Fee-bumping with presigned transactions protocols

Antoine Poinsot (@darosior)

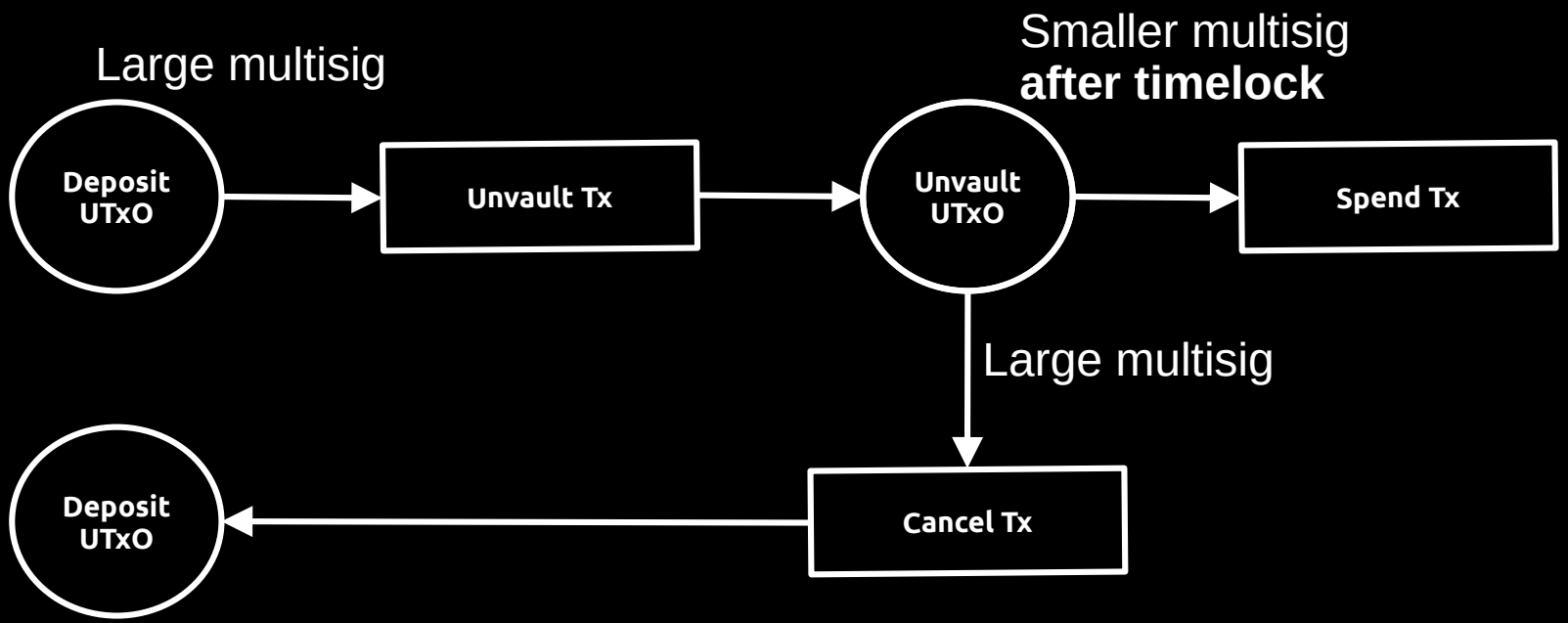
Why?

- Rely on timely confirmation
- Unilateral decision / multi-party contract
  - For security..
  - ..But not only!

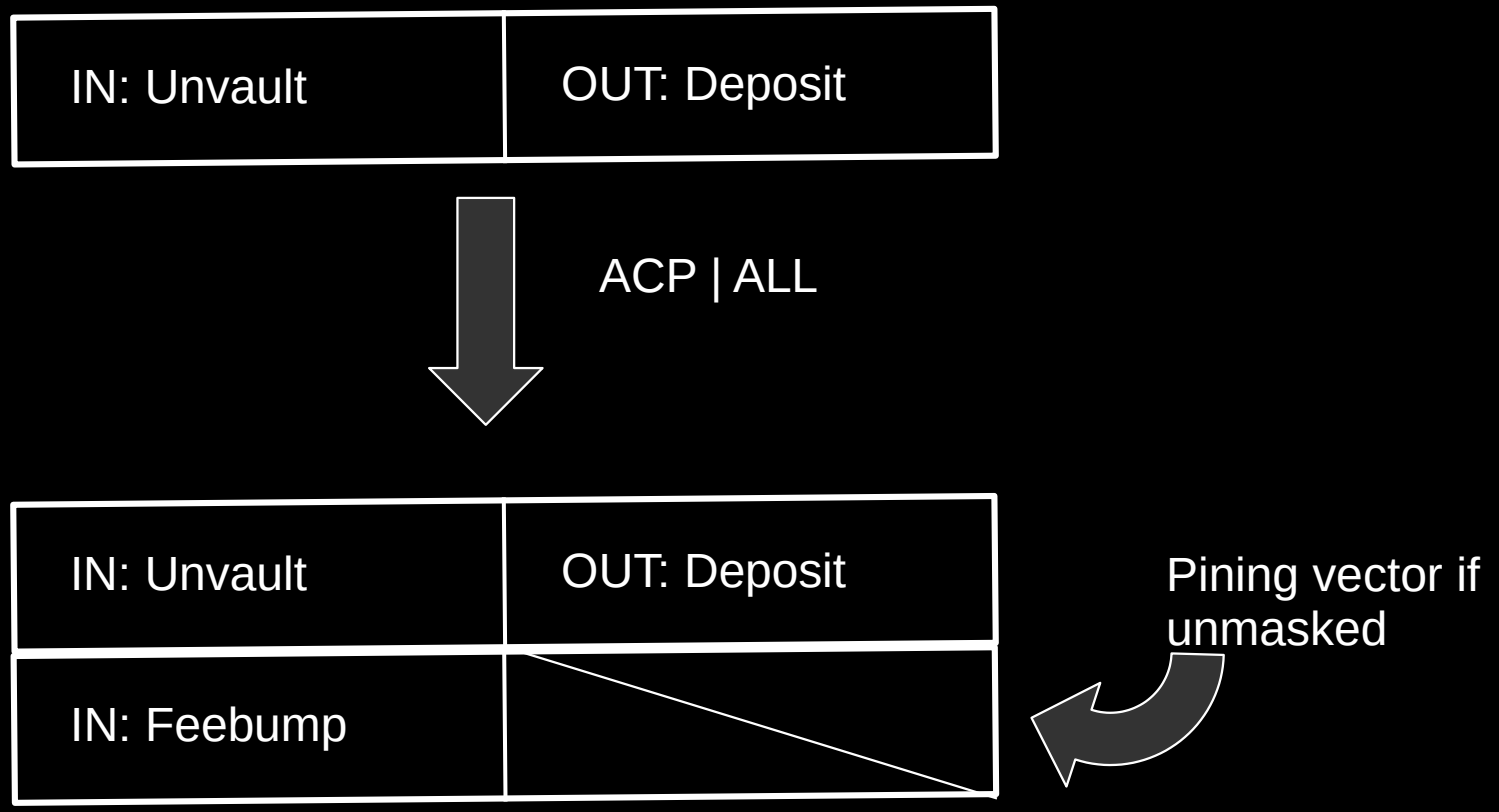
How?

- Anchor outputs on the commitment txs
- SINGLE|ACP for the HTLC transactions paying to us

Revault


Large multisig
Smaller multisig
after timelock
Deposit UTxO
Unvault Tx
Unvault UTxO
Spend Tx
Large multisig
Deposit UTxO
Cancel Tx

Revault


IN: Unvault
OUT: Deposit
ACP | ALL
IN: Unvault
OUT: Deposit
IN: Feebump
Pining vector if unmasked

Problem statement

- How to ensure confirmation of Cancel transaction 99.999% of the time?
- Assumptions
  - Miner are rationale (**and incentivized by public fees**)
- Constraints
  - Don’t overpay
  - Least possible number of added inputs
  - Least possible number of coin / vault

Unbounded problem

- In theory no maximum feerate
- Rationally, you'd spend as much as is under watch -1sat
  - Unreasonable! You won't keep dozens of coin sitting in a hot wallet to enforce the security of a coin of the same value!
- New assumption: the « reserve feerate »

Fee reserve

- How many sats to keep around for bumping?
  - Per-vault reserve * number of vaults
- How many sats to keep per vault?
  - Up to what feerate do we cover?
    - X th percentile over the last N blocks
    - Historical maximum (95th percentile to remove outliers)
    - Dollar-adjusted historical max?

UTxO pool layout / management

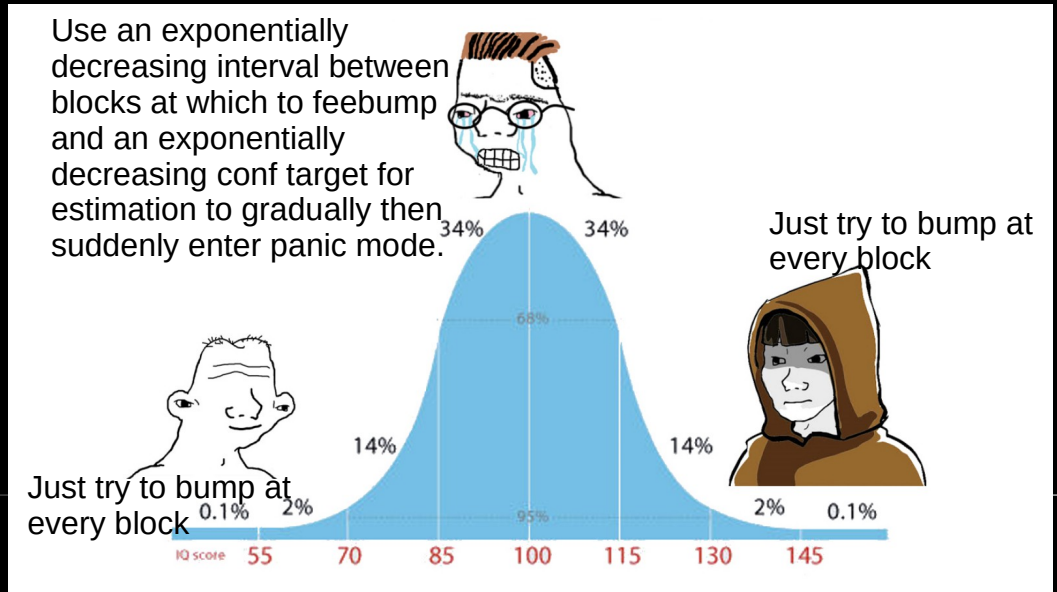
- How to split coins per vault
  - Not enough → overpayments
  - Too many → overpayments
- Manage the pool across time
  - Fanout the coins according to the layout
  - Consolidate during low fee periods

Coin selections

- Which coins are you going to allocate to a given vault?
- Which coin(s) are you going to select to bump the Cancel transaction?

Bumping : when

- Long timelocks, should we try to greed?
  - It depends™
  - Flatten the curve™?



Bumping : how

- Fee estimation tricks?
- What about re-bumping?
  - Every block?
  - By how much?
  - Panic mode?
    - Could skew miners incentives if you multiply feerate by >N and they have >=N % of the hashrate
  - Probably want a randomized delta to ensure propagation

Methodology

https://github.com/revault/research

- Rolled forward the chain with historical estimates from statoshi and txstats
- Different strategies w/ different configs
  - For the reserve
  - For the UTxOs amount distribution
  - For the to-consolidate and to-bump coin selections
  - For the rate of Unvault, invalid Unvault, and catastrophe
  - For the number of participants and vaults under watch

Choices

Reserve distribution

U_{n+1} *= U_n / 2*

U_0 *= reserve / 2*

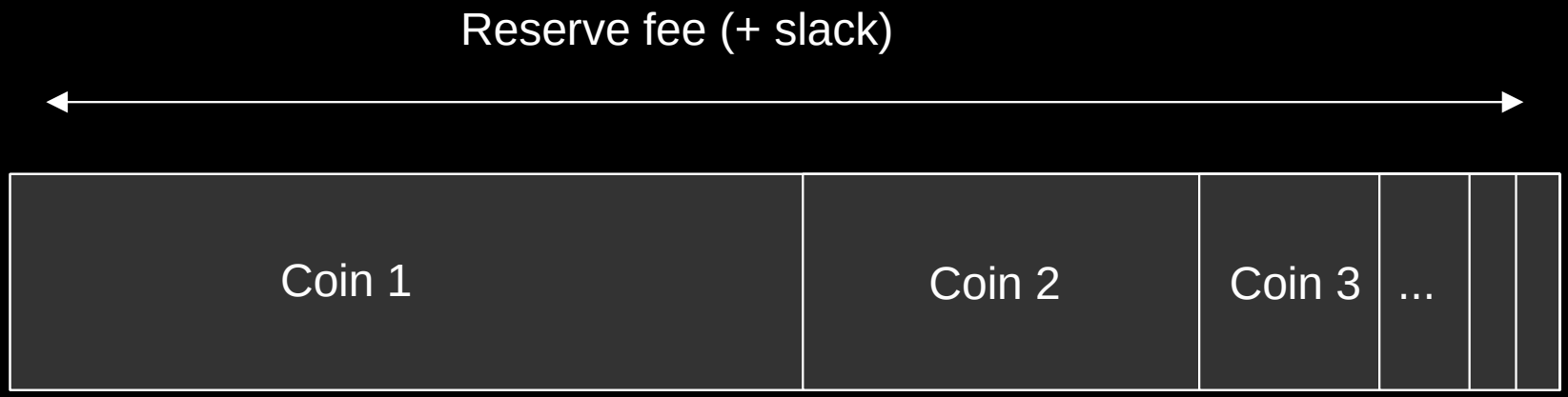
U_{min} *= pays for its fees at reserve feerate + bumps by 5sat/vb*

Bonus distribution

V_{n+1} *= V_n / 2*

V_0 *= U_{min} / 2*

V_{min} *= Cancel tx fee at current feerate*



Choices

- Cancel coin selection
  - Follows
  - Caps overpayment to the minimum coin value
- Allocation coin selection
  - Find coins with tolerance from 5 to 30%

Choices

- Reserve feerate: maximum of rolling 95th percentile feerate over historical data (90days, min 144 points)
  - About 750sat/vb currently
- Consolidate-fanout transaction
  - Different strategies for selecting coins to be consolidated
  - Create as many distributions as we can, bonus ones being optional

Choices

- Fee-bumping
  - Every block
  - Check if below the next block feerate, if so bump by at least RBF delta + small randomization
  - `estimatesmartfee 2 CONSERVATIVE`
    - Fall back to 85th percentile last 6 blocks
- Refill guesstimation

Chancellor on brink of second bailout for offchain contracts