SECURITY AUDIT OF

GPTVERSE TOKEN SMART CONTRACT

Public Report

Jan 5, 2024

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 was prepared by Verichains Lab on Jan 5, 2024. We would like to thank the GPTVERSE 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 GPTVERSE Token Smart Contract. 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 vulnerability issue in the contract code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About GPTVERSE Token Smart Contract

GptVerse is a multiplatform project which will have both a Dapp version and a Metaverse App version for products. GptVerse is not just another metaverse; it's a vibrant and immersive world where AI-driven technologies seamlessly integrate with social interactions, education, finance, marketing, shopping, events, design, and NFTs. Their mission is to create a dynamic and inclusive environment that empowers individuals and businesses to unlock the full potential of AI.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the GPTVERSE Token Smart Contract.

The audited contract is the GPTVERSE Token Smart Contract that deployed on Binance Smart Chain Mainnet at address `0x1F56eFffEe38EEeAE36cD38225b66c56E4D095a7`. The details of the deployed smart contract are listed in Table 1.

FIELD	VALUE
Contract Name	Gptverse
Contract Address	0x1F56eFffEe38EEeAE36cD38225b66c56E4D095a7
Compiler Version	v0.8.0+commit.c7dfd78e
Optimization Enabled	No with 200 runs
Explorer	*https://bscscan.com/address/0x1F56eFffEe38EEeAE36cD38225b66c56E4D095a7*

Table 1. The deployed smart contract details

1.3. Audit methodology

Our security audit process includes four steps:

- Mechanism Design is reviewed to look for any potential problems.

- Source codes are scanned/tested for commonly known and more specific vulnerabilities using public and our in-house security analysis tool.
- Manual audit of the codes for security issues. The source code is manually analyzed to look for any potential problems.
- Set up a testing environment to debug/analyze found issues and verifies our attack PoCs.

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 functioning; creates a critical risk to the application; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the application with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the application 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 2. Severity levels

1.4. Disclaimer

GPTVERSE acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. GPTVERSE understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, GPTVERSE agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the GPTVERSE will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the GPTVERSE, the final report will be considered fully accepted by the GPTVERSE without the signature.

2. AUDIT RESULT

2.1. Overview

The GPTVERSE Token Smart Contract was written in `Solidity` language, with the required version to be `^0.8.0`. The source code was written based on OpenZeppelin`s library.

The contract extends `ERC20Burnable` and `Ownable` contracts. With `Ownable`, by default, the contract owner is the contract deployer, but he can transfer ownership to another address at any time. `ERC20Burnable` allows token holders to destroy both their own tokens and those that they have an allowance for.

The smart contract is `ERC20` implementation that have some properties (as of the report writing time):

PROPERTY	VALUE
Name	Gptverse
Symbol	GPTV
Decimals	18
Total Supply	900,000,000 (x10^{18}) Note: the number of decimals is 18, so the total representation token will be 900,000,000 or 900 million.

Table 3. The GPTVERSE Token Smart Contract properties

For the `ERC20` token, the security audit team has the list of centralization issues below:

Checklist	Status	Passed
Upgradeable	No	Yes
Fee modifiable	No	Yes
Mintable	No	Yes
Burnable	No	Yes
Pausable	No	Yes

Checklist	Status	Passed
Trading cooldown	No	Yes
Has blacklist	No	Yes
Has whitelist	No	Yes

Table 4. The decentralization checklist

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of GPTVERSE Token Smart Contract.

2.3. Additional notes and recommendations

2.3.1. Unused Ownable contract INFORMATIVE

At the beginning of the source code, the contract imports the `Ownable` abstract contract, but it is not used within the contract.

RECOMMENDATION

We recommend removing it for readability.

APPENDIX

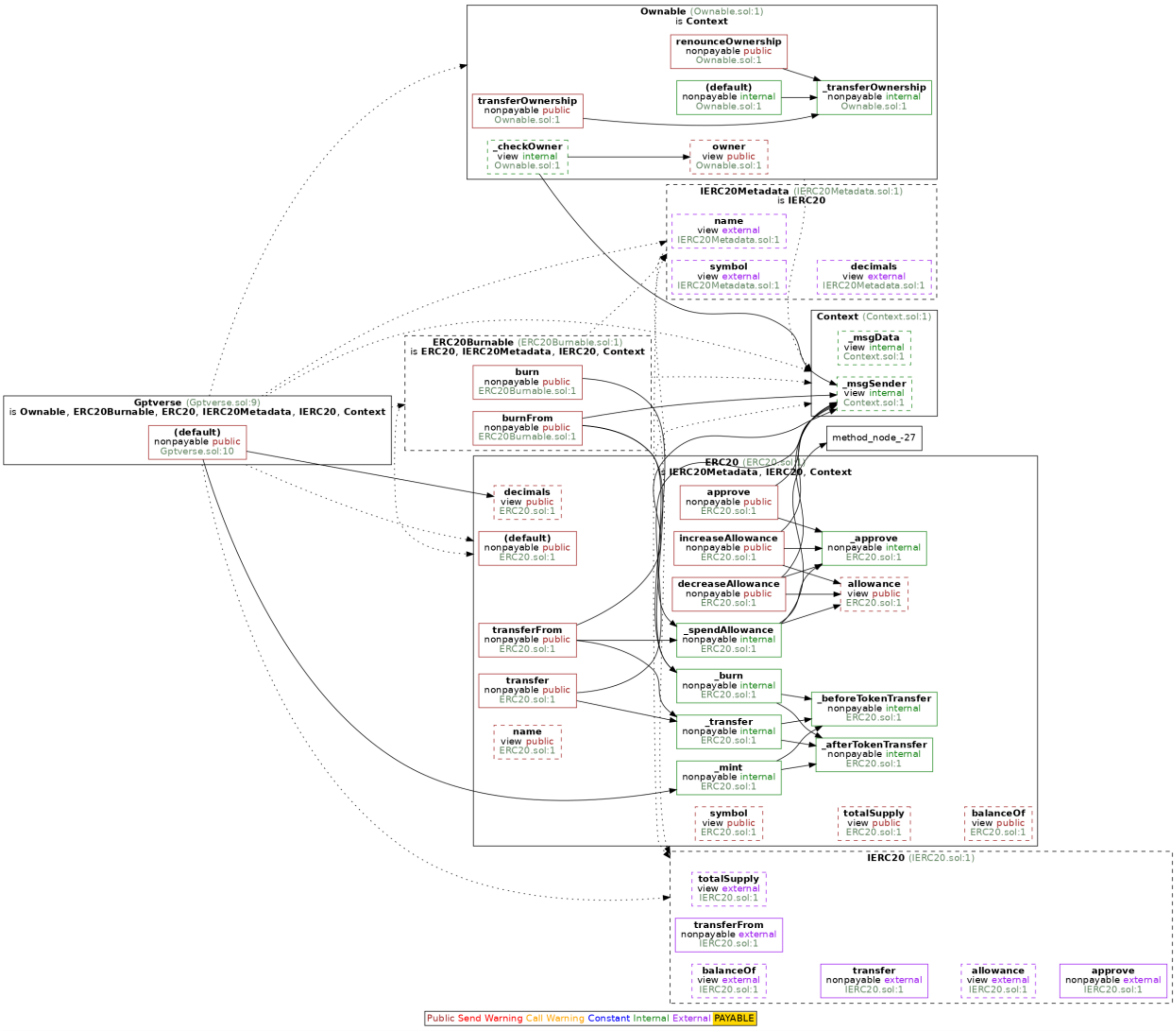

Image 1. GPTVERSE Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Jan 2, 2024*	Public Report	Verichains Lab
1.1	*Jan 5, 2024*	Public Report	Verichains Lab

Table 5. Report versions history