

HOMEWORK 7

Part 1 - Analyze [DogCoinGame contract](#)

Using Static Analysis Plugin in Remix

1. Gas requirement of function DogCoinGame.payout is infinite.
Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
2. Gas requirement of function DogCoinGame.payWinners is infinite.
Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
3. For loop over dynamic array: Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas

Using Solidity Metrics in VSCode

Part 2

How would you classify the following points from an audit ?

1. Contract Size Exceeds 24576 Bytes.

CRITICAL

2. Strings in require statements can be shortened to reduce gas.

INFORMATIONAL

3. The initialise function in an upgradable contract has no access control, and can be called multiple times.

MAJOR

4. The README file is out of date and does not reflect the functionality of the system.

INFORMATIONAL

5. The ERC20 approval race vulnerability described here.

MAJOR