Wallet Risk Scoring: Methodology & Explanation

This document details the methodology used to build the wallet risk scoring model, from data collection to final analysis.

1. Data Collection Method

- **Source**: The transaction history for each wallet was fetched directly from the Ethereum blockchain using the **Etherscan API**.
- **Process**: A Python script was used to send programmatic requests to the account module of the Etherscan API. For each wallet, the txlist action was called to retrieve all normal transactions associated with the address.
- **Scalability**: To ensure compliance with the free API tier's limits (5 requests/second), a 0.2-second delay was implemented between each API call, making the process scalable and robust for larger datasets.

2. Feature Selection Rationale

The goal was to create features reflecting a wallet's age, activity level, network interaction, and potential exposure to high-risk DeFi activities.

- **wallet_age_days**: A measure of longevity. Older, more established wallets are often considered less likely to be associated with fleeting scams.
- **tx_count**: Represents the overall activity level of the wallet.
- **avg_eth_sent**: A proxy for the wallet's financial capacity and the scale of its operations.
- **unique_recipients**: Measures the breadth of the wallet's network. A very high number could indicate mixer-like activity or fund distribution from a hack.
- **mock_liquidations & mock_high_ltv_borrows**: These are crucial risk indicators specific to lending protocols. Since fetching real liquidation and loan-to-value (LTV) data is complex, these features were **mocked** to demonstrate the scoring logic. In a production system, they would be sourced from a service like The Graph and would strongly signal high-risk borrowing behavior.

3. Scoring Method

A weighted, normalized scoring model was implemented to generate a final risk score between 0 and 1000. The process is as follows:

1. **Feature Normalization**: All calculated features were first normalized to a common scale (0 to 1) using **Min-Max scaling**. This prevents features with naturally large values (like wallet age) from unfairly dominating the score.
2. **Weighted Sum**: Each normalized feature was multiplied by a predefined weight, reflecting its importance in assessing risk. For example, a liquidation event

(mock_liquidations) was assigned a very high weight (0.5), while wallet age had a negative weight (-0.1) to reduce risk.

3. **Scaling**: The resulting "raw score" was then scaled from its own range to the final 0-1000 range, providing a clear and easy-to-interpret final output.

4. Justification of Risk Indicators

The chosen indicators are justified as they represent common patterns of on-chain risk:

- **Age and Activity (wallet_age_days, tx_count)**: Legitimate users typically have older wallets with a consistent transaction history. Conversely, wallets created for a single, malicious purpose are often young with a sudden flurry of activity.
- **Financial Behavior (avg_eth_sent, unique_recipients)**: Unusual financial patterns, such as sending funds to an exceptionally large number of unique addresses, can be a red flag for illicit activities like airdrop scams.
- **Lending Protocol Risk (liquidations, high_ltv_borrows)**: These are direct measures of financial distress and high-leverage risk-taking within DeFi. A history of being liquidated is one of the strongest indicators that a wallet engages in high-risk strategies it cannot consistently manage