



•• AI-Powered
Smart-Contracts Auditor
By ChainGPT AI

Smart Contract Audit Report

Chain GPT

AUDIT ID : 52f0f09e-1827-4020-aba5-6d39...
GPT VERSION : ^0.8.0
DATE : 2025-08-20T14:43:15.967629



DISCLAIMER :

This report was auto-generated by ChainGPT's beta Smart-Contract Auditor; no human has reviewed it. It is provided "as-is," with zero warranties—including accuracy, completeness, merchantability, or fitness for purpose. The tool can miss critical bugs or fraud and does not certify project legitimacy. Use it only for an initial look and obtain an independent professional audit (e.g., CertiK, OpenZeppelin) before any production deployment. You bear all risk; ChainGPT and its contributors accept no liability for losses of any kind arising from use of this report or the underlying code.

CHAIN GPT

Welcome 1

Table of Contents 2-5

Smart Contract Audit Overview 6

Audit Score & Severity Summary 7

Findings Summary 8-13

Detailed Findings 14-63

FND-File 1, Line 500: ERC20._spendAllowance(address owner, address spender, uint256 amount) 14

FND-File 1, Line 654: ERC20Burnable.burnFrom(address,uint256) 15

FND-File 1, Line 268: ERC20.approve(address spender, uint256 amount) 16

FND-File 1, Line 658: ChainGPT constructor _mint(msg.sender, 1e9 * 10 ** decimals()) 17

FND-File 1, Line 560: ERC20Burnable.burnFrom and ERC20.decreaseAllowance 18

FND-File 1, Line 639: ERC20Burnable.burn(uint256) 19

FND-File 1, Line 364: ERC20.approve(address,uint256) and ERC20Burnable.burnFrom(address,uint256) 20

FND-File 1, Line 340: transfer() / _transfer() 21

FND-File 1, Line 652: contract ChainGPT (no token rescue/sweep function) 22

FND-File 1, Line 652: contract ChainGPT (no receive()/withdraw functions) 23

FND-File 1, Line 76: Ownable.transferOwnership(address newOwner) 24

FND-File 1, Line 548: ERC20Burnable.burn(uint256 amount) and ERC20.transferFrom(...) 25

CHAIN GPT

CONTRACT NAME & SYMBOL

Chain GPT - (CGPT)

CONTRACT ADDRESS & NETWORK

Ethereum

COMPILER VERSION

^0.8.0

PRAGMA SOLIDITY VERSION

Version: ^0.8.0

DETECTED STANDARDS

ERC-20

SOURCE CODE

2542ec95504f7c19081d...

Contract Purpose

This contract implements a standard ERC20 token named ChainGPT (symbol: CGPT) using OpenZeppelin libraries, with 18 decimals and a fixed supply of 1,000,000,000 tokens minted once to the deployer at deployment. It includes burn functionality, allowing holders or approved spenders to destroy tokens, and basic ownership controls (transfer/renounce ownership) for administration. Beyond these, it has no special mechanics—no fees, pausing, blacklisting, or post-deployment minting—making it a straightforward, burnable fixed-supply ERC20.

CHAIN GPT

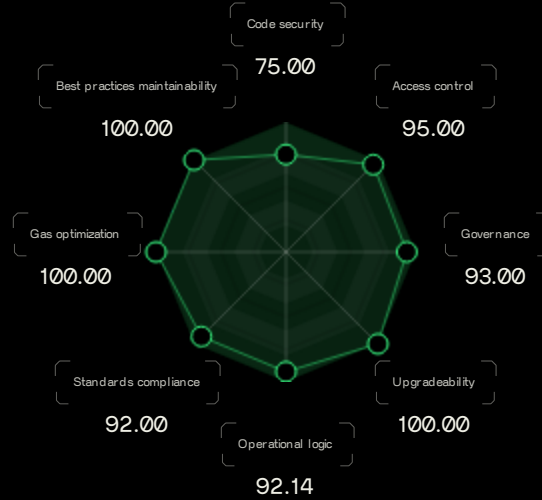
Security Score

Final Audit Score

88.2%

Breakdown

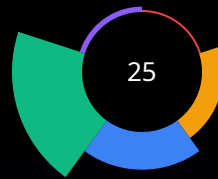
The audit assessed the contract across multiple dimensions, including code integrity, community trust, market activity, and governance structure. The findings indicate a well-structured codebase with minor areas for improvement in operational robustness.



Severity of findings

The contract exhibited moderate issues primarily in gas optimization and edge-case handling. No critical vulnerabilities were identified.

- Critical 0
- High 4
- Medium 7
- Low 13
- Info 1



FINDINGS SUMMARY TABLE

ID	Title	Severity	Category	Location	Page
1	Infinite allowances enable unlimited token destruction by the approved spender	High	General	contracts/ERC20_spe...	File 1, Line 500
2	Approved spenders can irreversibly burn holder tokens via burnFrom, enabling malicious dApps to deflate supply through allowances	High	General	contracts/ERC20Burn...	File 1, Line 654
3	Infinite allowances enable unlimited token destruction by the approved spender	High	General	contracts/ERC20_spe...	File 1, Line 500
4	Approved spenders can irreversibly burn holder tokens via burnFrom, enabling malicious dApps to deflate supply through allowances	High	General	contracts/ERC20Burn...	File 1, Line 654

FND-FILE 1, LINE 340: TRANSFER() / _TRANSFER()

Severity: ● MEDIUM
Category: operational_logic
Code Location: `TOKEN.SOL` `TRANSFER()` / `_TRANSFER()` , line File 1, Line 340

Description

The token uses a standard ERC20 implementation without Pausable. There is no way to halt transfers, burns, or other operations in case of an emergency or exploit. This prevents the project from halting token operations in response to emergencies.

Impact

Inability to stop malicious or erroneous token movements during incidents can exacerbate losses. Inability to stop token operations can exacerbate the impact of exploits or misconfigurations.








Remediation

Integrate OpenZeppelin Pausable and guard transfer-related functions with whenNotPaused. Inherit Pausable and guard sensitive functions with whenNotPaused; restrict pause control to a secure multisig.

STANDARD COMPLIANCE CHECKLIST

Standard	Status	Notes
ERC_20	● PASS	Fully compliant
ERC_173	● PASS	Fully compliant

FORMAL VERIFICATION

Assertion Tested	Result	Notes
Arithmetic Safety	 PASS	No Mythril vulnerabilities detected
Balance Consistency	 PASS	No Mythril vulnerabilities detected
Access Control	 PASS	No Mythril vulnerabilities detected
Reentrancy Safety	 PASS	No Mythril vulnerabilities detected
Asset Safety	 PASS	No Mythril vulnerabilities detected
Invariant Preservation	 PASS	No Mythril vulnerabilities detected
Call Integrity	 PASS	No Mythril vulnerabilities detected

NARRATIVE SUMMARY

Audit score: **88.2 / 100**

What this contract does?

Our review of Chain GPT (CGPT) assessed a straightforward, OpenZeppelin-based ERC20 with 18 decimals, a fixed 1,000,000,000 token supply minted entirely to the deployer, standard ownership controls, and burn functionality (self-burn and burnFrom). No fees, pausing, blacklisting, or post-deployment minting are present. Across 26 findings, the final security...

High-risk findings

- ⦿ Infinite allowances enable unlimited token destruction by the approved spender
- ⦿ Approved spenders can irreversibly burn holder tokens via burnFrom, enabling malicious dApps to deflate supply through allowances
- ⦿ Infinite allowances enable unlimited token destruction by the approved spender
- ⦿ Approved spenders can irreversibly burn holder tokens via burnFrom, enabling malicious dApps to deflate supply through allowances

Overall Recommendation

- ✓ ACCEPTABLE: Minor issues detected
- 🔧 Consider addressing low severity issues
- 🛠️ Implement improvements for better security

DISCLAIMER | CHAINGPT AI AUDITING TOOLE

This audit report ("Report") was automatically generated by the ChainGPT AI Smart Contract Auditing Tool ("Auditing Tool") and is provided subject to the terms and conditions outlined herein. The Auditing Tool operates using advanced artificial intelligence and automated analysis methods, without manual human review. It is provided on an "as-is," "where-is," and "as-available" basis, without any express or implied warranties regarding accuracy, completeness, correctness, merchantability, fitness for a particular purpose, or otherwise.

This Report is intended solely as an initial analysis of smart contract code to identify potential security vulnerabilities, logical errors, compliance issues, optimization opportunities, and general coding concerns. It does not represent a formal security audit, nor does it provide any form of assurance, certification, or endorsement regarding project legitimacy, team credibility, economic viability, asset value, regulatory compliance, or the underlying business model.

The Auditing Tool and this Report may contain errors, omissions, false positives, false negatives, or other inaccuracies. The technology underlying the Auditing Tool is subject to continuous development and improvements, and results are inherently probabilistic, uncertain, and subject to technical limitations.

Blockchain and smart contract technologies carry inherent risks and vulnerabilities, including but not limited to technical bugs, security flaws, malicious attacks, exploits, logic errors, operational risks, compliance risks, and regulatory uncertainties. ChainGPT explicitly disclaims all liability and responsibility for any losses, damages, or claims arising directly or indirectly from reliance upon, or the use or misuse of, this Report and the Auditing Tool.

This Report is not, and should not be considered, financial, investment, legal, tax, regulatory, technical, or professional advice of any kind. ChainGPT does not warrant or guarantee that the audited code or project will be secure, error-free, or free from vulnerabilities. You are strongly advised to conduct your own comprehensive due diligence, engage qualified professional auditors for thorough manual security reviews (such as CertiK, OpenZeppelin, or other reputable firms), and perform continuous security monitoring and maintenance of all smart contracts and related systems.

To the maximum extent permitted by applicable law, ChainGPT and its affiliates, subsidiaries, directors, employees, contractors, and agents expressly disclaim all warranties, liabilities, and responsibilities (express or implied) arising out of or related to the Auditing Tool, this Report, the audited code, or any associated services, including but not limited to implied warranties of merchantability, fitness for a particular purpose, non-infringement, security, reliability, availability, accuracy, completeness, compatibility, or performance.

DISCLAIMER | CHAINGPT AI AUDITING TOOLE

You acknowledge and agree that any use, reliance upon, or decisions made based on this Report and/or the Auditing Tool are solely at your own risk. ChainGPT, its affiliates, subsidiaries, directors, employees, contractors, or agents will not be liable to you or any third party for any direct, indirect, incidental, special, punitive, consequential, or exemplary damages arising out of or in connection with your use of, reliance upon, or inability to use or rely upon, this Report, including but not limited to losses resulting from bugs, vulnerabilities, hacks, exploits, errors, interruptions, inaccuracies, omissions, defects, harmful code, or loss of profits or revenues.

This Report and any associated materials provided by ChainGPT are intended solely for the named Customer's internal review and use, and may not be disclosed, transmitted, distributed, relied upon, or otherwise provided to any third party without ChainGPT's explicit prior written consent.

By accessing, reviewing, or otherwise using this Report, you accept and agree to all of the terms, conditions, and limitations set forth in this Disclaimer. ChainGPT reserves the right, in its sole discretion, to modify, update, or revise these terms at any time without prior notice.