



# **SOLIDITY AUDIT**

# **CRYPTOGEM TRADING**



# Contents

**Project Information**

**Scope of Audit**

**Check Vulnerabilities**

**Issue Categories**

**Security issues per severity**

**Transaction code**

**Compiler Testing**

**Testing Contract**

**Result**

**Closing Summary**

# Project Information

**Project Name: CRYPTO GEM TRADING**

**Network: BSC (BINANCE SMART CHAIN)**

**Contract Address:**

**0xF8105B03deD1D6aeB5b46ebB4416F960f12e3644**

**Type: INVESTMENT**

**Max amount: N/A**

**Min amount: 50 USDT**

**Dev fee: 1%**

**Owner fee: 0%**

**Marketing: 0%**

**Withdraw system:**

**Once a day**

**Minimum Withdrawal: 50 USDT**

**Referral: 7%, 3%, 1%**

**Withdraw referral: Automatic**

**Max Referral: Unlimited**

**Reward system: Daily 2%**

**Bonus Reward: CGT Token**

# Token Information

**Token Name: CRYPTO GEM TRADING TOKEN**

**Network: BSC (BINANCE SMART CHAIN)**

**Contract Address:**

**0xF8105B03deD1D6aeB5b46ebB4416F960f12e3644**

**Supplies: 1,000,000,000**

**Decimal: 18**

**Token: ERC20**

**Use case: ROI rewards.**

**Total burn: 0%**

**Token sell rate: 1,000 = 1 USDT**

**Owner address:**

**0xe3aef9e4cacf5d37f8116961c67a963b6d7bd9cd**

**Dev address:**

**0xe3aef9e4cacf5d37f8116961c67a963b6d7bd9cd**

**Dev address: can be change**

**Renounce Owner: NO**



# Scope of Audit

**The scope of this audit was to analyze and document the Cryptogemtrading smart contract codebase for quality, security, and correctness. Any error or incorrect will fixed by our team.**

## Check Vulnerabilities

**We scanned and check those commonly known and specific vulnerabilities base on the solidity code of the project. Here are some of the commonly known vulnerabilities that we considered.**

- **Compiler**
- **Struct**
- **Plan**
- **Functions**
- **Users Checkpoint**
- **Timestamp**
- **Gas Limit and Loops**
- **Byte array**
- **Backdoor**
- **Transfer forward**
- **Redundant fallback**



## Issue Categories

**Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.**

<b>Risk-level</b>	<b>Description</b>
<b>High</b>	A high severity issue or vulnerability means that your smart contract can be exploited. Issue on this level is critical to the smart contract's performance of functionality and we recommended these issues be fixed before moving to the public.
<b>Medium</b>	The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on his level could potentially bring problems, and they should still be fixed.
<b>Low</b>	Low level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.
<b>Informational</b>	These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information there is a lot-to-no-impact.



## Number of issues per severity

Type	High	Medium	Low	Informational
Open	0	1	0	0
Acknowledge	0	0	2	1
Closed	0	0	2	1

## Transaction Code

### 1. Cryptogemtrade (ROI)

1. Invest function
2. Payout function

Other function is for public viewing which allowing the people to view such as allowance, balanceOf, getBalance, getOwner, invested, isDaily, isScheduled, memberDeposit, memberDownline, nextwithdraw...



## **2. Cryptogentrade (CGT) token**

- 1. Approve**
- 2. Burn**
- 3. decreaseAllowance**
- 4. increaseAllowance**
- 5. renounceOwnership**
- 6. setDays**
- 7. setDev**
- 8. setScheduled**
- 9. transfer**
- 10. transferFrom**
- 11. transferOwnership**
- 12. sellTokens**

**All function in highlighted with white is normal and common function of ERC20 tokens.**

**Function sellTokens is highlighted with blue color severity issue **Medium** token can be sold in the contract.**

**Function sellTokens is public function that people can sold their token in the contract.**





## Compiler Test

**Compiled and tested under 3<sup>rd</sup> party solidity compiler.**

0.8.9+commit.e5eed63a	SUCCESS
No Warning Detected	SUCCESS
Compiled Success	SUCCESS

## Contract Testing

**Contract deployed and tested with our team before we released the audited report.**

## Result

**1 minor issue was found, some false positive errors were reported by the tool. All the other issues have been categorized according to their level of severity, team improved and fixed it before the publicity of the project.**

## Closing Summary

**Overall, smart contract is very well written and adhered to guidelines. Minor issues were discovered during the audit.**

