verichains

SECURITY AUDIT OF

ABI SMART CONTRACTS

Public Report

Dec 15, 2021

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report prepared by Verichains Lab on Dec 15, 2021. We would like to thank the ABIGames 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 ABI Smart Contracts. 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 issue in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About ABIGames

ABI Game Studio is an independent team within Onesoft Studio. It has been one of the top 10 major game companies in Southeast Asia, and currently ranked 2nd in the most recent Top Publishers Awards by App Annie.

1.2. About ABI Smart Contracts

ABI Crypto Games Platform is a community-driven GameFi platform that empowers users by rewarding them for their engagement and enjoyment. ABI Gamefi Platform implements the innovative ABI tokenomics that combines finance and game and uses the best of DeFi and NFTs to create a truly unique and everlasting FREE TO PLAY, PLAY FOR FUN, PLAY TO EARN ECOSYSTEM.

1.3. Audit scope

This audit focused on identifying security flaws in code and the design of ABI Smart Contracts. It was conducted on commit 2036afa72e2b4cc20aba0f74ab7715ab6fb2a137 from git repository link: *https://github.com/ABICryptoGames/smartcontract*.

1.4. 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 was considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference

- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- 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.
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

1.5. 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 initial review was conducted on Dec 05, 2021 and a total effort of 5 working days was dedicated to identifying and documenting security issues in the code base of the ABI Smart Contracts.

2.2. Contract code

The ABI Smart Contracts was written in Solidity language, with the required version to be ^0.8.0. The source code was written based on OpenZeppelin's library.

2.2.1. ABItoken contract

The ABI token contract is an ERC20 token contract. Besides the default ERC20 functions, the contract implements five functions which allow owner can set pool addresses. Pools are the contracts that supports the ABIGames to release ABI tokens. They are mainPool, playPool, partnerPool, miningPool, marketingPool.

Table 2 lists some properties of the audited ABItoken contract (as of the report writing time).

PROPERTY	VALUE
Name	ABI
Symbol	ABI
Decimals	18
Total Supply	1,000,000,000 ($x10^{18}$) Note: the number of decimals is 18, so the total representation token will be 1,000,000,000 or 1 billion.

Table 2. The ABI token contract properties

2.2.2. BoxToken contract

The BoxToken contract is an ERC1155 token contract. The contract inherits the ERC1155Supply contract, so the contract adds tracking of total support per id.The contract implements mint, mintBatch, burn, burnBatch external function with onlyOwner modifier. So only Operator of contract can uses these functions.

2.2.3. GARToken contract

The GARToken contract is an ERC20 token contract. Currently, the contract doesn't have exactly value of totalSupply. The contract implements mint external function with onlyOwner modifier. So the only owner of the contract can mint new tokens which can change the totalSupply of the contract.

In addition, the contract implements the burnFrom function. So an allowance account can call this function to remove the owner balances.

Table 3 lists some properties of the audited GARtoken contract (as of the report writing time).

PROPERTY	VALUE
Name	Galaxy Attack Revolution
Symbol	GAR
Decimals	18

Table 3. The GARToken contract properties

2.2.4. ShipToken contract

The ShipToken contract is an ERC721 token contract. The contract implements mint external function with onlyOperator modifier. So only Operator of contract can mint new tokens.

2.3. Findings

During the audit process, the audit team found no vulnerability in the given version of ABI Smart Contracts.

2.4. Additional notes and recommendations

2.4.1. Unnecessary usage of SafeMath library in Solidity 0.8.0+ INFORMATIVE

All safe math usages in the contract are for overflow checking, solidity 0.8.0+ already do that by default, the only usage of safemath now is to have a custom revert message which isn't the case in the auditing contracts. We suggest using normal operators for readability and gas saving.

Currently, the methods of SafeMath are used in ABIToken.sol, BoxToken.sol, GARToken.sol files.

RECOMMENDATION

We suggest changing all methods from SafeMath library to normal arithmetic operator in the files that we regarded above.

UPDATES

- *Dec 15,2021*: This issue has been acknowledged and fixed by the ABIGames team in commit b9c04310d640c750c6b83f2093d984eca9d34f6b.

2.4.2. Unused SafeERC20 library INFORMATIVE

Both ABIToken and GARToken contract imported SafeErc20 library. The SafeER20 is used for IERC20 but the methods of SafeER20 isn't used anywhere.

RECOMMENDATION

We suggest removing them for readability (including the import SafeER20 statements and the codes uses SaferERC20 for IERC20).

UPDATES

- *Dec 15,2021*: This issue has been acknowledged and fixed by the ABIGames team in commit b9c04310d640c750c6b83f2093d984eca9d34f6b.

APPENDIX

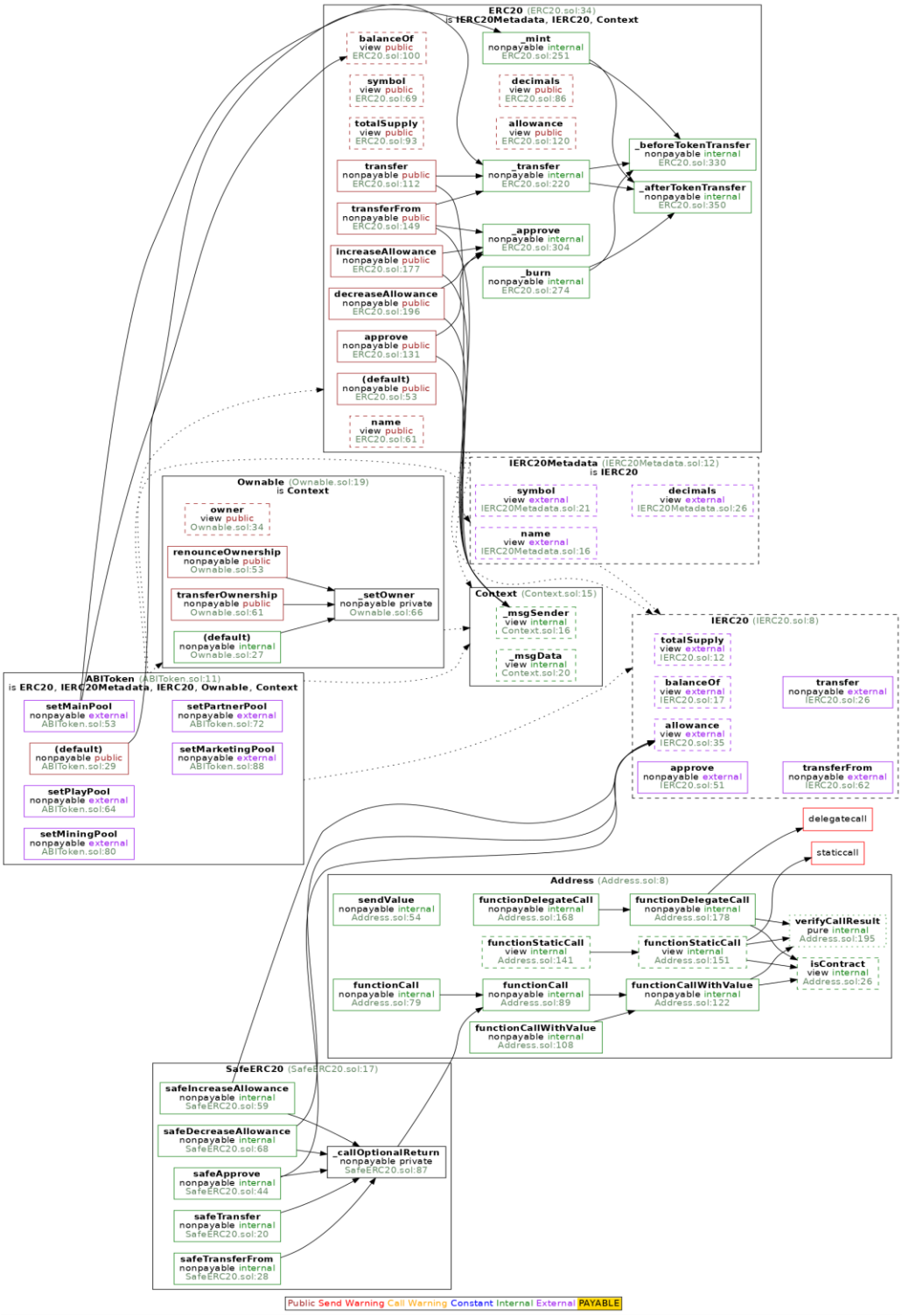

Image 1. ABI token smart contract call graph

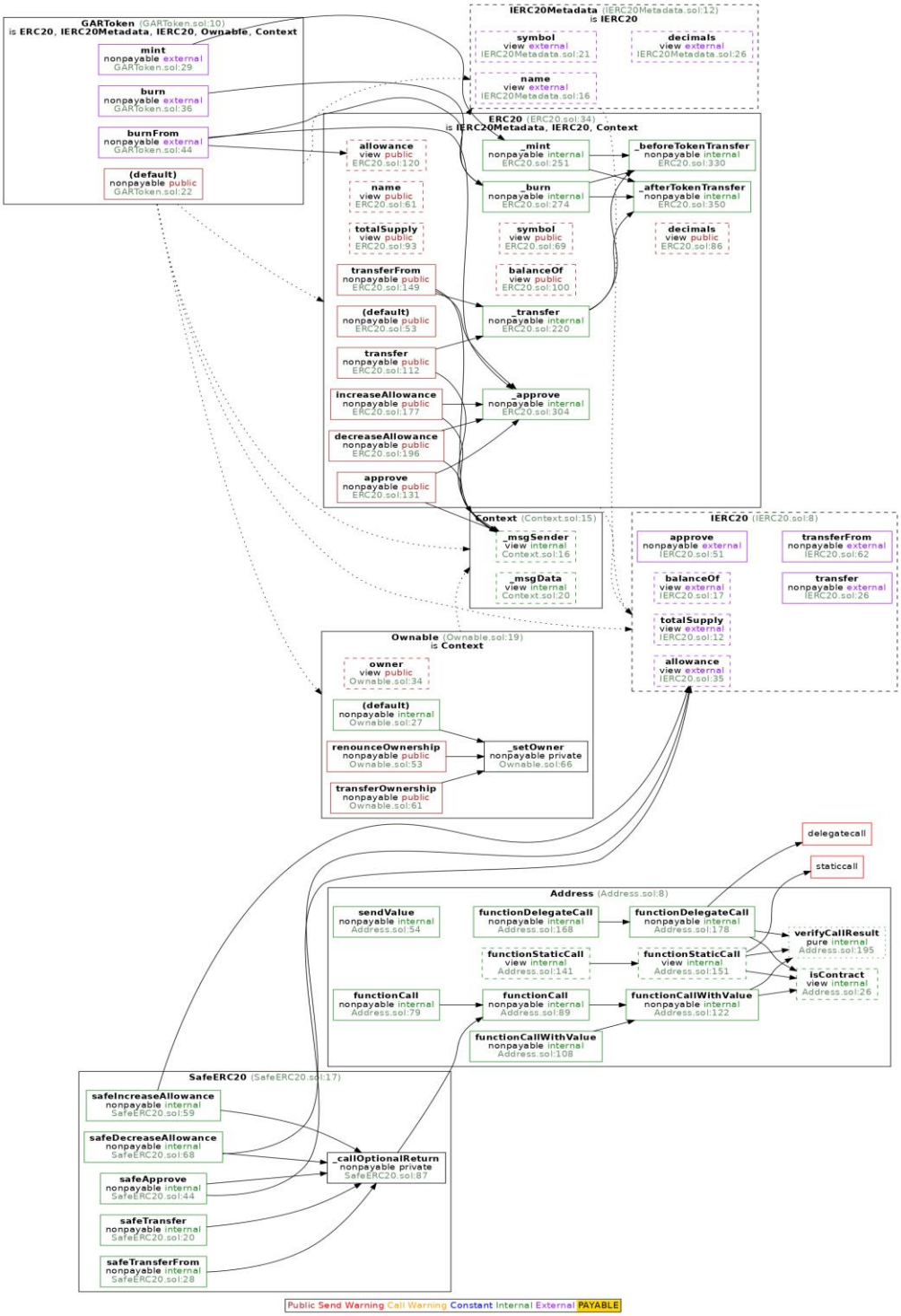

Image 2. GAR token smart contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Dec 10, 2021*	Public Report	Verichains Lab
1.1	*Dec 13, 2021*	Public Report	Verichains Lab
1.2	*Dec 15, 2021*	Public Report	Verichains Lab

Table 4. Report versions history