**Blockchain Privacy
Add-on/Mixer Privacy**

Blockchain Privacy Solutions

CoinJoin

0.25 BTC

$@_{Bob}$

1 BTC

$@_{Alice}$

0.75 BTC

$@_{Alice}$

4 BTC

$@_{Eve}$
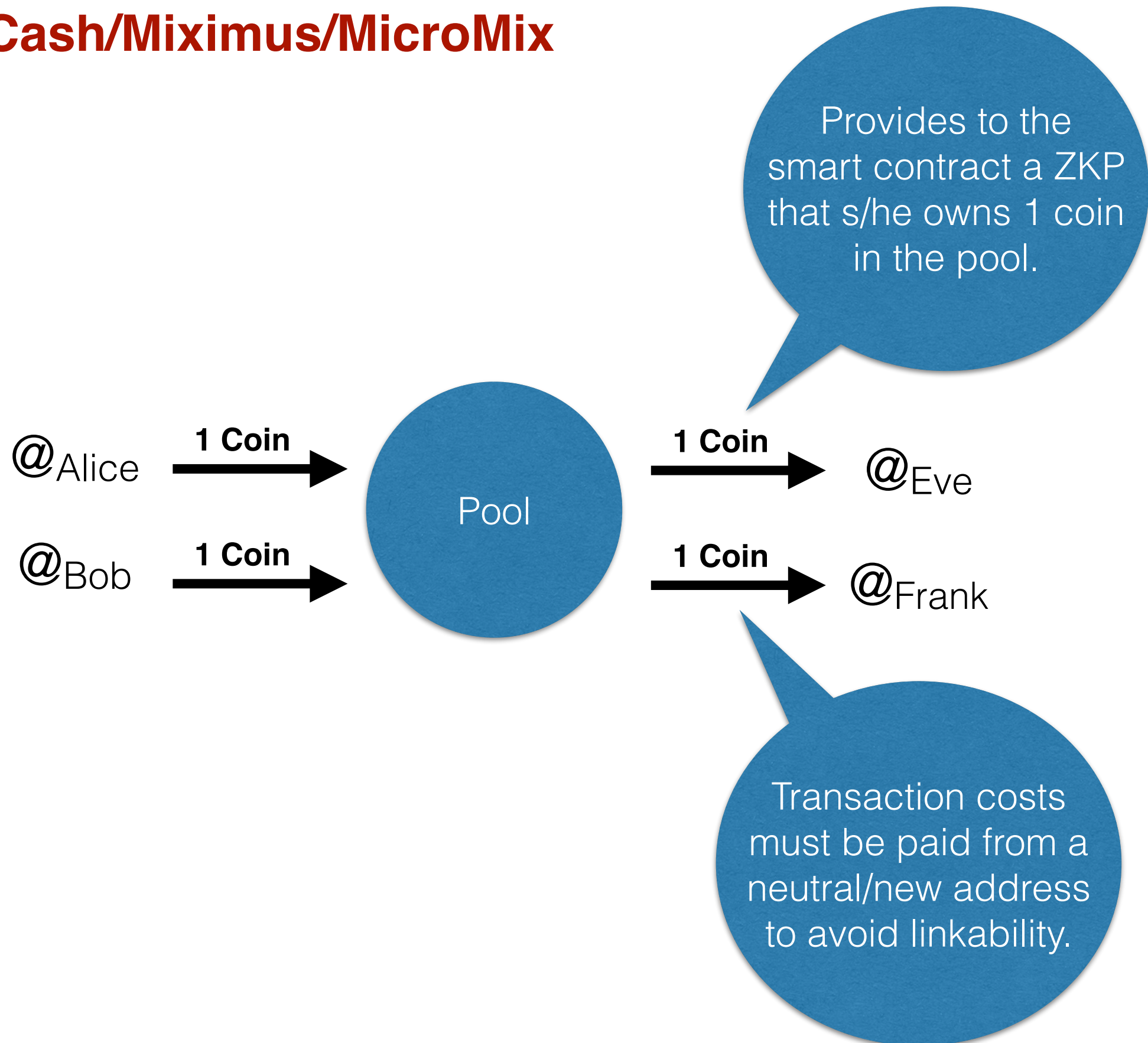
5 BTC

$@_{Frank}$

1 BTC

$@_{Frank}$
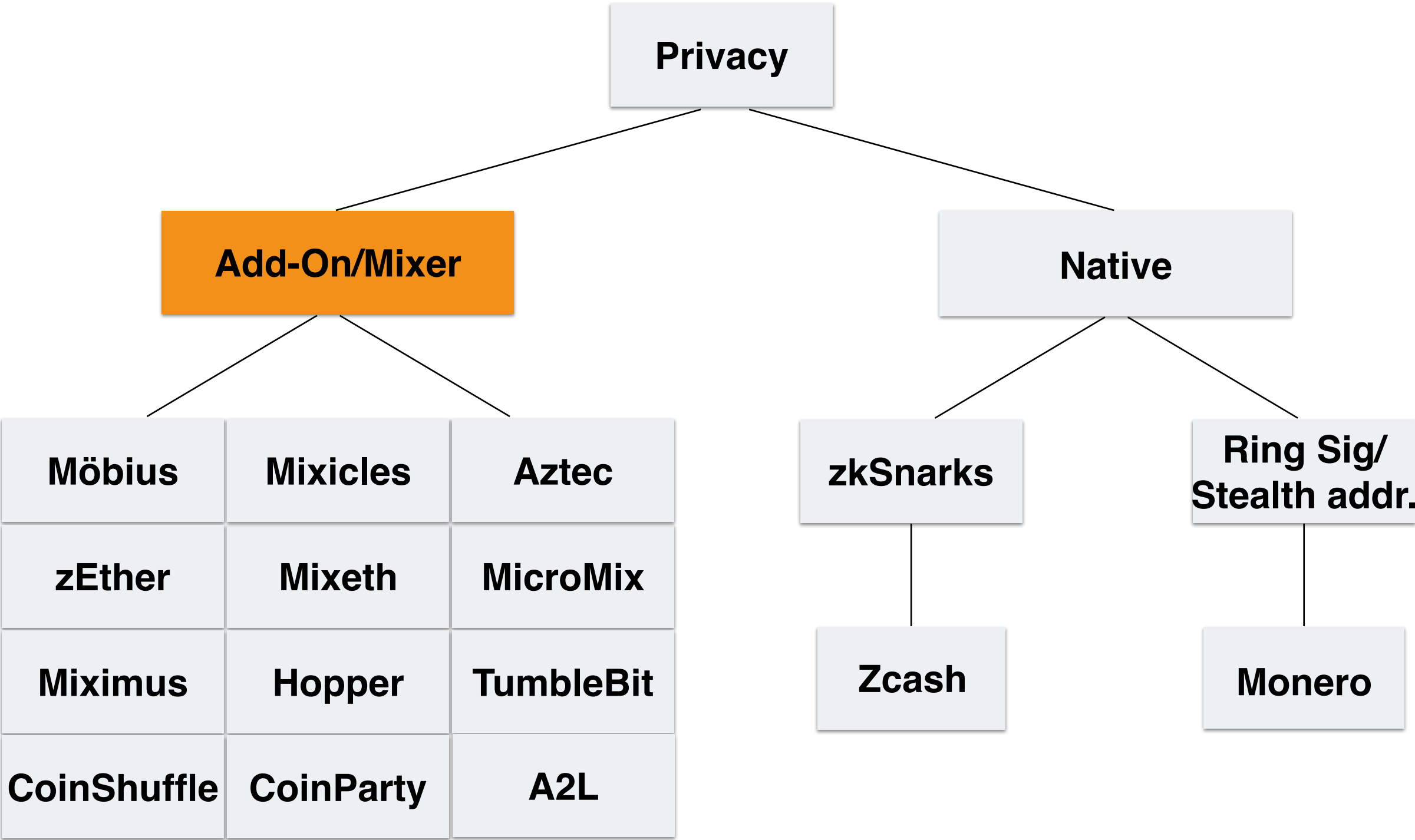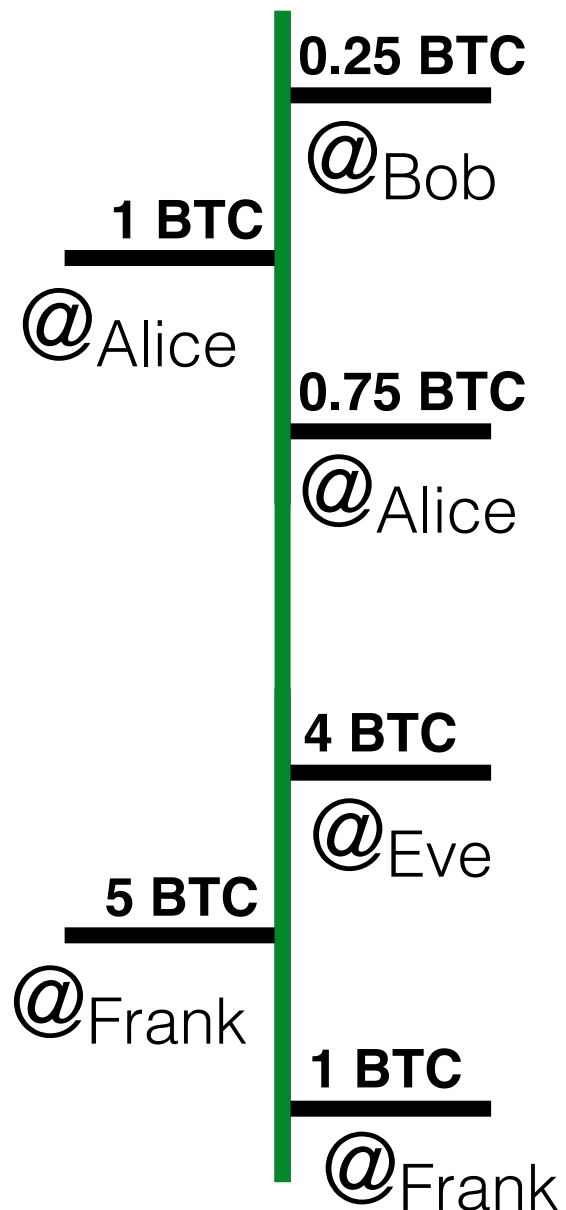
Transaction

Advantages 👍

- Hides the originator of a transaction

Drawbacks 👎

- Need for a *trusted third party* to merge the transactions

- No "spontaneous" mixing

- Doesn't hide amounts

- "Small" anonymity set

Tornado Cash/Miximus/MicroMix

@Alice ——**1 Coin**——▶ Pool ——**1 Coin**——▶ @Eve

@Bob ——**1 Coin**——▶ Pool ——**1 Coin**——▶ @Frank

Provides to the smart contract a ZKP that s/he owns 1 coin in the pool.

Transaction costs must be paid from a neutral/new address to avoid linkability.

Tornado Cash/Miximus/MicroMix

Advantages 👍

- Hides the originator of a transaction

- Increasing anonymity set
  (as long as not everyone withdraws)

- No coordination among users

Drawbacks 👎

- Need for fresh coins to withdraw **or**
  a third party relayer

- Non user-friendly amounts

Pool

1 Coin → @Eve

1 Coin → @Frank