**Scam Detection Logic Documentation**

**Overview**

The Crypto Scam Address Detector is a tool that identifies potentially fraudulent cryptocurrency wallet addresses (Bitcoin and Ethereum). It operates by combining a public blacklist of known scams with blockchain behaviour analysis to flag suspicious activity.

**Address Type Detection**

Before performing scam checks, the system first verifies whether an address is valid and classifies it as either a Bitcoin or Ethereum address using regular expressions:

* **Bitcoin Address Pattern:**  
  ^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$  
  Description: Matches legacy Bitcoin addresses that start with 1 or 3 and are 26–35 characters long.
* **Ethereum Address Pattern:**  
  ^0x[a-fA-F0-9]{40}$  
  Description: Matches Ethereum addresses that start with 0x followed by 40 hexadecimal characters.

**Bitcoin Scam Detection**

**1. Reported Scam Check**

The system fetches a blacklist of reported Bitcoin scam addresses from the open-source GitHub repository:  
<https://github.com/mitchellkrogza/Badd-Boyz-Bitcoin-Scammers>

The input address is checked directly against this list to determine if it has already been reported as fraudulent.

**2. Blockchain Behavior Analysis**

API Used: https://blockchain.info/rawaddr/{address}  
The system analyzes the transaction history of the address to determine behavior consistent with known scams.

**Metrics Extracted:**

* **Total Inputs:** Number of transactions where the address received BTC.
* **Total Outputs:** Number of transactions where the address sent BTC.
* **Large Transactions:** Count of individual transaction outputs greater than 1 BTC.
* **High-Recipient Transactions:** Count of transactions with more than 10 recipients (i.e., outputs).

**3. Scam Behavior Criteria**

An address is flagged as suspicious if **either** of the following is true:

* More than 2 large transactions.
* More than 2 high-recipient transactions.

**Ethereum Scam Detection**

**1. Transaction History Retrieval**

API Used: https://api.etherscan.io/api  
Endpoint parameters:

* module=account
* action=txlist
* address={address}

This endpoint returns a complete list of transactions for the specified Ethereum address.

**2. Blockchain Behavior Analysis**

**Metrics Extracted:**

* **Total Inward Transfers:** Number of times ETH was received.
* **Total Outward Transfers:** Number of times ETH was sent.
* **Large Transactions:** Count of outgoing transfers greater than 1 ETH (in Wei: 1 × 10^18).

**3. Scam Behavior Criteria**

An address is flagged as suspicious if it has **more than 2 large outgoing ETH transactions**.

**Result Summary**

| **Feature** | **Bitcoin** | **Ethereum** |
| --- | --- | --- |
| Reported scam check | Yes (via public blacklist) | No |
| Blockchain data analyzed | Yes (via Blockchain.info) | Yes (via Etherscan API) |
| Large transaction threshold | Greater than 1 BTC | Greater than 1 ETH |
| High-output detection | Transactions with more than 10 outputs | Not applicable |
| Scam behavior flagging rule | >2 large or high-output transactions | >2 large outgoing transactions |