Zellic

LayerZero Solidity Examples

Smart Contract Patch Review

January 19, 2023

Prepared for:

Ryan Zarick

LayerZero

Prepared by:

Katerina Belotskaya

Zellic Inc.

About Zellic

Zellic was founded in 2020 by a team of blockchain specialists with more than a decade of combined industry experience. We are leading experts in smart contracts and Web3 development, cryptography, web security, and reverse engineering. Before Zellic, we founded perfect blue, the top competitive hacking team in the world. Since then, our team has won countless cybersecurity contests and blockchain security events.

Zellic aims to treat clients on a case-by-case basis and to consider their individual, unique concerns and business needs. Our goal is to see the long-term success of our partners rather than to simply provide a list of present security issues. Similarly, we strive to adapt to our partners' timelines and to be as available as possible. To keep up with our latest endeavors and research, check out our website zellic.io or follow @zellic_io on Twitter. If you are interested in partnering with Zellic, please email us at hello@zellic.io or contact us on Telegram at https://t.me/zellic_io.

1 Introduction

We were asked to review a patch to the LayerZero Solidity Examples. The update added possibility to users to send and receive batch of tokenIds. We did not find any issues with the patch.

1.1 Scope

The engagement involved a review of the following targets:

proof-lib

Repository	https://github.com/LayerZero-Labs/solidity-examples
Versions	`306a8eb6d96959d51eadcb54ebd885c97ca45441`
Programs	• ONFT721 • ONFT721Core • UniversalONFT721 • ProxyONFT721
Type	Solidity
Platform	Ethereum (and other compatible chains)

Contact Information

The following project managers were associated with the engagement:

Jasraj Bedi, Co-founder
jazzy@zellic.io

The following consultants were engaged to conduct the assessment:

Katerina Belotskaia, Engineer
kate@zellic.io

1.2 Disclaimer

This assessment does not provide any warranties on finding all possible issues within its scope; i.e., the evaluation results do not guarantee the absence of any subsequent issues. Zellic, of course, also cannot make guarantees on any additional code added

to the assessed project after our assessment has concluded. Furthermore, because a single assessment can never be considered comprehensive, we always recommend multiple independent assessments paired with a bug bounty program. Finally, this assessment report should not be considered as financial or investment advice.

2 Patch Review

The patch itself was an update to the ONFT721, ONFT721Core, UniversalONFT721 and ProxyONFT721 contracts.

Updating the constructors of the ONFT721, UniversalONFT721 and ProxyONFT721 contracts. Added the `_minGasToTransfer` value to pass to the constructors of `ONFT721Core` contracts.

The changes listed below relate to the **ONFT721Core** contract:

Added `minGasToTransferAndStore` variable This value determines the minimum amount of gas at which the processing of the received message will be stopped and all necessary information will be saved to resume the receipt of tokens from this message.

Added the `sendBatchFrom` function. This function allows to send multiple `tokenIds`.

Added the `estimateSendBatchFee` function. This function returns the expected amount of gas required to send current batch of `tokenIds`.

Updation the internal `_send` function. The changes relate to the fact that the function now processes an array of `_tokenIds` instead of a single `_tokenId`.

Added the `storedCredits` mapping. This mapping is used to save the remaining batch of sent `tokenids`.

Added the `clearCredits` external function. This function is designed to resume sending `tokenids`, which was stopped due to insufficient gas amount.