's" key features and its operational framework within the Metaplex ecosystem on Solana.

Within the data segment of the Gatsby token's metadata, key characteristics such as the asset's name `Gatsby`, its symbol `GATSBY`, and a URI linking to its visual representation are disclosed. This URI, "https://bafkreidx6eluhgkjiuynlm62zzjcsw3ydtxzn2bv7cuckvj2c5vrk3rlpm.ipfs.nftstorage.link", serves as a gateway to the asset's digital identity, enhancing its visibility and accessibility. The asset enforces a zero seller fee basis points policy, indicating an absence of transaction fees for trades. The metadata further reveals that the primary sale of the asset has not occurred (`primarySaleHappened` : 0), and its mutable status (`isMutable` : 1) allows for future modifications. An `editionNonce` of 255 signifies its unique edition, and adherence to the `tokenStandard` : 2 ensures its compliance and interoperability within the Solana ecosystem. This comprehensive metadata encapsulates the Gatsby token's foundational aspects, providing a clear and detailed overview of its operational parameters and its place within the broader Metaplex and Solana frameworks.

Field	Value	Description
key	4	Account discriminator that identifies the type of metadata account

updateAuthority	FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM	The public key that is allowed to update this account
mint	28WnzzzJPix9oUa4kd9LXhfQa1DPofYPaoMyjwcRkygX	The public key of the Mint Account it derives from
name	Gatsby	The on-chain name of the token
symbol	GATSBY	The on-chain symbol of the token
uri	https://bafkreidx6eluhgkjuynlm62zzjcsw3ydtxzn2bv7cuckvj2c5vrk3rlpm.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	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	WEB: gatsbytoken.io, TG: t.me/GATSBYcommunity, X: x.com/GatsbyToken	The description of the asset
image	https://bafkreiaendowxbqr4x4i3cmka7b5mmqtvtaplhwnzoeh33xoulo6ikkafi.ipfs.nftstorage.link	URL pointing to the asset's logo

Findings Breakdown

Critical	4
Medium	0
Minor / Informative	0

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	4	0	0	0
Medium	0	0	0	0
Minor / Informative	0	0	0	0

ELFM - Exceeds Fees Limit

Criticality	Critical
Location	Gatsby
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 `setTaxFeePercent` 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.

MT - Mints Tokens

Criticality	Critical
Location	Gatsby
Status	Unresolved

Description

The token is currently configured in a manner that grants the account `FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM` the exclusive capability to mint new tokens at will. This unrestricted minting authority poses a significant risk of token inflation for the `GATSBY` token. If the minting capability is exercised without stringent controls or limitations, it could lead to a scenario where the supply of `GATSBY` 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. 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 `GATSBY` token can maintain a stable supply, preserving its value and ensuring a fair and predictable market for all stakeholders.

BC - Blacklists Addresses

Criticality	Critical
Location	Gatsby
Status	Unresolved

Description

The Gatsby token is currently configured in such a way that the freeze account authority, identified by the address `FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM`, possesses the unilateral power to freeze token accounts. This centralized control mechanism introduces a significant security risk, as it allows a single entity to potentially disrupt the token's liquidity and user access without consensus or warning. The existence of such authority without appropriate checks and balances or a decentralized governance structure can lead to scenarios where user funds are unjustly frozen, undermining trust in the token's operational integrity and fairness. This configuration could deter potential investors and users, fearing arbitrary account freezes that could lock them out of their assets.

Recommendation

It is recommended to revoke the `freeze` account authority to mitigate the risk associated with centralized token control. Removing this authority would prevent any single entity from having the capability to freeze accounts, thereby enhancing the token's trustworthiness and appeal to a broader number of holders.

UA - Update Authority

Criticality	Critical
Location	Gatsby
Status	Unresolved

Description

The contract is currently configured in a manner that allows the update authority, identified by the address `FoazePZPhw4VEYkftpxgGz5QcrBkyQUNrSdCu4JYiWaM`, to retain privileges that enable the modification of crucial metadata fields. The failure to revoke the `update` authority 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. 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 Gatsby token, built on the Solana network, implements a robust smart contract structure that was initialized using the Token program, with analysis revealing 4 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