< Back to articles

MintDAO: Cross-chain NFTs audit summary

Aleksandra Yudina // AUDITS, ETHEREUM, WAKE MAY 23, 2023

MintDAO is a company that is dedicated to providing advanced cross-chain NFT solutions to the ever-growing NFT market.

MintDAO engaged Ackee Blockchain to perform a security review of contracts that focus on cross-chain manipulation of NFTs. The total time donation was 3 engineering days in a

period between January 30 and February 3, 2023, the audit has been performed on the commit **5ad4033** (Revision 1.0).

The MintDAO team provided an updated codebase that addresses issues from the Revision 1.0. On February 19, 2023, Ackee Blockchain reviewed the fixes which were provided in a private repository with the commit **784ebac**.

METHODOLOGY

We began our review by using static analysis tools, namely Slither and Woke. We then took a deep dive into the logic of the contracts. Additionally, we implemented cross-chain test using Wake testing framework.

During the review, we paid special attention to:

- ensuring that NFTs can't be duplicated by cross-chain transfers, • looking for common issues such as data validation,
- validating the interactions with the Axelar contracts
- validating the correctness of the upgradeability pattern,
- ensuring that the contracts follow the architecture recommended by Axelar,
- detecting possible ERC721 reentrancies in the code,
- testing that cross-chain interactions are working as expected,
- ensuring that the owner role can't be abused or compromised.

SCOPE

We performed a security review of contracts that focus on cross-chain manipulation of NFTs, the audit has been performed on the commit **5ad4033** (Revision 1.0). Later on, Ackee Blockchain reviewed the fixes which were provided in a private repository with the commit **784ebac** (Revision 1.1).

FINDINGS

Here we present our findings.

Critical severity

No critical severity issues were found.

High severity

No high severity issues were found.

Medium severity

M1: Two-phase Owner transfer

M2: Lack of data validation in init functions

M3: Owner Can Cause DoS

M4: Data Validation in sendNFTs()

Low severity

L1: Lack of logging

L2: Constructor Without Initializer

L3: Upgradeable Contract Without Storage Gap

Warning severity

W1: Usage of solc optimizer

W2: Owner role can be renounced

W3: Exposure of sensitive data

W4: Floating pragma

W5: Inconsistency of safeMint And transferFrom

Informational severity

I1: Abstract Contract Named As Interface

CONCLUSION

Our review resulted in **13** findings, ranging from *Info* to *Medium* severity.

We recommended MintDAO to:

- pay more attention to data validation,

- address all other reported issues.

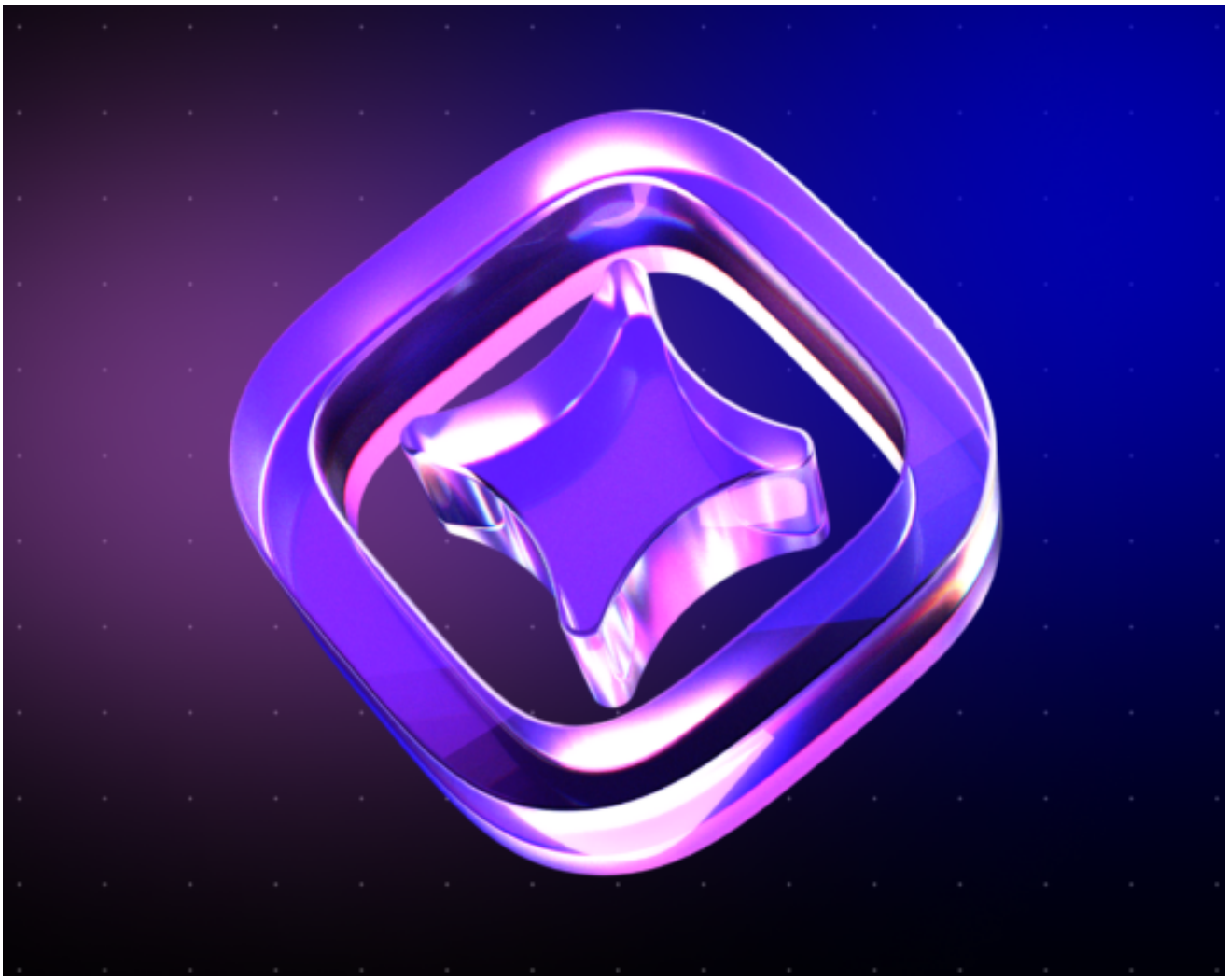
Update: The MintDAO team provided an updated codebase that addresses issues from the Revision 1.0. We consider the fixes to be well-implemented. Some of the issues were not intentionally addressed, and are marked as ‘acknowledged’.

We were delighted to audit **MintDAO** and look forward to working with them again.

Audit Audit Summary MintDAO Wake

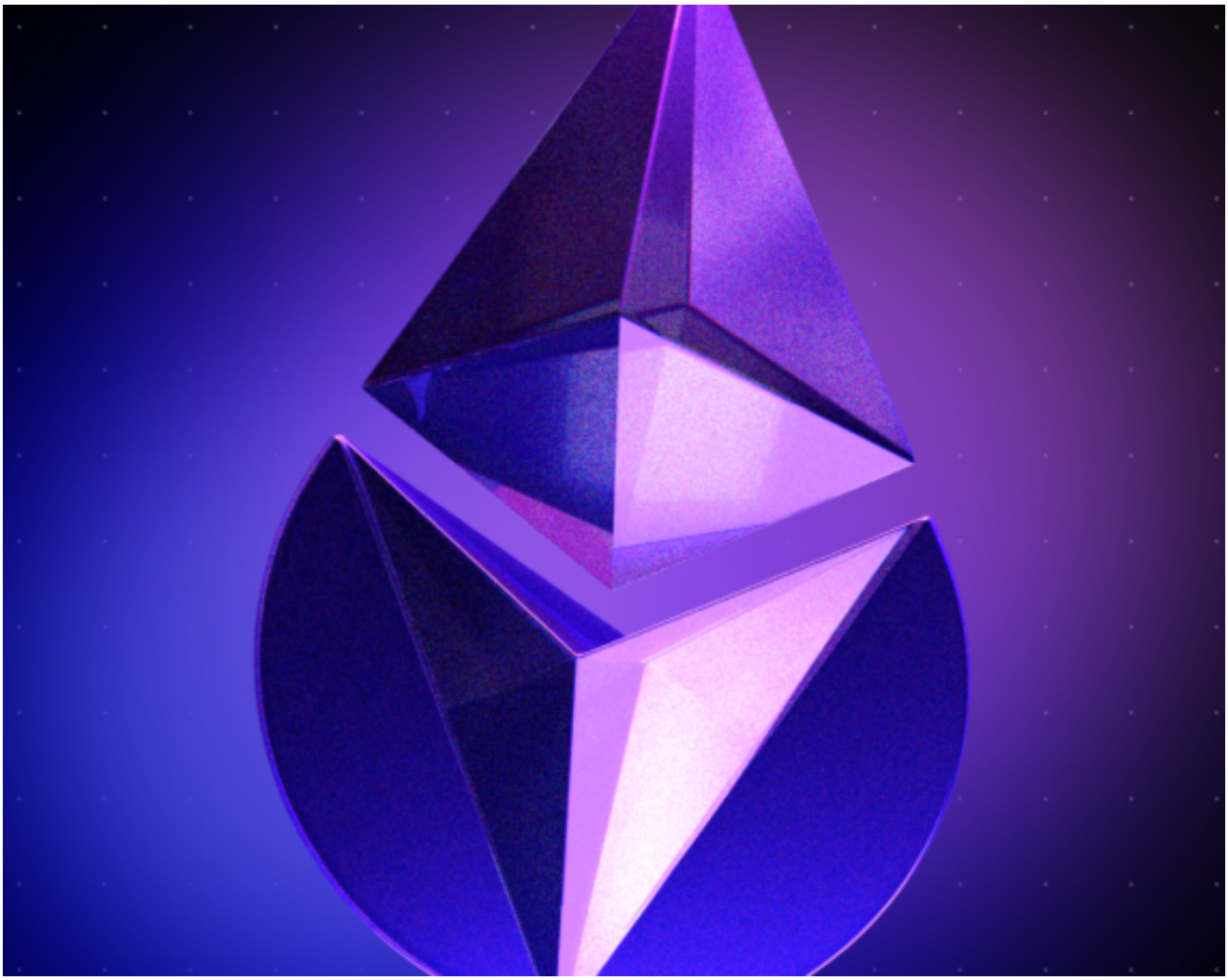
Aleksandra Yudina

You May Also Like



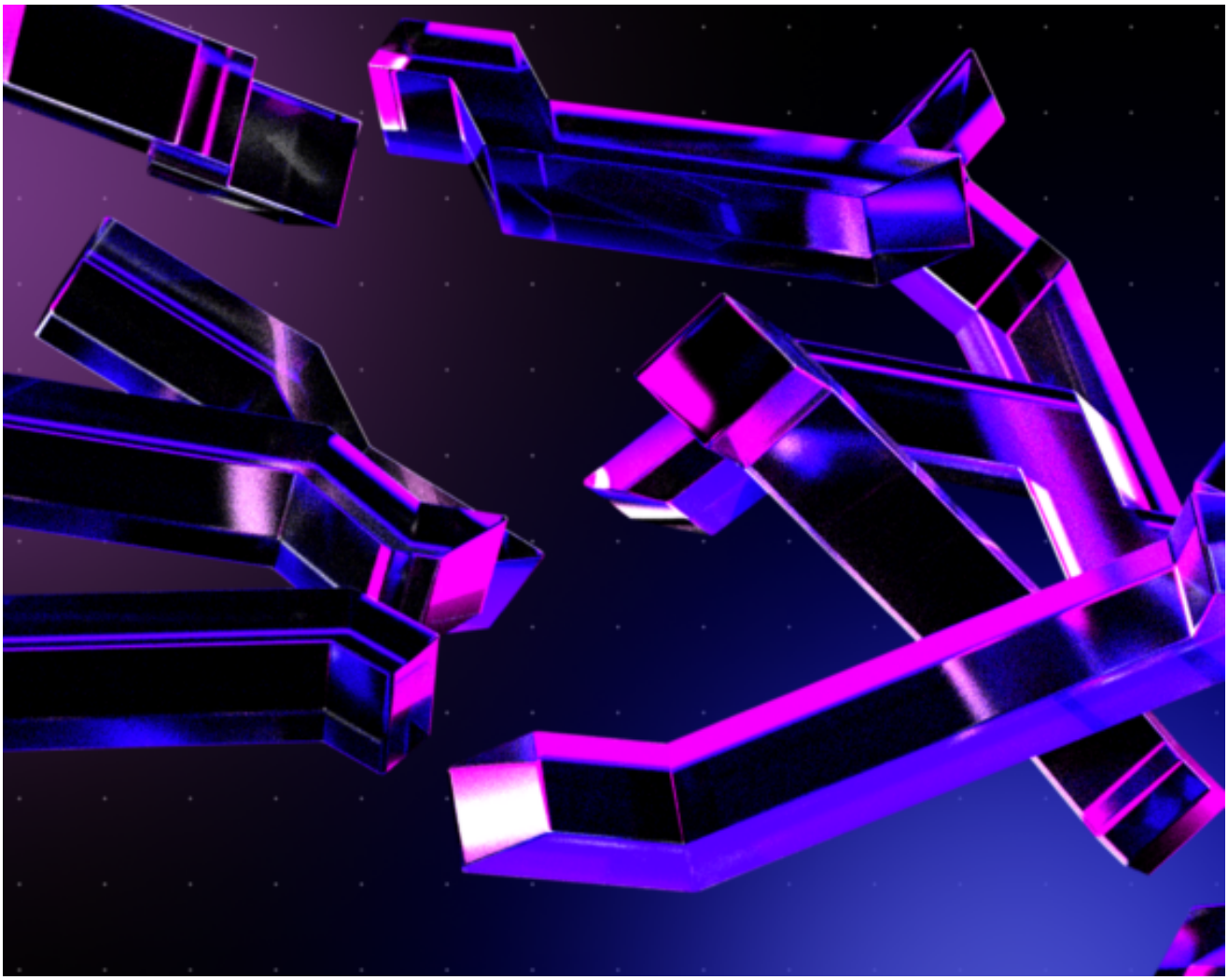
// AUDITS ETHEREUM WAKE AUGUST 2, 2024

Rhinestone Module Registry Audit Summary



// AUDITS ETHEREUM WAKE JULY 29, 2024

Lido stETH on Optimism Audit Summary



// EDUCATION, ETHEREUM, HACKS, TUTORIAL, WAKE JULY 11, 2024

Cross Contract Reentrancy Attack