



QuillAudits

Audit Report January, 2022



For



ARCHEAN

Contents

Scope of Audit	01
Check Vulnerabilities	01
Techniques and Methods	02
Issue Categories	03
Number of security issues per severity.	03
Introduction	04
High Severity Issues	05
Medium Severity Issues	05
Low Severity Issues	05
Informational Issues	05
Functional Tests	06
Functionality Tests Performed	07
Automated Tests	08
Closing Summary	09

Scope of the Audit

The scope of this audit was to analyze and document the Archean Token smart contract codebase for quality, security, and correctness.

Checked Vulnerabilities

We have scanned the smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

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. Contracts were completely manually analysed, 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 behaviour 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

Remix IDE, Truffle, Truffle Team, Solhint, Mythril, Slither, Solidity statistic analysis, Theo.

Issue Categories

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.

Risk-level	Description
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.

Number of issues per severity

Type	High	Medium	Low	Informational
Open	0	0	0	0
Acknowledged	0	0	0	0
Closed	0	0	0	0

Introduction

During the period of **January 12, 2022 to January 14, 2022** - QuillAudits Team performed a security audit for the ArcheanGoldToken smart contract. The code for the audit was taken from the following:-

<https://rinkeby.etherscan.io/address/0x768f3FeB5781a8Cb8d26027BB345A1C5975DbA52#code>

The contract was deployed and tested on Ropsten and you can find it here:
ArcheanGoldToken: [0xAC2dfE9FFBE0178E393EB7E7D67a5Ec46946BA6F](https://ropsten.etherscan.io/address/0xAC2dfE9FFBE0178E393EB7E7D67a5Ec46946BA6F)

Issues Found – Code Review / Manual Testing

High severity issues

No issues were found.

Medium severity issues

No issues were found.

Low severity issues

No issues were found.

Informational issues

No issues were found.



Functional Tests

Function Names	Testing results
transfer	Passed
transferFrom	Passed
burn	Passed
burnFrom	Passed
approve	Passed
initialize	Passed
mint	Passed
increaseAllowance	Passed
decreaseAllowance	Passed
assignMinterRole	Passed
grantRole	Passed
renounceRole	Passed
revokeRole	Passed

Functional Testing Results

- Users should be able to transfer tokens not more than their balance. PASS
- approve. PASS
- Users should be able to transferFrom tokens not more than their approval and also not more than the owner's(token owner not the contract owner) balance. PASS
- Users should be able to burn tokens not more than their balance. PASS
- Users should be able to burnFrom tokens not more than their approval. PASS
- Only the default admin should be able to grantRole. PASS
- Only the account with the role should be able to renounceRole. PASS
- Users should be able to increaseAllowance. PASS
- Users should be able to decreaseAllowance. PASS
- Only the default admin should be able to revokeRole. PASS
- Only the default admin should be able to assignMinterRole. PASS
- Only an account with a minter role should be able to mint tokens. PASS
- The contract should only initialize once. PASS

Automated Tests

Mythril

Mythril is a security analysis tool for EVM bytecode. It detects security vulnerabilities in smart contracts built for Ethereum, Hedera, Quorum, VeChain, Roostock, Tron and other EVM-compatible blockchains. It uses symbolic execution, SMT solving and taint analysis to detect a variety of security vulnerabilities. Mythril raised the following concerns:

```
The analysis was completed successfully. No issues were detected.
```

Contract Library

Contract-library contains the most complete, high-level decompiled representation of all Ethereum smart contracts, with security analysis applied to these in real-time.

We performed analysis using the contract Library on the Ropsten address of the Archean contract used during manual testing:

Archean: [0xAC2dfE9FFBE0178E393EB7E7D67a5Ec46946BA6F](#)

Results

No issues were found in the audit.

Closing Summary

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

The audit showed no issues.



Disclaimer

Quillhash audit is not a security warranty, investment advice, or an endorsement of the Archean platform. This audit does not provide a security or correctness guarantee of the audited smart contracts. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the Archean Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

Audit Report January, 2022

For



ARCHEAN



QuillAudits

📍 Canada, India, Singapore, United Kingdom

🌐 audits.quillhash.com

✉️ audits@quillhash.com