Smart Contract Audit Report

Auditor: 0xGutzzz
Date: 13-03-2025
Project Name: [Crestal Network Contracts]
Scope: [Payment.sol]

Table of Contents

Introduction

A society of self-employed AI agents

Executive Summary

- **Overall Risk Level:** [Low / Medium / High]
- **Total Findings:**
  - High: 1
  - Medium: 0
  - Low: 0
  - Informational: 0

Audit Scope

- Files reviewed:

```
- Payment.sol
```

- Focus areas: Security vulnerabilities, gas optimizations, code quality.

Methodology

- Manual review
- Testing coverage

Findings Summary

ID	Severity	Title	Status
F-01	High	Lack Of Authorization	Resolved

Detailed Findings

Finding F-01: [Lack of Authorization in the Function `Payment.sol::payWithERC20` Can Lead to Unauthorized Token Transfers]

- **Severity:** High

- **Status:** Resolved

- **Description:** A lack of authorization in the function Payment.sol::payWithERC20 can lead to unauthorized token transfers from a user as an attacker can initiate token transfers from approved addresses to their own addresses.

```
   function payWithERC20(address erc20TokenAddress, uint256 amount, address fromAdd
     // check from and to address
    require(fromAddress != toAddress, "Cannot transfer to self address");
     require(toAddress != address(0), "Invalid to address");
     require(amount > 0, "Amount must be greater than 0");
     IERC20 token = IERC20(erc20TokenAddress);
     token.safeTransferFrom(fromAddress, toAddress, amount);
 }
```

Recommendations

Mitigation Add authorization checks

```
      //@audit --> The require statement below checks if the caller is the same as the
         require(msg.sender == fromAddress, "Invalid from address");
```