Cyberscope

Audit Report

Crash

March 2024

Network	SOL
Type	Token Program
Address	Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs
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

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs#metadata
Fixed Supply	100,000,000
Website	https://solanacrash.io
Social Channels	https://twitter.com/solanacrashio https://t.me/solanacrashio
Token name	Solana Crash (CRASH)
Token address	Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs
Owner Program	Token Program
Decimals	6
Signature	4iWUvCZEkst1Hfbg1C9FCUGwAg2b6z2iBPTpady73akad3ydFBq6VHdxCKxF8ENjinkeAR4T4xV8y3dz7MRhcuK
Block	257209340
Deploy Time	March 29, 2024 19:23:56 +UTC
By	RUzWwy4Kxf239VobvBh86aD2LbBB7T626MnytFBqyNm
MintTokens Authority	Revoked
Metadata File Type	JSON
Name	Solana Crash
Symbol	CRASH

Image	https://arweave.net/YcUI_hmPhC_L6rxYLAYzQPZjg1FIkGjRh7b QvWwL3C8
Badge Eligible	Yes

Audit Updates

Initial Audit	28 Mar 2024

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/Crashu2xZABC37wX3cs3rMQAe7Rpdy LU8qyhRcDehpDs#metadata

Overview

The `Solana Crash` token symbolized as `CRASH`, is a distinguished SPL (Solana Program Library) token initialized using the `Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs` Token Program on the Solana blockchain. The `CRASH` token has a fixed supply of `100,000,000.00` 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://arweave.net/BaAexFLtmGdQhZ49kKRuMxTmePSjE_07ARdbN-YklFw, which points to a decentralized storage service while the https://arweave.net/YcUI_hmPhC_L6rxYLAYzQPZjg1FlkGjRh7bQvWwL3C8 image is used for visual identification of the token across various platforms and marketplaces. Overall, the `CRASH` token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Metadata

MetaplexMetadata

The Metaplex Metadata provides details of the characteristics of the `CRASH` token which uses the `CRASH` 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 update authority attribute specifies the account `RUzWwy4Kxf239VobvBh86aD2LbBB7T626MnytFBqyNm` authorized to modify the metadata. The mint attribute specifies the account `Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs` authorized for the initial token mint.

```
{
    "key": 4
    "updateAuthority": "RUzWwy4Kxf239VobvBh86aD2LbBB7T626MnytFBqyNm"
    "mint": "Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs"
    "data":{
        "name": "Solana Crash"
        "symbol": "CRASH"
        "uri":
"https://arweave.net/BaAexFLtmGdQhZ49kKRuMxTmePSjE_07ARdbN-YklFw"
        "sellerFeeBasisPoints":0
    }
    "primarySaleHappened":0
    "isMutable":0
    "editionNonce":255
    "tokenStandard":2
    "name": "Solana Crash"
    "image": "https://arweave.net/YcUl_hmPhC_L6rxYLAYzQPZjg1FIkGjRh7bQvWwL3C8"
    "symbol": "CRASH"
    "description": "Provably fair crash game on Solana."
    "extensions":{
        "twitter": "https://twitter.com/solanacrashio"
        "website": "https://solanacrash.io"
        "telegram": "https://t.me/solanacrashio"
    }
    "seller_fee_basis_points":0
}
```

Metadata description

The data section within the metadata discloses the asset's name as `CRASH` , its trading symbol as `CRASH` , and the URI pointing to "https://arweave.net/BaAexFLtmGdQhZ49kKRuMxTmePSjE_07ARdbN-YklFw". The metadata indicates that the asset has not yet undergone its primary sale (`primarySaleHappened` : 0) and is marked as mutable (`isMutable` : 0). An `editionNonce` of 255 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 `CRASH` key features and its operational framework within the Metaplex ecosystem on Solana.

Findings Breakdown
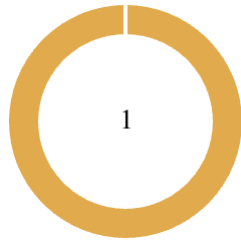
● Critical   0

● Medium   1

● Minor / Informative   0

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

UA - Update Authority

Criticality	Medium
Location	Gatsby
Status	Unresolved

Description

The contract is set up in a way that grants the `update` authority, with the address `Crashu2xZABC37wX3cs3rMQAe7RpdyLU8qyhRcDehpDs`, 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 SOLBULL token, built on the Solana network, implements a robust smart contract structure that was initialized using the Token program, with analysis revealing 1 medium issue.

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

https://solscan.io/tx/3awqZ5h2BDqSxoebRLVD4TQaPExeHVuXe3iBpponxGxEMJVSL2Uh MYRBLBU1Z21hWfTeBKaVWvdRzFHPsLqxEgi3

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