

# ERC721A Token Contract Audit Report

Auditor: Anurag Sahu

## Summary

This audit report evaluates the ERC721A token contract, which is an implementation of the ERC721 standard. The ERC721A contract allows for the creation and management of non-fungible tokens (NFTs) and includes minting and token URI retrieval functionality. The audit assesses the contract for security and adherence to best practices.

### Issue type: Low

Version difference as latest version of solidity is less tested

## Audit Findings

### 1. Inheritance and Constructor

- The contract inherits from ERC721A, which aligns with standard practices for ERC721 contracts.
- The constructor sets the token's name and symbol, as expected.
- It is important to verify the legitimacy of the imported ERC721A contract to ensure its trustworthiness.

### 2. mint Function

- The mint function allows the owner to create new NFTs and associate them with the owner's address.
- Access control for the mint function is correctly implemented, allowing only the owner to perform this action.
- The function complies with the ownership pattern, preserving the owner's exclusive minting rights.

### 3. tokenURI Function

- The tokenURI function is used to retrieve the URI of a given NFT.
- Proper access control is maintained to ensure the function can only be called for existing tokens.
- The function returns the URI of a token if it exists and is correctly formatted.

## Conclusion

The ERC721A token contract has undergone a thorough audit, and it demonstrates a secure and functional implementation. The contract includes a constructor for initializing the token name and symbol, and it adheres to the ERC721 standard. Access control is effectively implemented for both minting and token URI retrieval, ensuring that these actions are limited to the contract owner.