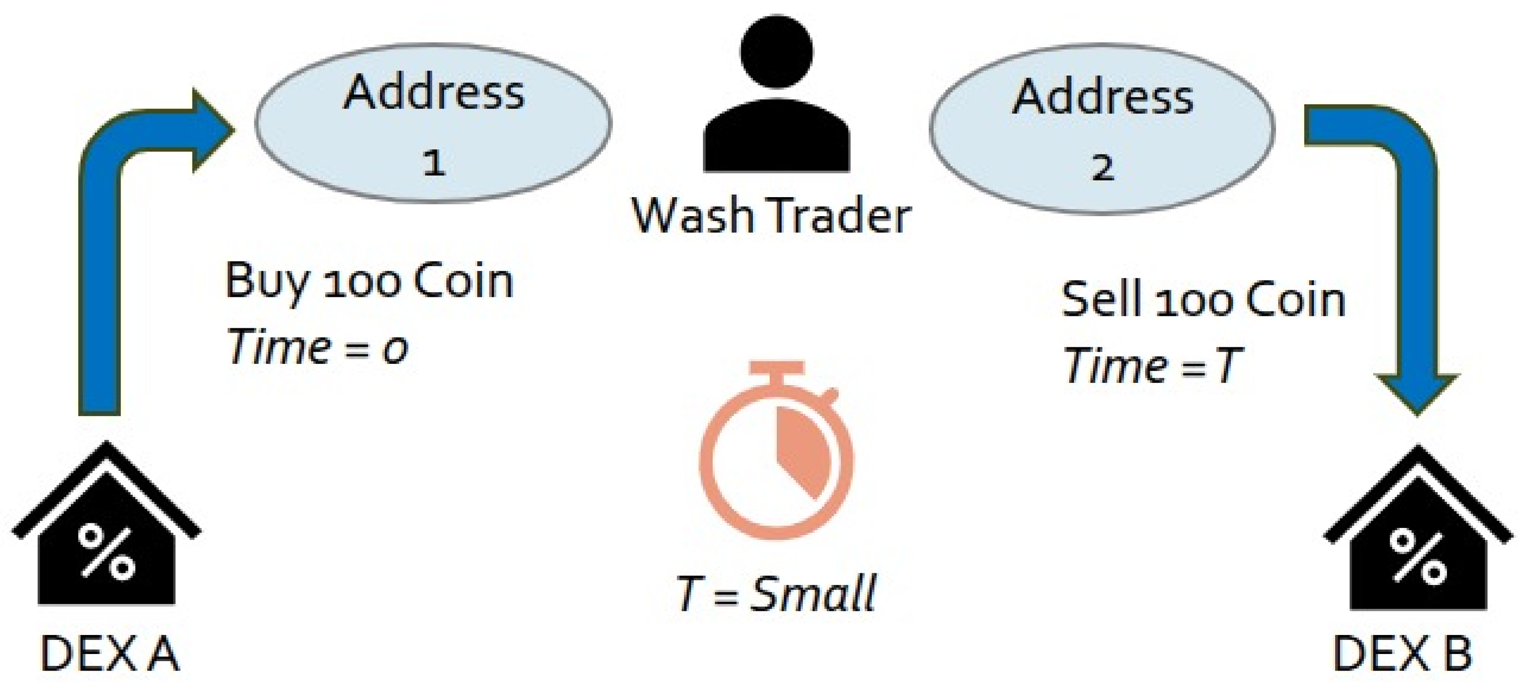
Wash Trading Detection and Quantification across Decentralized Exchanges (DEXs)

Sanidhay Arora [1] Yingjiu Li [1]

[1]Center for Cyber Security and Privacy

Introduction

Wash trading is a market manipulation tactic where a trader simultaneously buys and sells an asset to inflate trading volume without market risk or genuine economic intent.



- Wash trading inflates volume without real economic activity.
- DEXs pose new challenges: pseudonymity, no deposit addresses.
- Goal: Detect and quantify wash trading across DEXs using entity clustering and volume matching within small time windows.

Methodology

The key challenges are: (a) Pseudonymity of addresses, (b) Time window selection, and (c) lack of ground truth data.

The methodology comprises three main phases:

1. **Address Clustering**: Identify addresses controlled by the same entity using *novel* on-chain heuristics [1].
2. **Trade Graph Construction**: Model trades as a graph between entities, tracking volume, timestamps, and asset types.
3. **Detection and Quantification**: Apply volume-matching within small time windows to find trades with no net position change [2].

Data Source: Ethereum blockchain (2021 to 2024) using per-minute ERC-20 token and swap logs.

Expected Results

- Detection of coordinated clusters with repetitive trade patterns.
- Quantification of wash volume in millions (USD).
- Identification of DEX-to-DEX arbitrage-like loops.
- Insights into automation/bot behavior via timing and gas.

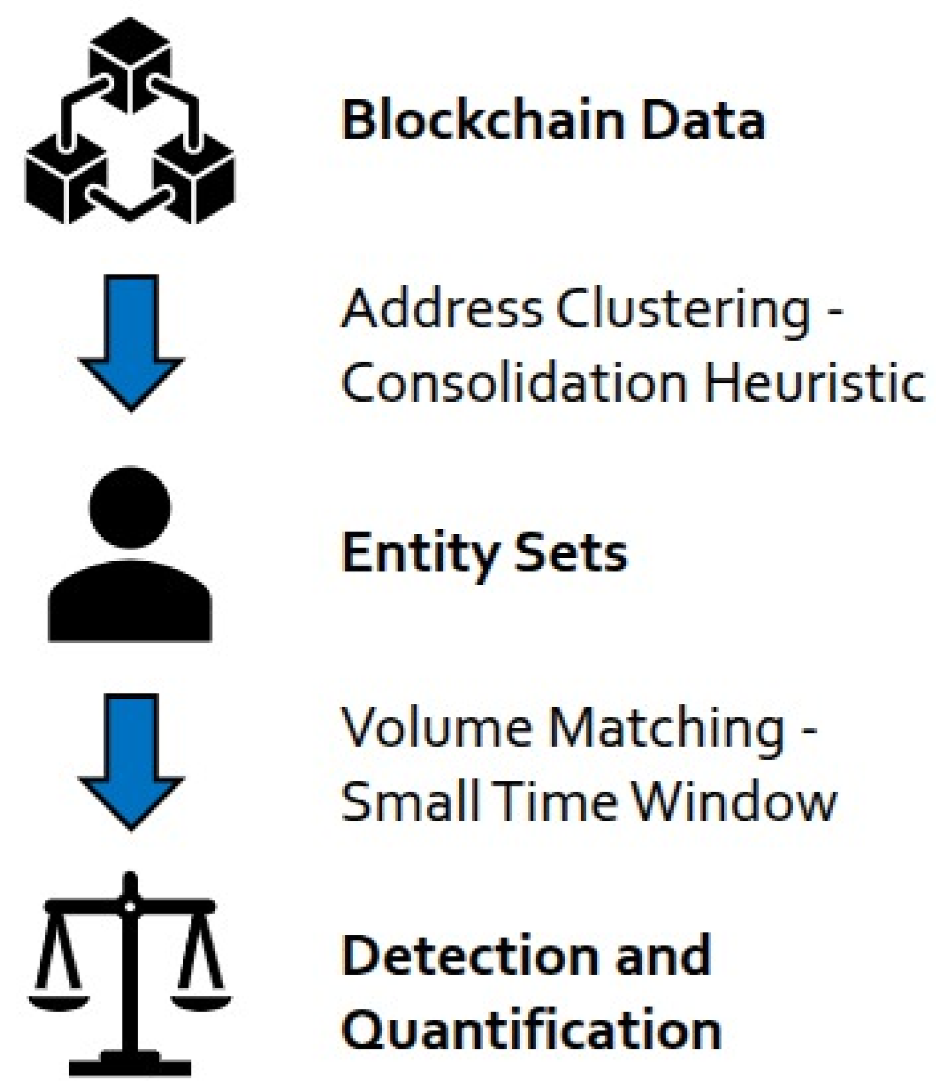
Detection and Quantification

The detection framework identifies wash trades by analyzing clustered entities for matched buy/sell behavior within short time windows.

Step 1: Address Clustering: Propose the Consolidation heuristic for address clustering. Build user and exchange entity maps: M_u, M_e.

Step 2: Suspicious Graph: Nodes = entity sets, edges = trades. Find Strongly Connected Components (SCCs) with frequent internal trading.

Step 3: Volume Matching: For each SCC U, compute buy/sell volume in $\mathcal{TW}$. If $|buy - sell| < \Delta$, label as wash trade.



Detection and Quantification Algorithm

Require: Trade set T, Entity map M_u, Volume threshold Δ, Time window $\mathcal{TW}$, Tokens $\mathcal{C}$
Ensure: Set of wash trades $\mathcal{W}$, Total wash volume V

```
Initialize W ← ∅, V ← 0
for all entity cluster U ∈ M_u do
    for all token c ∈ C do
        Compute buy ← Σ_{t∈T[U,TW,c]} incoming volume
        Compute sell ← Σ_{t∈T[U,TW,c]} outgoing volume
        if |buy − sell| < Δ then
            Mark trades in T[U,TW,c] as wash trade result τ
            W ← W ∪ {τ}
            V ← V + buy
        end if
    end for
end for
return W, V
```

Address Clustering

Challenge: Wallets on DEXs don't reuse identifiable deposit addresses.

- **Consolidation Heuristic:** $>= N$ addresses send swapped tokens to one address (A1) in time T.
- **Forwarding Ratio:** $R_f = A_{out}/A_{in}$, keep $R_{min} \leq R_f \leq R_{max}$.
- **Filter static holders**: temporary wallets used in wash loops.

Address Clustering Algorithm

Require: Trade Set Data T, Time window $\mathcal{TW}$, Sender threshold N, Forwarding ratio bounds $[R_{min}, R_{max}]$
Ensure: Set of consolidated address clusters $\mathcal{C}$

```
Initialize mapping R ← empty map of recipient → {senders}
Initialize C ← ∅
for all transfer (sender, receiver, amount, time) ∈ T do
    if sender = receiver then
        continue
    end if
    Add sender to R[receiver] if time within TW of previous senders
end for
for all receivers r with |R[r]| ≥ N_senders do
    Compute total inflow A_in to receiver
    Compute total outflow A_out from receiver within TW
    Compute R_f ← Amount_out/Amount_in
    if R_min ≤ R_f ≤ R_max then
        Add {r} ∪ R[r] to cluster set C
    end if
end for
return C
```

Discussion

- **Time Windows**: How to select low-volatility and small time windows to avoid false positives?
- **Thresholds:** How to calibrate N, R_f, Δ using historical data?
- **Obfuscation:** How to handle stealth addresses used to hide wash trade patterns?

References

[1] Friedhelm Victor.
Address clustering heuristics for ethereum.
In Joseph Bonneau and Nadia Heninger, editors, *Financial Cryptography and Data Security*, pages 617–633, Cham, 2020. Springer International Publishing.

[2] Friedhelm Victor and Andrea Marie Weintraud.
Detecting and quantifying wash trading on decentralized cryptocurrency exchanges.
CoRR, abs/2102.07001, 2021.

sanidhay@uoregon.edu