verichains

SECURITY AUDIT OF

BLAT TOKEN

Public Report

Jun 27, 2023

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Sui Blockchain	Sui is an innovative, decentralized Layer 1 blockchain that redefines asset ownership. Sui Move feels like a paradigm change in web3 development. Treating objects as 1st class citizens brings composability to a whole new level. Polymedia. We are thrilled to be building on Sui.
Sui Object	The basic unit of storage in Sui is object. In contrast to many other blockchains where storage is centered around accounts and each account contains a key-value store, Sui's storage is centered around objects.
Sui Framework	The Sui Framework includes the core on-chain libraries for Sui Move developers.
Move	Move is a new programming language that implements all the transactions on the Aptos/Sui blockchain.
Move Module	A Move module defines the rules for updating the global state of the Aptos/Sui blockchain. In the Aptos/Sui protocol, a Move module is a smart contract.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Jun 27, 2023. We would like to thank the BeLaunch for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the BLAT Token. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified NO vulnerable issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About BLAT Token

BLAT Token plays a crucial role in the Belaunch ecosystem, serving as the underlying token that drives its tokenomics. As per the documentation provided by Belaunch, BLAT Token is scheduled to undergo both a private sale and a public sale. The remaining tokens will be allocated towards supporting the ecosystem, staking, research and development, marketing activities, and community.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the BLAT Token. It was conducted on commit `e8b9497557bd686352c2d1417a23aa8ee33eafc0` from git repository link: *https://github.com/belaunch-io/belaunch-contract*

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Numerical precision errors
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- Gas Usage, Gas Limit and Loops
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.

SEVERITY LEVEL	DESCRIPTION
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure smart contract. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The BLAT Token was developed using the Move programming language and deployed on the Sui Blockchain.

Within the package, the BLAT module depend on the `coin module` provided by the `Sui Framework` mainnet version to facilitate the operations of the token.

The token is initialized with read-only permission for its Metadata access, and the owner mints 100 million tokens. Additionally, the Treasury object has been frozen, preventing the ability to mint additional tokens. As a result, the maximum capacity of the token is 100 million. Here is a table presenting some properties extracted from the token's metadata:

PROPERTY	VALUE
Name	BeLaunch Token
Symbol	BLAT
Decimals	9
Total Supply	100,000,000 ($x10^9$) Note: the number of decimals is 9, so the total representation token will be 100,000,000 or 100 million.
Capacity	100,000,000 ($x10^9$)

Table 2. The BLAT Token properties

2.2. Findings

During the audit process, the audit team had identified NO vulnerable issues in the smart contracts code.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Jun 27, 2023*	Public Report	Verichains Lab

Table 3. Report versions history