QuillAudits

Audit Report
December, 2024

For

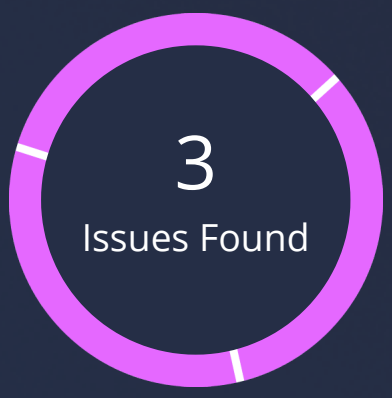
POWERED BY WADZCHAIN NETWORK

Table of Content

Executive Summary

Project Name	W Chain
Project URL	https://www.wadzchain-network.io/
Overview	W Chain is a hybrid blockchain platform that blends the openness and transparency of public blockchains with the control and security of private networks. This unique architecture ensures that businesses can operate with confidence, knowing they have the flexibility to maintain privacy where needed, while also benefiting from the decentralization of a public chain.
Audit Scope	The scope of this Audit was to analyze the W Chain Codebase for quality, security, and correctness.
Contracts In-Scope	https://github.com/wadzchain/wadzchain-node
Method	Manual Analysis, Functional Testing, Automated Testing
First Review	18th November 2024 - 11th December 2024
Updated Code Received	NA
Fixed In	NA

Number of Security Issues per Severity



High
Medium
Low
Informational

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	3
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	0	0

Checked Vulnerabilities

- Denial of Service (DoS) Attacks
- Consensus Mechanism Vulnerabilities
- RPC Interface Vulnerabilities
- Input Validation Issues
- Memory Consumption bug
- State Management Flaws
- Timejacking attack
- Double-spending attack
- 51% attack

Techniques and Methods

Throughout the audit of Codebase, care was taken to ensure:

- The overall quality of code.
- Security measures in Codebase
- Use of best practices.

The following techniques, methods, and tools were used to review Codebase.

Architecture Review

Assess the overall architecture of the L1 chain for resilience against attacks. This includes evaluating:

- The consensus mechanism's robustness.
- Node security and access control measures.
- Scalability to handle potential DDoS attacks

Static Analysis

A static Analysis of Codebase was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of Codebase.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Codebase were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behavior of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Go Sec, Static check

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

Informational Issues

1. EVM Support Focused on London Hardfork

Description

The current architecture of W Chain supports the EVM implementation up to the London Hardfork, ensuring compatibility with a wide range of smart contracts. While this provides a stable and reliable foundation, subsequent Ethereum hardforks have introduced additional features and optimizations, such as the PUSH0 opcode from the Paris upgrade. These features are currently not available on W Chain but can be incorporated through future updates.

Contracts compiled with Solidity versions up to 0.8.19 are fully supported on W Chain. However, for contracts utilizing newer Solidity compiler features introduced after this version, support will require an upgrade to the chain's EVM implementation.

Recommendation

Upgrade the chain's EVM implementation to support the latest hardforks listed in the Ethereum history.

Status

Acknowledged

2. Mandatory Bridge Requirement Conflicts with L1 Design Assumptions

Description

Current architecture of the code is intertwined with the bridge between rootchain and child chain and it is mandatory to run the bridge to start the blockchain, However As per W Chain team, they are L1 and there is no concept of root chain and child chain for them. Current code conflicts the assumption.

Recommendation

Refactor the architecture to decouple the bridge functionality from the blockchain's core operations. Ensure the chain can operate independently as a true L1 blockchain. Provide an option to deploy and use the bridge only when required, aligning with the stated assumptions of the client's infrastructure.

W Chain Team's Comment

The WCO bridge is designed as a bridge between L1 (ETH, BSC) and L1 (W Chain). The on-chain node is used as a signer for multi-signer bridging of the WCO. This is also to save EC2 resources. Please note this is a L1 <> L1. We believe there may have been a mistake in the interpretation thinking this is a bridge between L1 and L2.

Status

Acknowledged

3. Parent Repository Archived and No Longer Maintained

Description

Parent repository code as been archived, so no active development and support from the polygon team on polygon-edge code, However polygon introduced a new framework called polygon-cdk which can be used further down the line to keep getting the latest development changes, However W Chain has to upgrade the framework to get it supported.

Recommendation

An issue has been added Just to make sure that the W Chain Team is aware about this.

W Chain Team's Comment

We see no issue with the archived code of the Polygon repository. It has no relevance to W Chain which is a standalone L1 blockchain in its own right and receives no feed or updates from this pre-existing forked code. All code has been pushed to the W Chain repository and will also be where any blockchain updates and upgrades will also be housed.

Status

Acknowledged

Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

Closing Summary

In this report, we have considered the security of W Chain. We performed our audit according to the procedure described above.

Some issues of informational severity were found. Some suggestions, gas optimizations and best practices are also provided in order to improve the code quality and security posture.

Disclaimer

QuillAudits Smart contract security audit provides services to help identify and mitigate potential security risks in W Chain. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of W Chain. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of W Chain to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a leading name in Web3 security, offering top-notch solutions to safeguard projects across DeFi, GameFi, NFT gaming, and all blockchain layers. With six years of expertise, we've secured over 1000 projects globally, averting over $30 billion in losses. Our specialists rigorously audit smart contracts and ensure DApp safety on major platforms like Ethereum, BSC, Arbitrum, Algorand, Tron, Polygon, Polkadot, Fantom, NEAR, Solana, and others, guaranteeing your project's security with cutting-edge practices.

1000+
Audits Completed

$30B
Secured

1M+
Lines of Code Audited

Follow Our Journey

Audit Report
December, 2024

For

POWERED BY WADZCHAIN NETWORK

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com