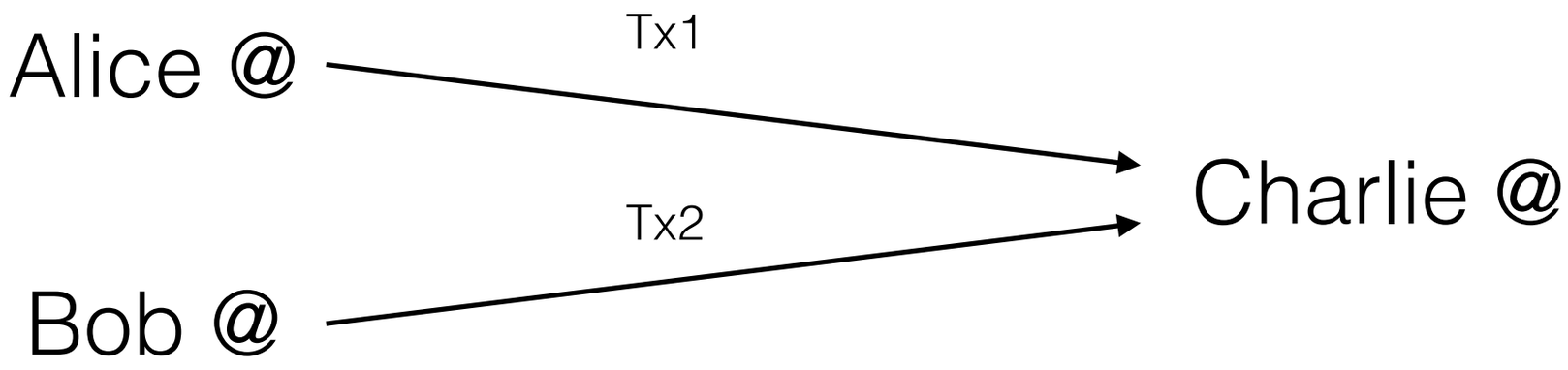
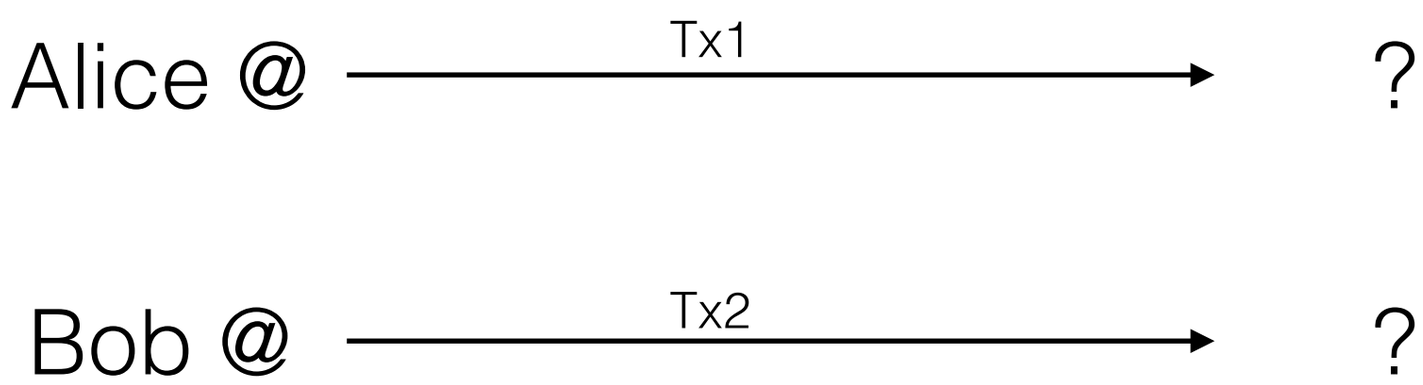
Blockchain Privacy
Privacy on the Transaction Layer

Linkability



Everybody sees the transactions go to the **same** recipient.

Unlinkability

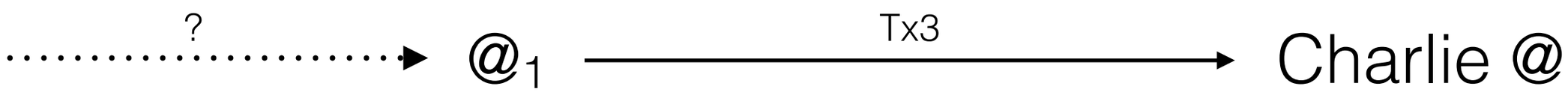


No idea where they go.

Traceability

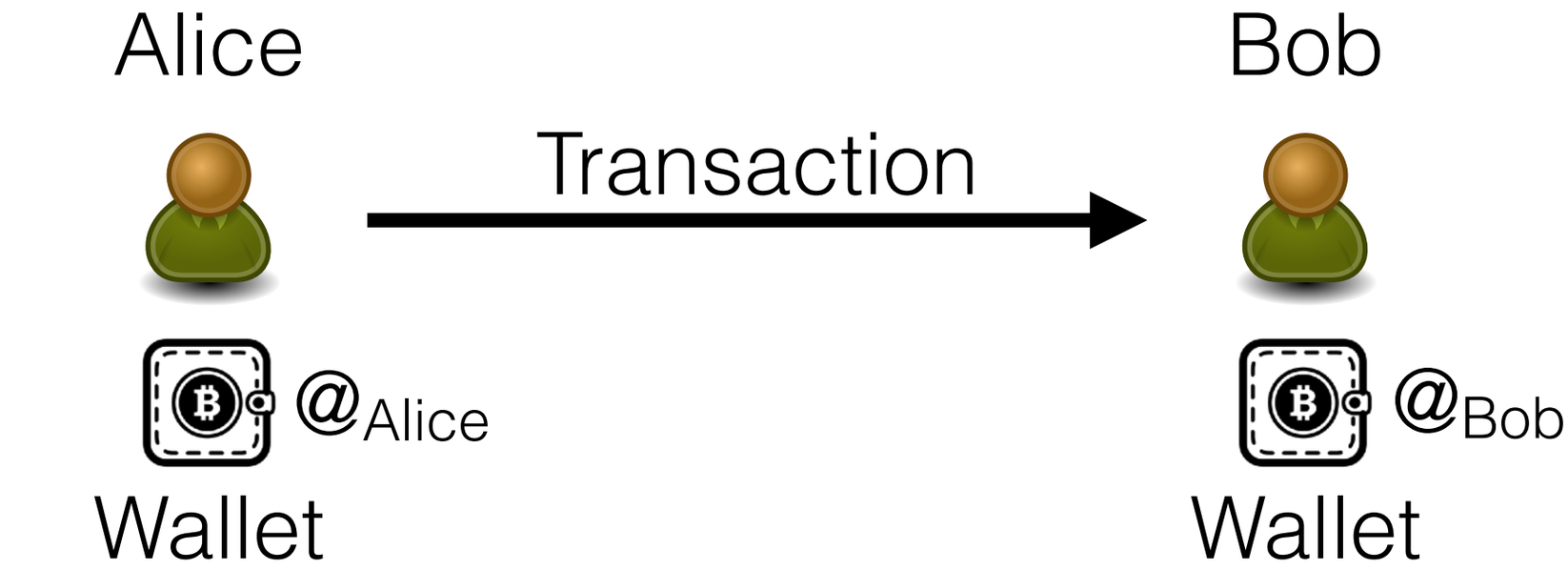
Tx3 spends funds received in Tx1 and Tx2.

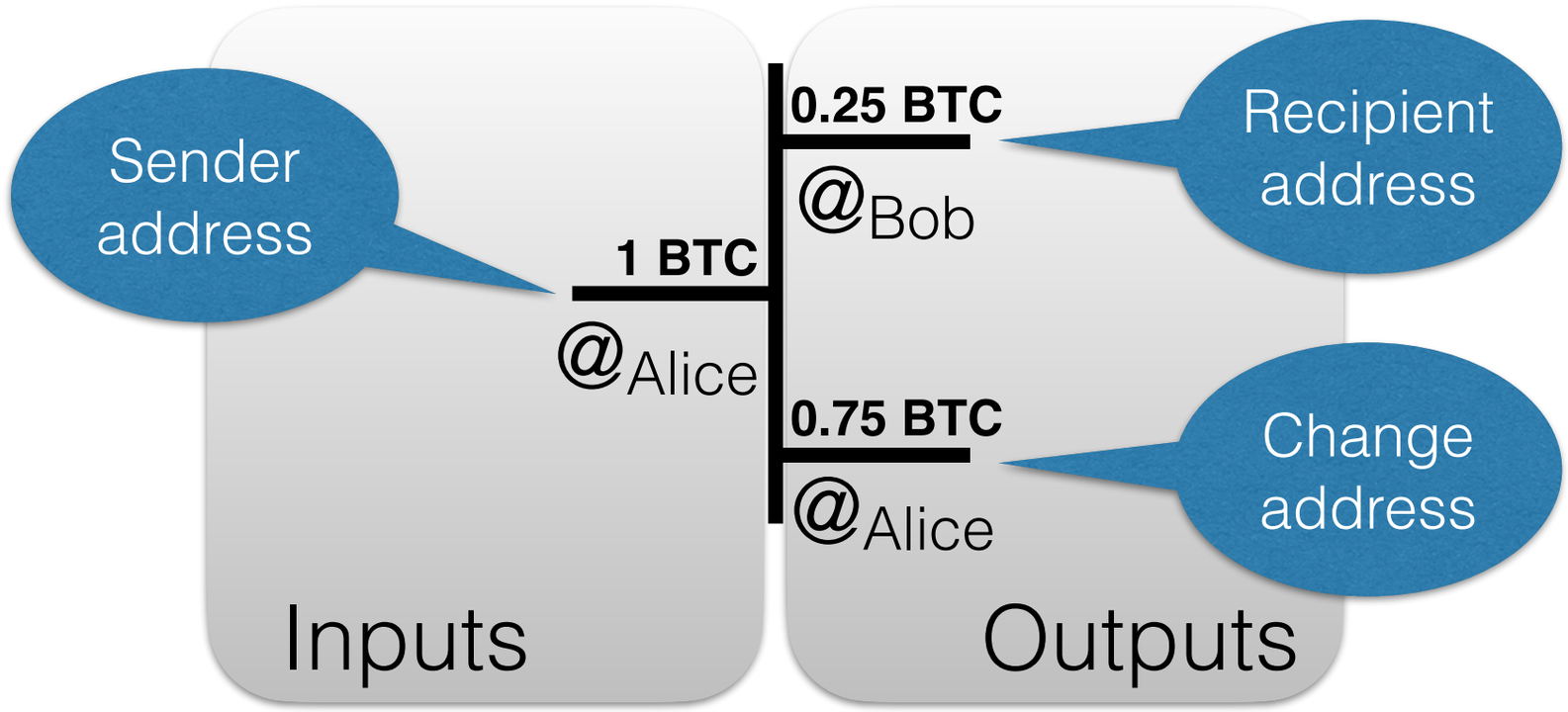
Untraceability



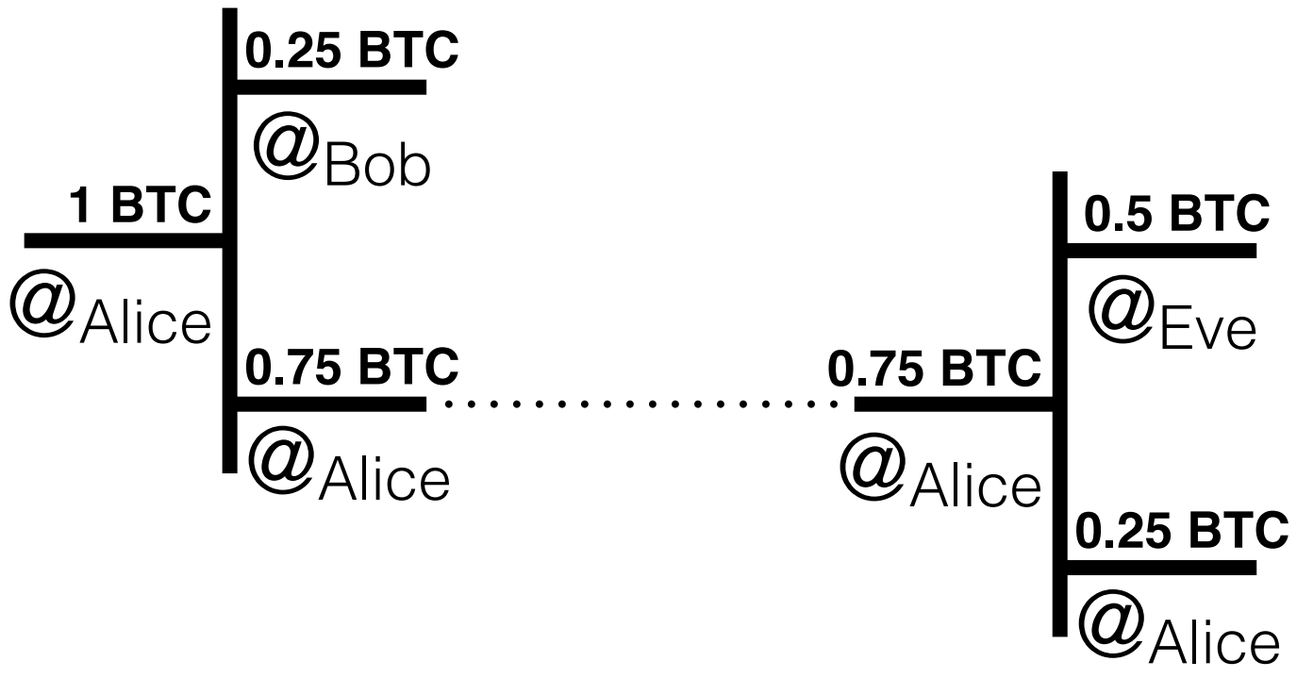
No idea where the funds from Tx3 come from.

Transactions in Bitcoin (UTXO model)





Transactions in Bitcoin

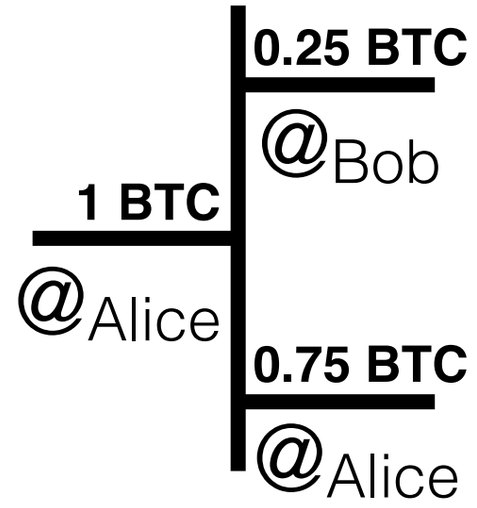


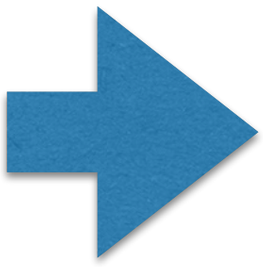
Transaction 1 Transaction 2

Heuristics to Cluster Bitcoin Addresses

- **Change Address**
  If new, then likely a change address

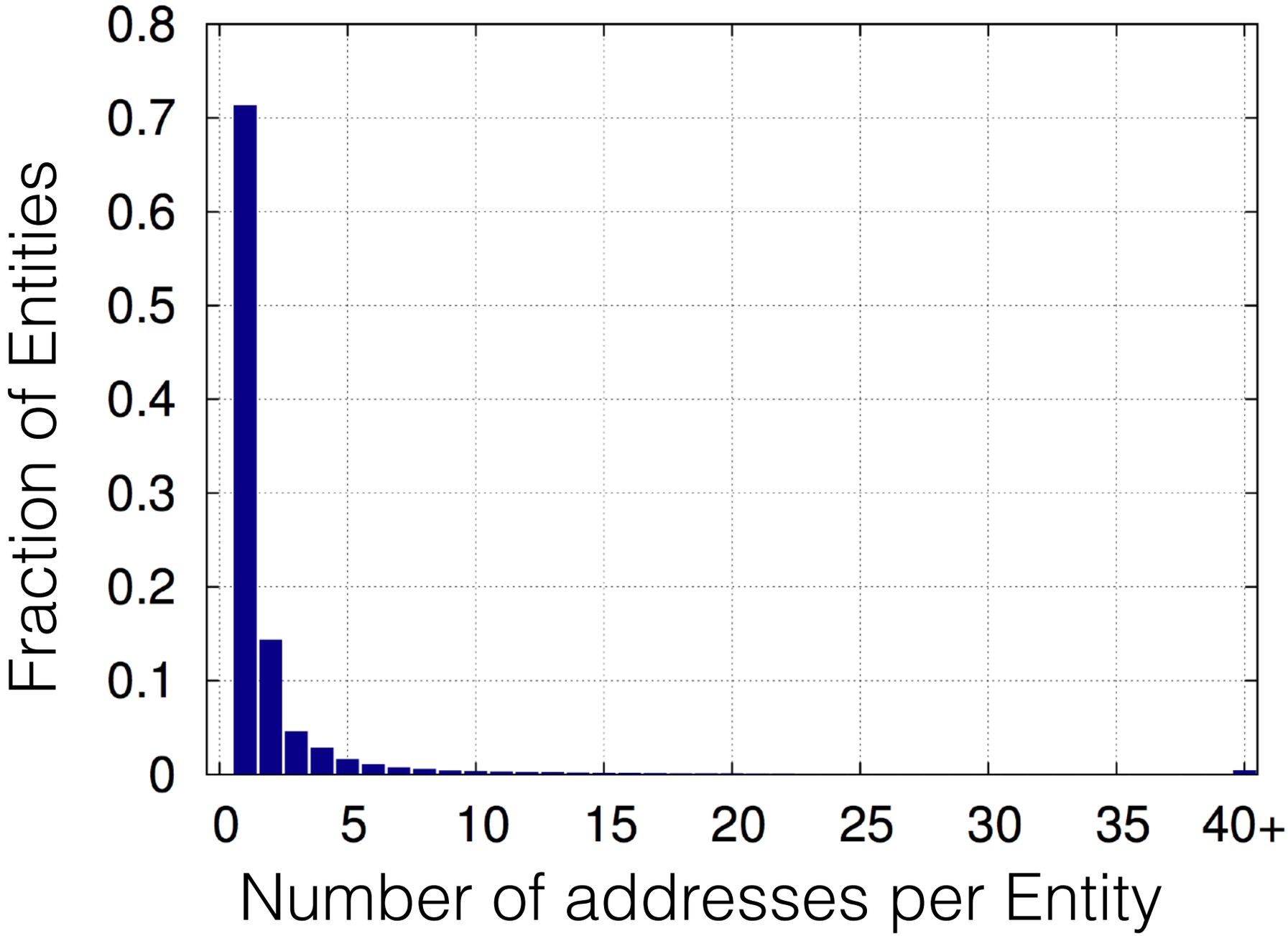
- **Multi-input Transactions**
  All inputs can be signed by the same entity.





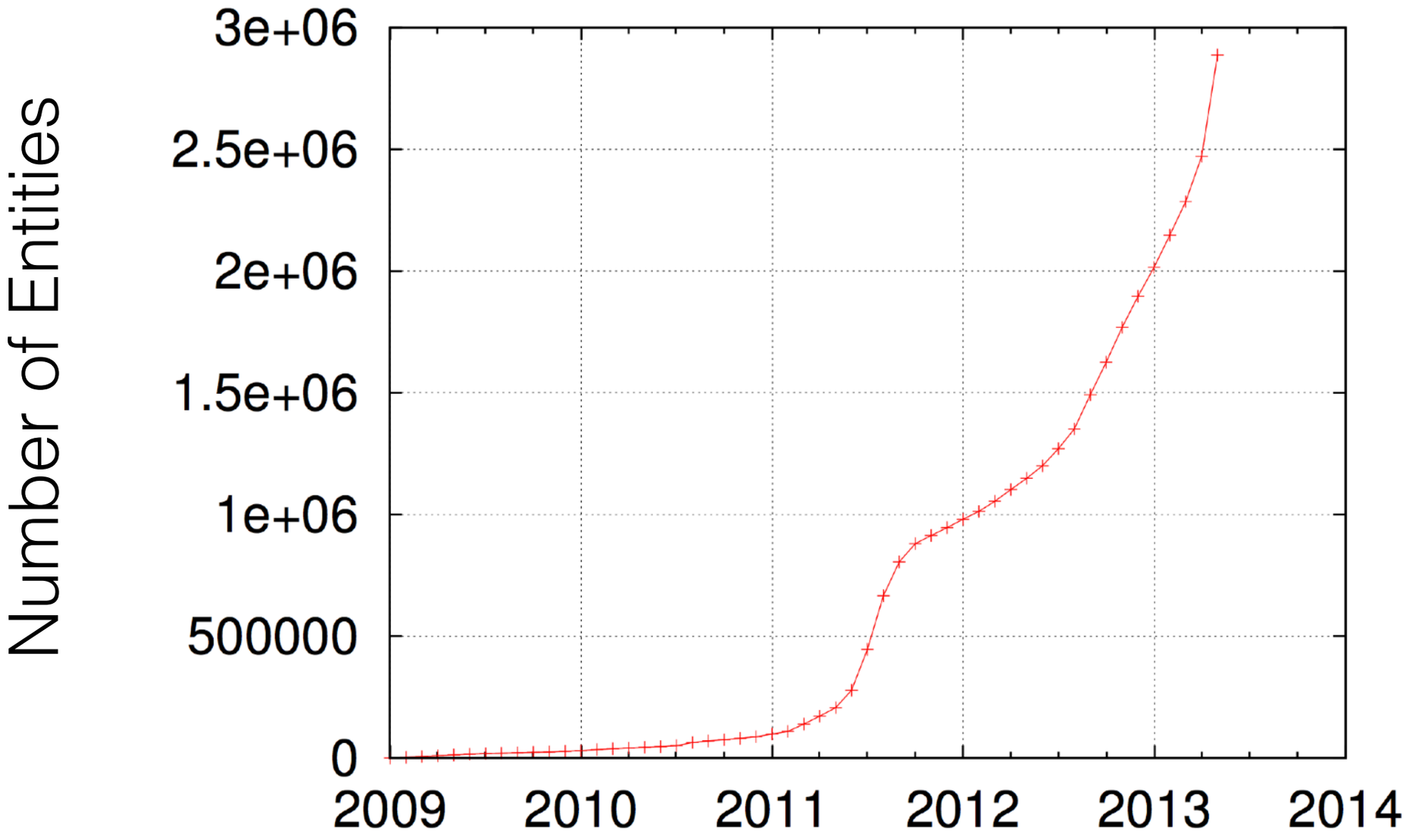
Possible to cluster addresses into cluster that might represent entities

Entity Cluster

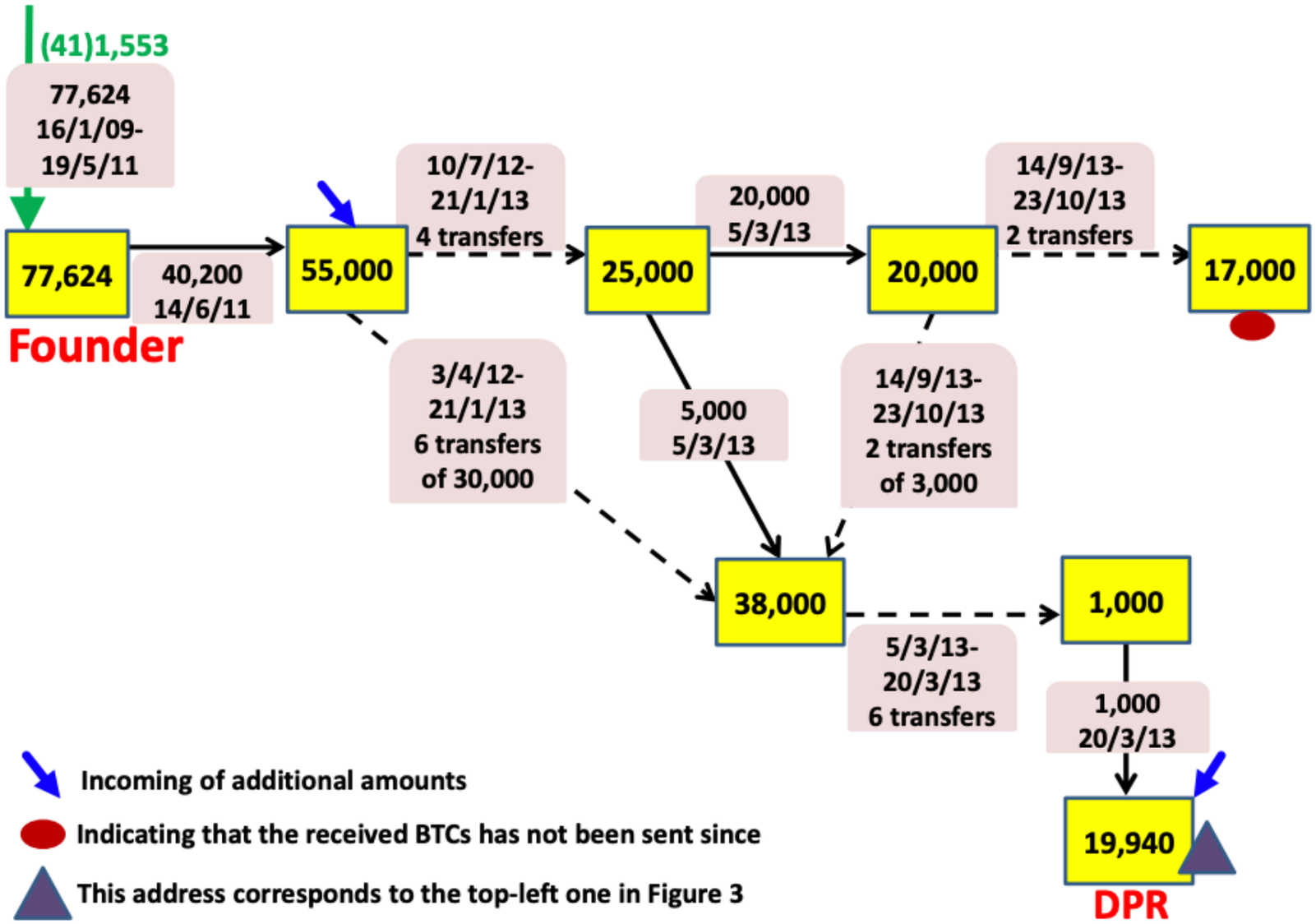


https://github.com/znort987/blockparser

Entity Evolution over Time



Easy to trace?



Published by FBI
After seizing Silk Road server