

VERIFIED CRYPTO

SMART CONTRACT AUDIT

The Monaverse

14/01/2022

Paris, France

verifiedcrypto.org



Table of Contents

Disclaimer	3
Overview	4
Summary	4
Audited Contracts	4
Vulnerability Summary	4
Findings	5
ID-1 TheMonaverseToken	6
ID-2 TheMonaverseToken	6
ID-3 TheMonaverse	6
ID-4 TheMonaverse	7

Disclaimer

Verified Crypto and its members, officers, directors, owners, employees, agents, representatives, suppliers and service providers provides this audit report for informational purposes only. Use of this report and access to the website www.verifiedcrypto.org (the "Site"), social accounts and the information, materials, services, and other content available in this report ("Content"), on or through the Site ("Content") are subject to these terms of use and all applicable laws. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. Further, this report may not be transmitted, disclosed, referred to or relied upon by any persons or parties on any objective, goal or justification without Verified Crypto prior written consent and approval.

The Content is for informational purposes only, you should not construe any such information or other material as legal, tax, investment, financial, or other advice. Nothing contained in this report or on our Site constitutes a solicitation, recommendation, endorsement, or offer by Verified Crypto or any third party service provider to buy or sell any securities or other financial instruments in this or in any other jurisdiction in which such solicitation or offer would be unlawful under the securities laws of such jurisdiction.

Verified Crypto disclaims all responsibility and responsibilities and no claim against Verified Crypto is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic losses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Verified Crypto retains full rights over all intellectual property (including expertise and new attack or exploit vectors) discovered during the audit process. Verified Crypto is therefore allowed and expected to re-use this knowledge in subsequent audits and to inform existing projects that may have similar vulnerabilities. Verified Crypto may, at its discretion, claim bug bounties from third-parties while doing so.



Blockchain technology, cryptocurrencies and any technologies by extension directly or indirectly related to blockchain are highly volatile, speculative by nature and represent high level of risk. DYOR: Do Your Own Research.

Overview

Summary

Project name	The Monaverse
URL	themonaverse.com
Platform	BSC
Language	Solidity

Audited Contracts

Name	Address	Live code match
TheMonaverse	Unavailable	
TheMonaverseToken	Unavailable	

Codebase	Commit
Github link	bed74ef96d44cef679d0c81289de41f766c7863b

Vulnerability Summary

Severity	Detected	Resolved	Acknowledged	Declined
 Critical	1	-	-	1
 Medium	-	-	-	-
 Low	-	-	-	-
 Informational	3	-	3	-

Findings

ID	Description	Severity	Status
1	onlyOwner modifier is corrupted	 Critical	Declined
2	Different Solidity versions across the contract	 Informational	Acknowledged
3	claimAllRedeemFee() optimisation	 Informational	Acknowledged
4	Different Solidity versions across the contract	 Informational	Acknowledged

ID-1 | TheMonaverseToken

Severity	Critical ●
Description	onlyOwner modifier is corrupted. The owner is able to control the contract even after the ownership revocation
Recommendation	<p>Use this modifier:</p> <pre>modifier onlyOwner() { require(_owner == _msgSender(), "Ownable: caller is not the owner"); _; }</pre> <p>and remove this line from Ownable contract:</p> <pre>_previousOwner = msgSender;</pre>
Resolution	Declined. The Monaverse team is willing to deploy the contract with this centralisation privilege

ID-2 | TheMonaverseToken

Severity	Informational ●
Description	Different Solidity versions across the contract
Recommendation	Use the latest version of Solidity
Resolution	Acknowledged

ID-3 | TheMonaverse

Severity	Informational ●
Description	claimAllRedeemFee() does not follow the check-effect-interaction standard.
Recommendation	Update the feeAmount and then call safeTransfer
Resolution	Acknowledged

ID-4 | TheMonaverse

Severity	Informational ●
Description	Different Solidity versions across the contract
Recommendation	Use the latest version of Solidity
Resolution	Acknowledged



VERIFIED CRYPTO
AUDIT
KYC
PENTEST

verifiedcrypto.org