ASTROBIATECH
BLOCKCHAIN SECURITY

SECURITY ASSESSMENT REPORT

PREPARED FOR

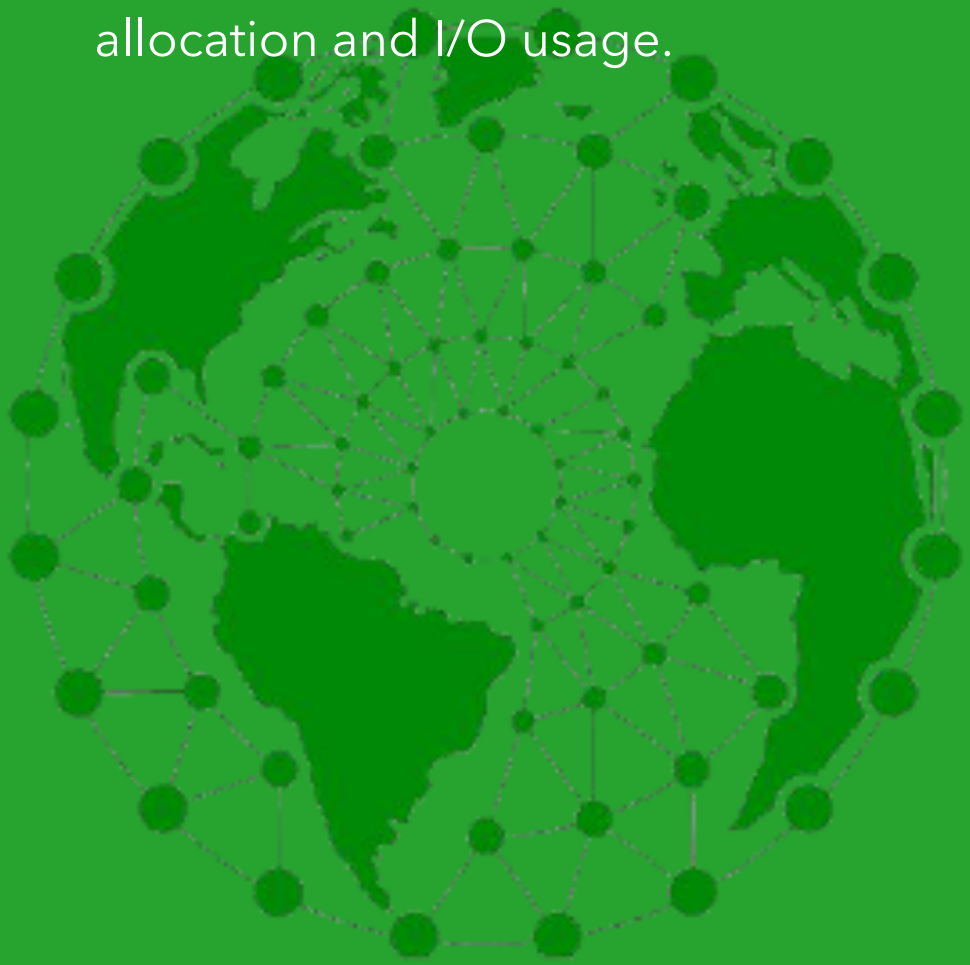
BAAZ CHAIN

OCTOBER
2024

TABLE OF CONTENT

SCOPE OF AUDIT

The purpose of this audit was to evaluate and document the Baaz Chain codebase, focusing on its quality, security, and correctness. Astrobiatech Blockchain Security conducted a thorough review, particularly examining potential vulnerabilities related to Denial-of-Service through excessive memory allocation and I/O usage.



TECHNIQUES AND METHODS

Throughout the audit of the code, care was taken to ensure :-

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Efficient use of inbuilt functionality.
- Code is safe from known attack vectors.

Structural Analysis

In this step, we conducted a comprehensive analysis of the codebase's design patterns and structure. We performed a detailed review to confirm that the code is organised in a way that minimises the risk of future issues.

Static Analysis

A static Analysis of the code base was done to identify vulnerabilities.

Code Review / Manual Analysis

A manual code analysis and review were conducted to identify any new vulnerabilities and to verify those detected during the static analysis. The modified code segments were thoroughly examined, with their logic assessed to ensure consistency and security alignment.

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.

Types of Severities

High
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
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
Low-level severity issues can cause minor impact and or 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 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.

INTRODUCTION

PROJECT NAME Baaz Chain

TIMELINE 22 October 2024 - 6 November 2024

RPC DETAILS

NAME	Baaz Chain
RPC URL	https://rpc.baazscan.com/
SYMBOL	BAAZ
CHAIN ID	1334
BLOCK EXPLORER	https://baazscan.com/

HIGH **MEDIUM**

LOW **INFORMATIONAL**

	HIGH	MEDIUM	LOW	INFORMATIONAL
Open Issues	0	0	2	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	0	0

CHECKED VULNERABILITIES

- SHA-256 Hash Function Integrity
- Denial of Service (DoS) Attack Prevention
- Consensus Rule Enforcement
- Block Synchronisation and Download Efficiency
- Peer-to-Peer (P2P) Network Security
- Centralisation Risk Assessment
- Transaction Validation and Filtering
- Memory Management and Resource Optimisation
- Network Latency and Fault Tolerance
- RPC Endpoint Security and Authentication
- Data Integrity and Consistency Verification
- Node Configuration and Access Control
- Encryption and Authentication of Signer Nodes

MANUAL ANALYSIS FINDINGS

HIGH SEVERITY ISSUES

No Issues Found

MEDIUM SEVERITY ISSUES

No Issues Found

LOW SEVERITY ISSUES

1. High Gas Limit Configuration

Description :- The gasLimit is set to "0x47b760" (4,716,000), which might be higher than necessary for a smaller or permissioned network. A high gas limit could lead to larger blocks, increased storage needs, and slower syncing for new nodes, especially if transaction volume is low.

Recommendation :- Adjust the gasLimit to better match your expected transaction volume, such as 2,000,000 or lower for PoS networks with moderate usage. This can improve sync speeds and reduce the computational load on nodes, making the chain more efficient.

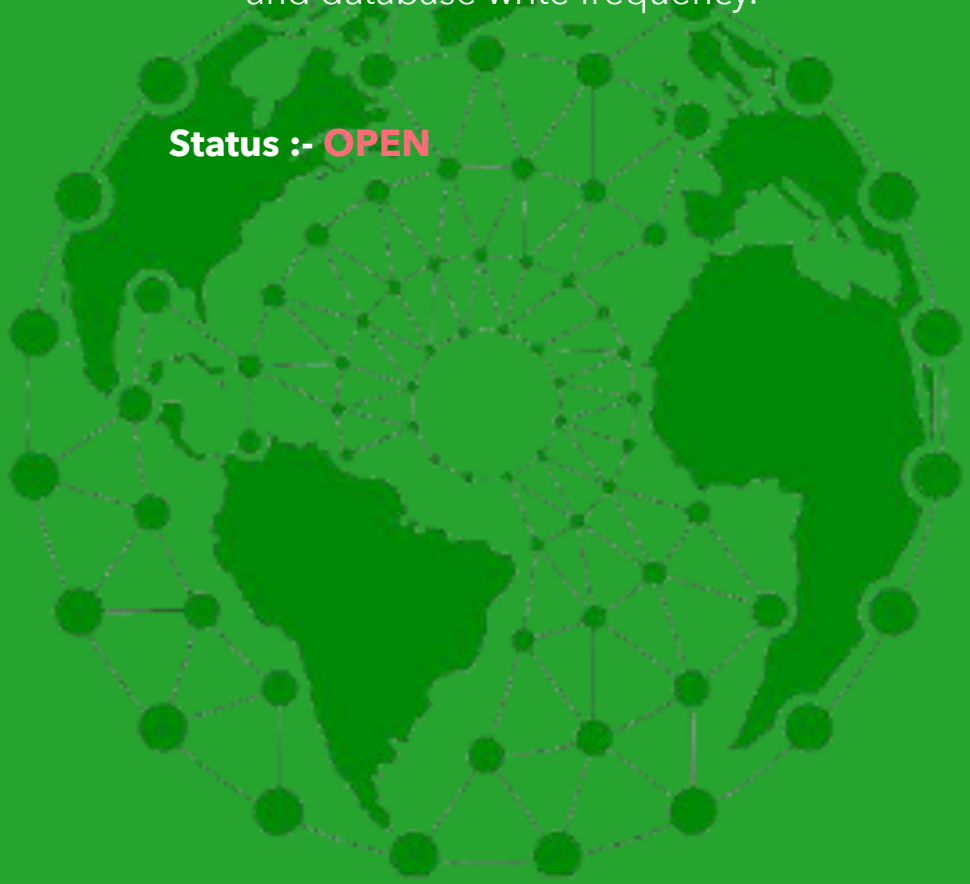
Status :- OPEN

2. Slow Sync Performance

Description :- Full and fast sync modes may lag if the blockchain size grows quickly, causing nodes to fall behind, impacting their ability to serve timely data to applications on Baaz Chain.

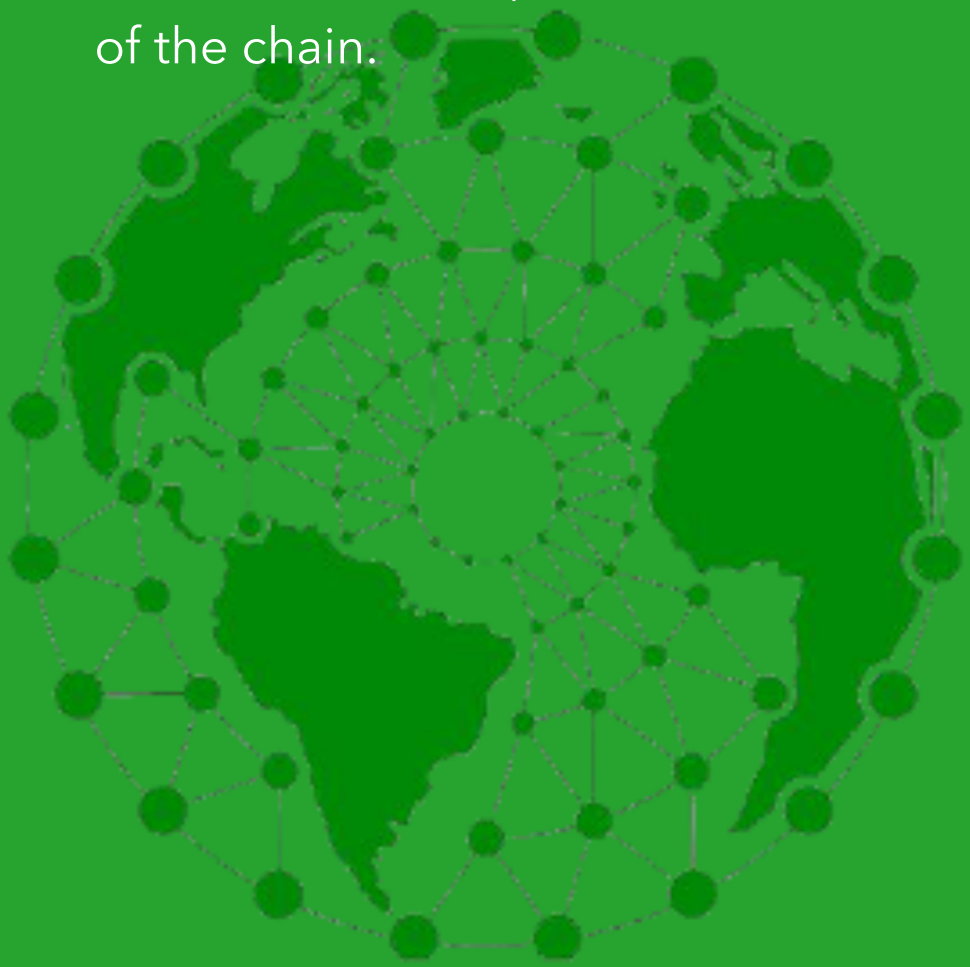
Recommendation :- Use the `snap` sync mode, which improves synchronisation speed by only downloading recent state data. Consider optimising sync configuration settings, such as cache and database write frequency.

Status :- OPEN



SUMMARY

During a security assessment of the Baaz Chain blockchain codebase, the Astrobiatech Blockchain Security team found the code to be of high quality and developed with a strong focus on security. No security vulnerabilities were identified. Only two low-severity issues were noted, neither of which impacts the security of the chain.



DISCLAIMER

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Astrobiatech Blockchain Security and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Astrobiatech BlockchainSecurity) owe no duty of care towards you or any other person, nor does Astrobiatech Blockchain Security make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Astrobiatech Blockchain Security hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Astrobiatech Blockchain Security hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Astrobiatech Blockchain Security, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

BAAZ CHAIN

Proofed by Astrobiatech

ASTROBIATECH
BLOCKCHAIN SECURITY

@astrobiatech
https://astrobiatech.in