

# CRYPTO GPT (CRGPT)

## Token Creation & Security Analysis Report

<b>Blockchain:</b>	Ethereum (ERC-20)
<b>Token Symbol:</b>	CRGPT
<b>Total Supply:</b>	21,000,000 (Fixed)
<b>Deployment Date:</b>	14 November 2023
<b>Contract Address:</b>	0x50739bd5b6aff093ba2371365727c48a420a060d
<b>Contract Owner:</b>	0x0000...000000 (Renounced)

## Executive Synopsis

This document provides a factual explanation of how the CRYPTO GPT (CRGPT) token was created, how it operates, and why a reported token loss by a holder is not related to the token's smart contract or its creators. All statements are supported by public, independently verifiable on-chain data and third-party security platforms.

**Key Findings:** The CRGPT token was created ethically through a transparent fair launch process. The smart contract is immutable with renounced ownership. All risks are technical and disclosed, not deceptive. The creators cannot manipulate users, supply, or trading.

## 1. Token Creation & Fair Launch

CRGPT was created on 14 November 2023 using PinkSale, a reputable third-party Ethereum launchpad, through a **fair launch** process.

### What is a Fair Launch?

- Public participation available to all
- Transparent launch process via established platform
- Automatic Uniswap listing after launch
- Liquidity locking via PinkLock

#### PinkSale Launch Page (Public Record):

<https://www.pinksale.finance/launchpad/ethereum/0x354015D55249D9970eB65c039FE407A98Cb387e7>

## 2. Smart Contract & Ownership

The CRGPT smart contract is fully decentralized at the contract level. Contract ownership has been permanently set to the null address (0x000...000), meaning it has been **renounced**.

### This means:

- No admin control exists
- No proxy contract (cannot be upgraded)
- No hidden owner address
- Contract rules are permanently fixed
- Nobody, including creators, can change the rules

### 3. Supply Integrity

The contract enforces hard limits on token supply, removing classic scam vectors:

Security Check	Status	Implication
Mint Function	■ None	Cannot create new tokens
Adjustable Max Supply	■ None	Supply permanently fixed
Hidden Minting	■ None	No secret token creation
Owner Balance Control	■ None	Cannot modify balances
Self-Destruct Function	■ None	Contract cannot be destroyed

### 4. Trading & Transfer Rules

CRGPT is a plain ERC-20 token with no restrictive mechanisms:

Parameter	Value
Buy Tax	0%
Sell Tax	0%
Transfer Tax	0%
Blacklist Function	None
Whitelist Function	None
Trading Suspension	Not Possible
Cooldown Traps	None
Honeypot Behavior	Not Detected

**Conclusion: Tokens can always be transferred and sold. No honeypot behavior detected.**

## 5. Liquidity & Locking

### Current Liquidity Status:

- Current liquidity: ~\$47,000 on Uniswap (WETH/CRGPT)
- Liquidity is **100% locked**
- Liquidity provider tokens are locked via PinkLock
- Locked liquidity is NOT withdrawable by the team

### Why PinkLock Was Used:

PinkLock is a third-party liquidity locking service commonly used to prevent rug pulls, prove long-term commitment, and make liquidity non-withdrawable. This is a **protective mechanism**, not a risk.

### Known Risk (Transparent & Declared):

Security scanners flag **low liquidity** as a medium-risk item. Low liquidity results in higher volatility. Low volume indicates limited current market interest. These are **market conditions**, not design flaws or fraud indicators.

## 6. Holder Distribution

Category	Percentage	Explanation
Burn Address	~35%	Permanently removed from circulation
Locked Tokens (Vesting)	~43%	Held in time-locked contracts
Circulating & Unlocked	~21%	Available for trading
Owner Holdings	0%	Creators hold no special allocation
Creator Holdings	~0%	Creators cannot dump tokens

## 7. Independent Security Verification

Two independent security platforms have analyzed the CRGPT contract:

### De.Fi Scanner Report:

<https://de.fi/scanner/contract/0x50739bd5b6aff093ba2371365727c48a420a060d?chainId=eth>

### GoPlus Labs Token Security Report:

<https://gopluslabs.io/token-security/1/0x50739bd5b6aff093ba2371365727c48a420a060d>

### Security Scores:

Platform	Score
De.Fi Safety Score	93/100
De.Fi AI Score	69/100
De.Fi Overall Score	79%
GoPlus Risky Items	0

GoPlus Attention Items	1 (Low Liquidity)
------------------------	-------------------

## 8. Airdrop Scam Incident — Critical Clarification

A reported token loss by a holder was caused by a **third-party phishing/fake airdrop scam** at the wallet level. This section explains why this incident is unrelated to the CRGPT contract.

### Did CRGPT Create an Airdrop?

**No.** The CRGPT contract does NOT contain:

- Any airdrop functionality
- Any claim logic
- Any reward distributor
- Any external call hooks
- Any approval-based drain logic

Independent scanners explicitly confirm: **"No airdrop-specific code found"**

### Can the CRGPT Team Create an Airdrop?

**No.** Because ownership is renounced, the contract is immutable, and no admin functions exist.

### How Did the Holder Lose Tokens?

This is a classic **wallet-level scam**, not a token-level issue:

1. A scammer creates a fake website or fake token
2. Labels it something like "CRGPT Airdrop" or "CRYPTO GPT Rewards"
3. User is asked to "Claim," "Verify," or "Approve"
4. User signs a malicious wallet approval
5. Attacker uses that approval to transfer tokens from the wallet

**Important:** The CRGPT smart contract is NOT involved in this process. No tokens are minted, moved, or controlled by the CRGPT contract in such scams.

### Can Anyone Create a Fake Airdrop?

**Yes. Anyone. For any token.** ERC-20 tokens are permissionless. Scammers do NOT need contract access, team approval, or ownership rights. They only need a fake frontend and a malicious approval request. This is the same attack used against major projects including Uniswap, MetaMask, Arbitrum, Optimism, ENS, and many others.

### Legal Distinction:

This incident qualifies as:

- ■ NOT a token exploit
- ■ NOT a contract vulnerability
- ■ NOT creator negligence
- ■ User-level wallet compromise via third-party phishing

This is equivalent to clicking a fake 'bank login' email and entering credentials. The bank's systems are not compromised; the user was deceived externally.

## 9. What This Token Is NOT

For complete clarity, CRGPT is NOT:

- A guaranteed investment
- A yield-promising scheme
- A custodial product
- A hidden-fee token
- A contract with admin backdoors

It is simply: **A fixed-supply ERC-20 token with locked liquidity and no owner control.**

## 10. Conclusion

Based on independent security audits and publicly verifiable on-chain data:

Finding	Evidence
Token created ethically	Fair launch via PinkSale, public participation
Rules are immutable	Ownership renounced to null address
Risks are transparent	Low liquidity disclosed by scanners
Risks are NOT deceptive	No hidden mechanisms or admin functions
Creators cannot manipulate	No mint, blacklist, or balance control
Airdrop scam is external	No airdrop code in contract

---

**Final Statement: CRGPT is a standard ERC-20 token with transparent creation, immutable rules, locked liquidity, no central control, and no hidden mechanisms. The token's structure follows best practices for ethical deployment. No evidence exists of malicious intent, contract exploitation, or creator misconduct.**

## Supporting References (All Publicly Accessible)

### PinkSale Launch Page:

<https://www.pinksale.finance/launchpad/ethereum/0x354015D55249D9970eB65c039FE407A98Cb387e7>

### De.Fi Security Scanner:

<https://de.fi/scanner/contract/0x50739bd5b6aff093ba2371365727c48a420a060d?chainId=eth>

### GoPlus Labs Token Security:

<https://gopluslabs.io/token-security/1/0x50739bd5b6aff093ba2371365727c48a420a060d>

### Ethereum Contract (Etherscan):

<https://etherscan.io/token/0x50739bd5b6aff093ba2371365727c48a420a060d>