Audit Report Summary

14th February 2025

Wanchain - Bridge

Contents

This document is provided to Wanchain as a strip down version of the full report generated by TxPipe. This document lacks all technical sections, including detailed explanations of all validators and minting policies, diagrams and explanations of all transactions involved in the protocol, and two anexes listing all compilation and hlint warnings that are referenced in findings WAN-303 and WAN-304. The full report was also provided to Wanchain on February 14th

1 - Summary

This report provides a thorough audit of the Wanchain Bridge, specifically focusing on the part of the protocol responsible for managing assets being transferred from and to the Cardano Blockchain. The audit process revealed potential vulnerabilities related mostly to the protocol deployment.

The audit is conducted without warranties or guarantees of the quality or security of the code. It's important to note that this report only covers identified issues, and we do not claim to have detected all potential vulnerabilities.

1.a - Overview

The Wanchain Bridge is a platform dedicated to enabling interoperability between different blockchain networks, allowing seamless cross-chain transactions and data transfers.

From the Cardano user perspective, the protocol enables users to lock assets into treasuries, which will be transferred to other blockchains. Dually, they can mint wrapped versions of assets coming from other blockchains into Cardano.

1.b - Process

Our audit process involved a thorough examination of Wanchain validators. Areas vulnerable to potential security threats were closely scrutinized, including those where attackers could exploit the validator's functions to disrupt the platform and its users. This included evaluating potential risks, such as stealing the tokens locked in the treasuries or using the mapping token policy to mint wrapped tokens illegally. It also included evaluating common vulnerabilities, such as double satisfaction and minting policy vulnerabilities.

Findings and feedback from the audit were communicated regularly to the Wanchain team through Telegram. Diagrams illustrating the necessary transaction structure for proper interaction with Wanchain are attached as part of the full report. The Wanchain team addressed these issues in an efficient and timely manner, enhancing the overall security of the platform.

2 - Audited Files

Below is a list of all audited files in this report. Any files **not** listed here were **not** audited. The final state of the files for the purposes of this report is considered to be commit `71f4424b8e87201cb137355cc16fc9e55a1d110a`.

Filename
./CrossChain/NFTMappingToken.hs
./CrossChain/GroupNFT.hs
./CrossChain/Types2.hs

./CrossChain/Treasury.hs

./CrossChain/GroupNFTHolder.hs

./CrossChain/NFTTreasuryCheck.hs

./CrossChain/Types.hs

./CrossChain/NFTRefHolder.hs

./CrossChain/TreasuryCheck.hs

./CrossChain/MappingToken.hs

./CrossChain/NFTMintCheck.hs

./CrossChain/NFTTreasury.hs

./CrossChain/StakeCheck.hs

./CrossChain/CheckToken.hs

./CrossChain/MintCheck.hs

./CrossChain/AdminNFTHolder.hs

./CrossChain/StoremanStake.hs

3 - Findings

ID	Title	Severity	Status
WAN-001	Multiple check tokens can be locked in the same UTxO	Critical	Resolved
WAN-101	Treasury UTxOs can contain more than one token	Major	Resolved
WAN-201	Possible protocol lockdown by providing an invalid list of signatories	Minor	Acknowledged
WAN-301	Prevent inclusion of reference scripts	Info	Acknowledged
WAN-302	Mapping tokens could be minted during the mintCheckToken burn operations	Info	Acknowledged
WAN-303	Multiple compilation warnings present	Info	Acknowledged
WAN-304	Hlint style suggestions	Info	Acknowledged
WAN-305	Commented code in all modules	Info	Acknowledged

A Appendix

A.1 Terms and Conditions of the Commercial Agreement

A.1.1 Confidentiality

Both parties agree, within a framework of trust, to discretion and confidentiality in handling the business. This report cannot be shared, referred to, altered, or relied upon by any third party without Txpipe LLC, 651 N Broad St, Suite 201, Middletown registered at the county of New Castle, written consent.

The violation of the aforementioned, as stated supra, shall empower TxPipe to pursue all of its rights and claims in accordance with the provisions outlined in Title 6, Subtitle 2, Chapter 20 of the Delaware Code titled "Trade Secrets,", and to also invoke any other applicable law that protects or upholds these rights.

Therefore, in the event of any harm inflicted upon the company's reputation or resulting from the misappropriation of trade secrets, the company hereby reserves the right to initiate legal action against the contractor for the actual losses incurred due to misappropriation, as well as for any unjust enrichment resulting from misappropriation that has not been accounted for in the calculation of actual losses.

A.1.2 Service Extension and Details

This report does not endorse or disapprove any specific project, team, code, technology, asset or similar. It provides no warranty or guarantee about the quality or nature of the technology/code analyzed.

This agreement does not authorize the client Wanchain to make use of the logo, name, or any other unauthorized reference to Txpipe LLC, except upon express authorization from the company.

TxPipe LLC shall not be liable for any use or damages suffered by the client or third-party agents, nor for any damages caused by them to third parties. The sole purpose of this commercial agreement is the delivery of what has been agreed upon. The company shall be exempt from any matters not expressly covered within the contract, with the client bearing sole responsibility for any uses or damages that may arise.

Any claims against the company under the aforementioned terms shall be dismissed, and the client may be held accountable for damages to reputation or costs resulting from non-compliance with the aforementioned provisions. **This report provides general information and is not intended to constitute financial, investment, tax, legal, regulatory, or any other form of advice.**

Any conflict or controversy arising under this commercial agreement or subsequent agreements shall be resolved in good faith between the parties. If such negotiations do not result in a conventional agreement, the parties agree to submit disputes to the courts of Delaware and to the laws of that jurisdiction under the powers conferred by the Delaware Code, TITLE 6, SUBTITLE I, ARTICLE 1, Part 3 § 1-301. and Title 6, SUBTITLE II, chapter 27 §2708.

A.1.3 Disclaimer

The audit constitutes a comprehensive examination and assessment as of the date of report submission. The company expressly disclaims any certification or endorsement regarding the subsequent performance, effectiveness, or efficiency of the contracted entity, post-report delivery, whether resulting from modification, alteration, malfeasance, or negligence by any third party external to the company.

The company explicitly disclaims any responsibility for reviewing or certifying transactions occurring between the client and third parties, including the purchase or sale of products and services.

This report is strictly provided for ***informational purposes*** and reflects solely the due diligence conducted on the following files and their corresponding hashes using sha256 algorithm:

Filename: `./CrossChain/NFTMappingToken.hs` **Hash**: `d6135c51c6c0dba0e8e18b2a8f749a9de1729fcac8a710632e9a1604d2b5e644`
Filename: `./CrossChain/GroupNFT.hs` **Hash**: `c6ff123d58eb30ae47f0945a88407d7b268ff04d354baf33cdcef3ad4be4e864`
Filename: `./CrossChain/Types2.hs` **Hash**: `e66706328216c3db5a662bff044d68a597e5f5177a0efcd38e459429beda82c0`
Filename: `./CrossChain/Treasury.hs` **Hash**: `64ef48c7a35ee4b27cf2afae9114bba61d4345fb4c188bdd66c0e51987c3848c`
Filename: `./CrossChain/GroupNFTHolder.hs` **Hash**: `290971720060b7e2ab883a55af9fc55851caaf7d7e2143bdbce2031d4435cfb9`
Filename: `./CrossChain/NFTTreasuryCheck.hs` **Hash**: `e965b435e2f6bdcf8c8b0b1f5de26ab35211f49881365271c9827f4bd55a2791`
Filename: `./CrossChain/Types.hs` **Hash**: `9475ca2619d09fcb8de07cd02fcc215a8c386d05cbd6c6ea3b2ef21d95679575`
Filename: `./CrossChain/NFTRefHolder.hs` **Hash**: `ab7c33cc316f891a37edcd789d5d6cf44edcd3c81e75ab033314161a1486e244`
Filename: `./CrossChain/TreasuryCheck.hs` **Hash**: `e799b8121b5acf9d47e644dde3cce2609dbae304b9787d252227cb143c695a3a`
Filename: `./CrossChain/MappingToken.hs` **Hash**: `a6728d5948c8ac74d4023ed2799ba4fa15acd6459b80c14cab10f142ee05fa4b`
Filename: `./CrossChain/NFTMintCheck.hs` **Hash**: `7a987c75788def42f03ea441a1ac1a01fdfd4a6193d44664b97a509e39e6594a`
Filename: `./CrossChain/NFTTreasury.hs` **Hash**: `cc5c3c71eb7a03458a2f8dd969a8c2173e7d169c2385a297fcea6e73716ec532`
Filename: `./CrossChain/StakeCheck.hs` **Hash**: `dc44f5a0bc6860801b88258e19822809ec428e6e2338438747447adb419384ed`
Filename: `./CrossChain/CheckToken.hs` **Hash**: `c26303a17924418d1bb2ab1e4adbda14aee3a641b1aed88d66d1538aca9decce`
Filename: `./CrossChain/MintCheck.hs` **Hash**: `daa21d5d5746e9c6748ea53f263698a0014964322e1c9a4ba712662011b8c192`
Filename: `./CrossChain/AdminNFTHolder.hs` **Hash**: `3e21aa884d5bb19755df930b85acee7b49c8491890c8e30016ebd98d6cd37a9c`
Filename: `./CrossChain/StoremanStake.hs` **Hash**: `76479ec119b9ad8cf64504dc205eceb52a3c7d4a0244986d7aca9277412edb5c`

TxPipe advocates for the implementation of multiple independent audits, a publicly accessible bug bounty program, and continuous security auditing and monitoring. Despite the diligent manual review processes, the potential for errors exists. TxPipe strongly advises seeking multiple independent opinions on critical matters. It is the firm belief of TxPipe that every entity and individual is responsible for conducting their own due diligence and maintaining ongoing security measures.

A.2 Issue Guide

A.2.1 Severity

Severity	Description
Critical	Critical issues highlight exploits, bugs, loss of funds, or other vulnerabilities that prevent the dApp from working as intended. These issues have no workaround.
Major	Major issues highlight exploits, bugs, or other vulnerabilities that cause unexpected transaction failures or may be used to trick general users of the dApp. dApps with Major issues may still be functional.
Minor	Minor issues highlight edge cases where a user can purposefully use the dApp in a non-incentivized way and often lead to a disadvantage for the user.
Info	Info are not issues. These are just pieces of information that are beneficial to the dApp creator. These are not necessarily acted on or have a resolution, they are logged for the completeness of the audit.

A.2.2 Status

Status	Description
Resolved	Issues that have been **fixed** by the **project** team.
Acknowledged	Issues that have been **acknowledged** or **partially fixed** by the **project** team. Projects can decide to not **fix** issues for whatever reason.
Identified	Issues that have been **identified** by the **audit** team. These are waiting for a response from the **project** team.

A.3 Revisions

This report was created using a git based workflow. All changes are tracked in a github repo and the report is produced using typst. The report source is available here. All versions with downloadable PDFs can be found on the releases page.

A.4 About Us

TxPipe is a blockchain technology company responsible for many projects that are now a critical part of the Cardano ecosystem. Our team built Oura, Scrolls, Pallas, Demeter, and we're the original home of Aiken. We're passionate about making tools that make it easier to build on Cardano. We believe that blockchain adoption can be accelerated by improving developer experience. We develop blockchain tools, leveraging the open-source community and its methodologies.

A.4.1 Links

- Website
- Email
- Twitter