SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

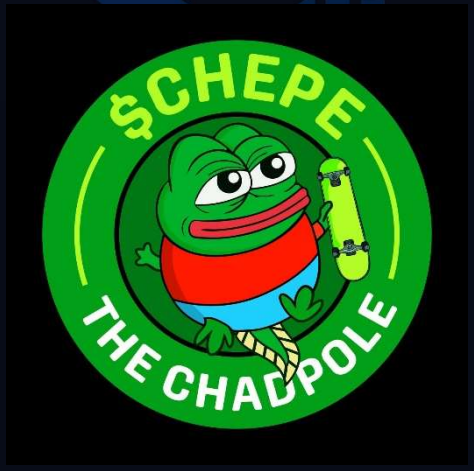
Chepe
The Chadpole

AUDIT

SECURITY ASSESSMENT

29. March, 2024

FOR



Content

Introduction

SolidProof.io is a brand of the officially registered company MAKE NetworkGmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should be considered, an "endorsement"or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any"product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (suchas Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors.
SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveragedas investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending tohelp our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Chepe the Chadpole
Website	https://www.chepechadpole.com
About the project	Pepe's delinquent teenage son looking to step out of his father's shadow.
Chain	Solana
Language	Rust
Codebase	https://solscan.io/token/8fGif1gx7Gq3QkmnWFBnNgEWhKQTd9bdNnv9FE5pPTGw
Commit	N/A
Unit Tests	Not Provided

Social Medias

Telegram	https://t.me/ChepeLiquidityPondSecurity
Twitter	https://twitter.com/ChepeChadpole
Facebook	N/A
Instagram	N/A
GitHub	N/A
Reddit	N/A
Medium	N/A
Discord	N/A
YouTube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Change Log
v1.0	29. March 2024	• Layout Project • Automated/Manual Functionality Review • Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract's logic. We cannot guarantee 100% logical correctness of the contract as it was not functionally tested by us.

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with a SHA-1 Hash.

1. n/a

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash valuemay (but need not) be an indication of a changed state or potential vulnerability thatwas not the subject of this scan.

Imported packages

Used code from other Frameworks.

1. n/a

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt thecontract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action toreduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in anunintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executingthe contract in a specific scenario.	Implementation of corrective actions in acertain period.
Low	2 – 3.9	A vulnerability that does not havea significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine alevel of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security- related issues, code quality, and compliance with specificationsand best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. **Code review that includes the following:**
   a. **Reviewing the specifications, sources, and instructions providedto SolidProof to ensure we understand the size, scope, andfunctionality of the smart contract.**
   b. **Manual review of the code, i.e., reading the source code line byline to identify potential vulnerabilities.**
   c. **Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructionsprovided to SolidProof.**

2. **Testing and automated analysis that includes the following:**
   a. **Test coverage analysis, which determines whether test cases actually cover code and how much code is executed when thosetest cases are executed.**
   b. **Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.**

3. **Review best practices, i.e., review smart contracts to improve efficiency,effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.**

4. **Concrete, itemized and actionable recommendations to help yousecure your smart contracts.**

Overall Security

Upgradeablility

Contract is not an upgradeable	✅ **Deployer cannot update the contract with new functionalities**
Description	**The contract is not an upgradeable contract. Thedeployer is not able to change or add any functionalities to the contract after deploying.**
Comment	**N/A**

Ownership

The ownership is renounced	✅ The owner is renounced
Description	The owner renounced the ownership that means the contract's owner will no longer have any controlor authority over the contract's operations.
Comment	N/A

Note - If the contract is not deployed then we would consider the ownership to be not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced.

Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refers to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or adesignated authority, who has the ability to add new tokens to the network's totalsupply.

Contract owner cannot mint new tokens	✅ Renounced mintAuthority
Description	The owner is not able to mint new tokens once thecontract is deployed.
Comment	N/A

Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens,reducing the total supply of a cryptocurrency or token. This is usually done to increasethe value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens	✅ The owner cannot burn tokens
Description	The owner is not able burn tokens without anyallowances.
Comment	N/A

Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses	✅ **The owner cannot blacklist addresses**
Description	**The owner is not able blacklist addresses to lock funds.**
Comment	**N/A**

Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%	✅ **The owner cannot set Fees or taxes**
Description	**The owner is not able to set the fees above 25%**
Comment	**N/A**

Lock User Funds

In a smart contract, locking refers to the process of restricting access tocertain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or useduntil the lock-up period has expired or certain conditions have been met.

Owner cannot lock the contract	✅ **Renounced freezeAuthority**
Description	**The owner is not able to freeze the token.**
Comment	**N/A**

Audit Results

Critical Issues

No critical issues

High Issues

No high issues

Medium Issues

No medium issues

Low Issues

No low issues

Informational Issues

#1 | Token metadata are saved

File	Severity	Location	Status
Continental	Informational	--	Open

Description

Token metadata are saved on “https://ipfs.nftstorage.link/” storage for an indefinite period. We recommend using the Arweave blockchain for indefinite storage (as the most popular tokens on the Solana blockchain use this service, which ensures uninterrupted operation)

Legend For the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY