SMART CONTRACT AUDIT REPORT

for

AVA/Wormhole Token (Solana)

Prepared By: Xiaomi Huang

PeckShield

Feburay 12, 2025

Document Properties

Client	AVA/Wormhole Token
Title	Smart Contract Audit Report
Target	AVA/Wormhole Token (Solana)
Version	1.0
Author	Daisy Cao
Auditors	Daisy Cao, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author	Description
1.0	Feburay 12, 2025	Daisy Cao	Final Release

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

PeckShield

1 Introduction

Given the opportunity to review the AVA/Wormhole Token (Solana) contract, which follows the Solana Program Library (SPL) token standard, we outline in the report a systematic approach to evaluate potential security concerns, assess SPL compliance. Unlike ERC20 tokens, SPL tokens typically rely on system instructions provided by Solana rather than custom contracts. With that, our analysis is based on the on-chain configuration and behavior of the given token, and we further examine whether the token settings align with best practices, ensuring secure and reliable functionality within the Solana ecosystem. Our findings indicate that the given token contract conforms to SPL standards without compliance issues or security vulnerabilities. This document outlines our audit results.

1.1 About AVA (Wormhole) token

The AVA (Wormhole) token is an SPL-compliant asset bridged via Wormhole from another blockchain. As there are no custom contracts involved, the security of the audited token contract primarily depends on the integrity of Solana's native token system and the Wormhole protocol for the cross-chain bridge support.

Table 1.1: Basic Information of AVA/Wormhole Token (Solana)

Item	Description
Name	AVA/Wormhole Token
Type	SPL token standard
Platform	Rust
Audit Method	Whitebox
Audit Completion Date	Feburay 12, 2025

In the following, we show the deployment address of the audited AVA/Wormhole token on Solana.

- https://solscan.io/token/G8LfyGVsjsLzetJ5RWZVAhMo4H9cb58ET1Z6gEZJQdPM

1.2 About PeckShield

PeckShield Inc. [2] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystem by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [1]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk;

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

We conduct a manual review to ensure that the token complies with SPL token standards and adheres to best practices.

Table 1.3: The Full List of Check Items

Check Item	Description
Decimals	Verify whether the decimal configuration is appropriate for the token
Token Metadata	Confirm whether the token metadata is complete, including name, symbol, and other relevant information
Token Supply	Check if there is a capped supply or mechanisms controlling token supply to prevent unlimited issuance
Mint Authority	Ensure mint authority is correctly configured, limiting minting permissions to authorized addresses
Freeze Authority	Verify whether freeze authority is enabled to allow freezing token accounts in case of misuse
Upgrade Authority	Ensure that upgrade authority is properly set to allow updates to token metadata

To evaluate the security and compliance of the SPL token, we review key check items and classify findings by severity. If no issues are identified for a specific check item, the token is deemed compliant with SPL standards. For any observed issues, we provide a detailed analysis and potential mitigation strategies. Given that an SPL-based token typically does not involve direct code deployment, our focus is on verifying key aspects of the token's configuration so as to ensure the compliance with best practices. The concrete list of check items is shown in Table 1.3.

1.4 Disclaimer

Note that this security audit is not intended to replace functional testing required before any token deployment and does not guarantee the identification of all potential security risks. The evaluation results do not ensure the absence of further security issues. Since a single audit cannot be considered exhaustive, we strongly recommend conducting multiple independent reviews and implementing a public bug bounty program to enhance security. Lastly, this audit should not be interpreted as financial or investment advice.

2 | Findings

Here is a summary of our findings after analyzing the AVA/Wormhole token on Solana. Our audit primarily focuses on verifying the token's configuration, including supply limits, metadata accuracy, and authority settings.

The token's configuration is correctly set up according to the SPL token standards. The Mint Authority is assigned to Wormhole, allowing it to mint AVA (Wormhole) tokens on Solana when assets are bridged from another chain. This is essential for cross-chain interoperability and is typically managed through a multisig mechanism. The Freeze Authority is not set, meaning token accounts cannot be arbitrarily frozen, ensuring uninterrupted token transfers.

Regarding supply management, the token does not have a fixed cap on Solana. Instead, its supply is dynamically influenced by the AVA supply on the source chain, ensuring proper cross-chain balance.

Overall, the token adheres to standard best practices, with no security concerns found in our audit.

PeckShield

3 Conclusion

In this security audit, we have examined the AVA/Wormhole token configuration and deployment on Solana. Our audit focused on verifying compliance with the SPL token standard, including proper settings for token metadata, supply management, and authority configurations. Our analysis shows that the token's mint authority is controlled by Wormhole for cross-chain minting, while freeze authority is unset, meaning accounts cannot be arbitrarily frozen. The token supply is dynamic, reflecting the supply on the source chain. Overall, we found no security or compliance issues in the token's setup. Meanwhile, as disclaimed in Section 1.4, we appreciate any constructive feedbacks or suggestions about our findings, procedures, audit scope, etc.

PeckShield

References

[1] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[2] PeckShield. PeckShield Inc. https://www.peckshield.com.

PeckShield