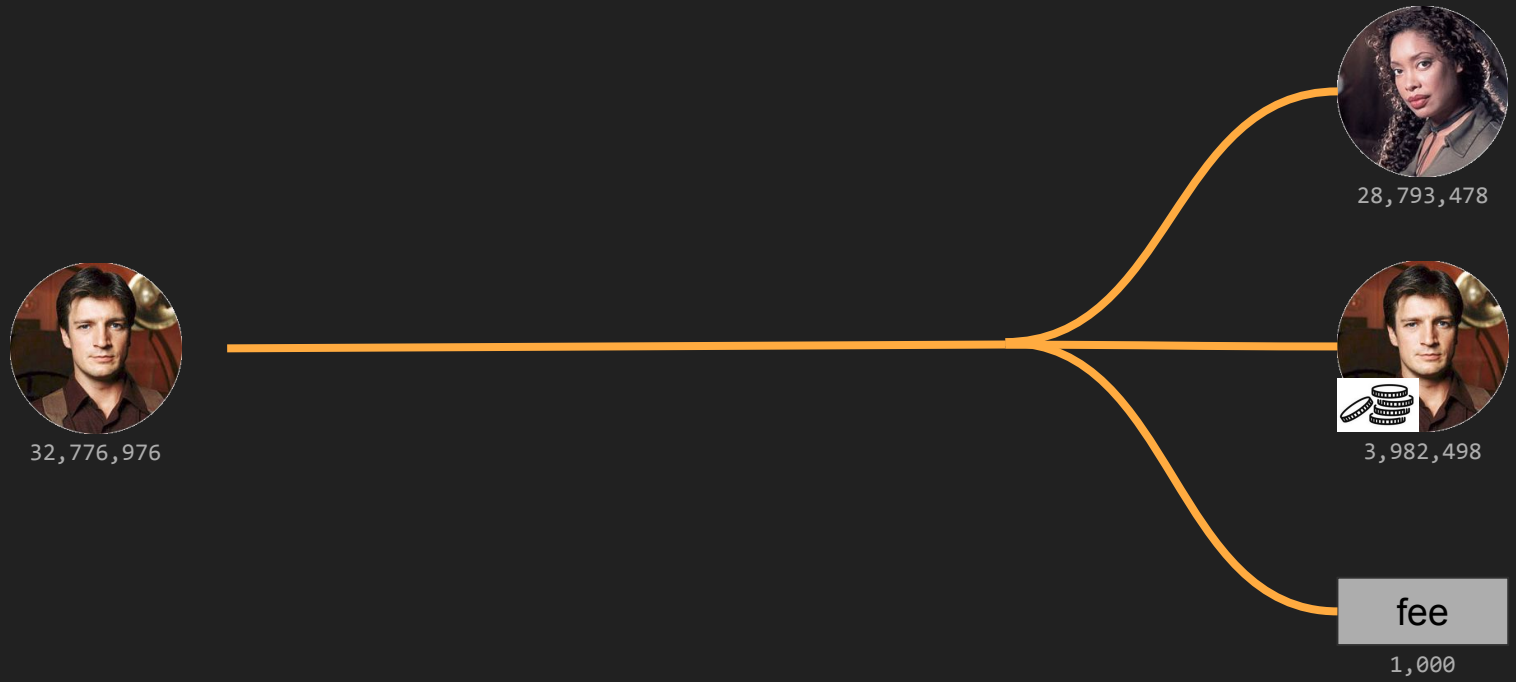
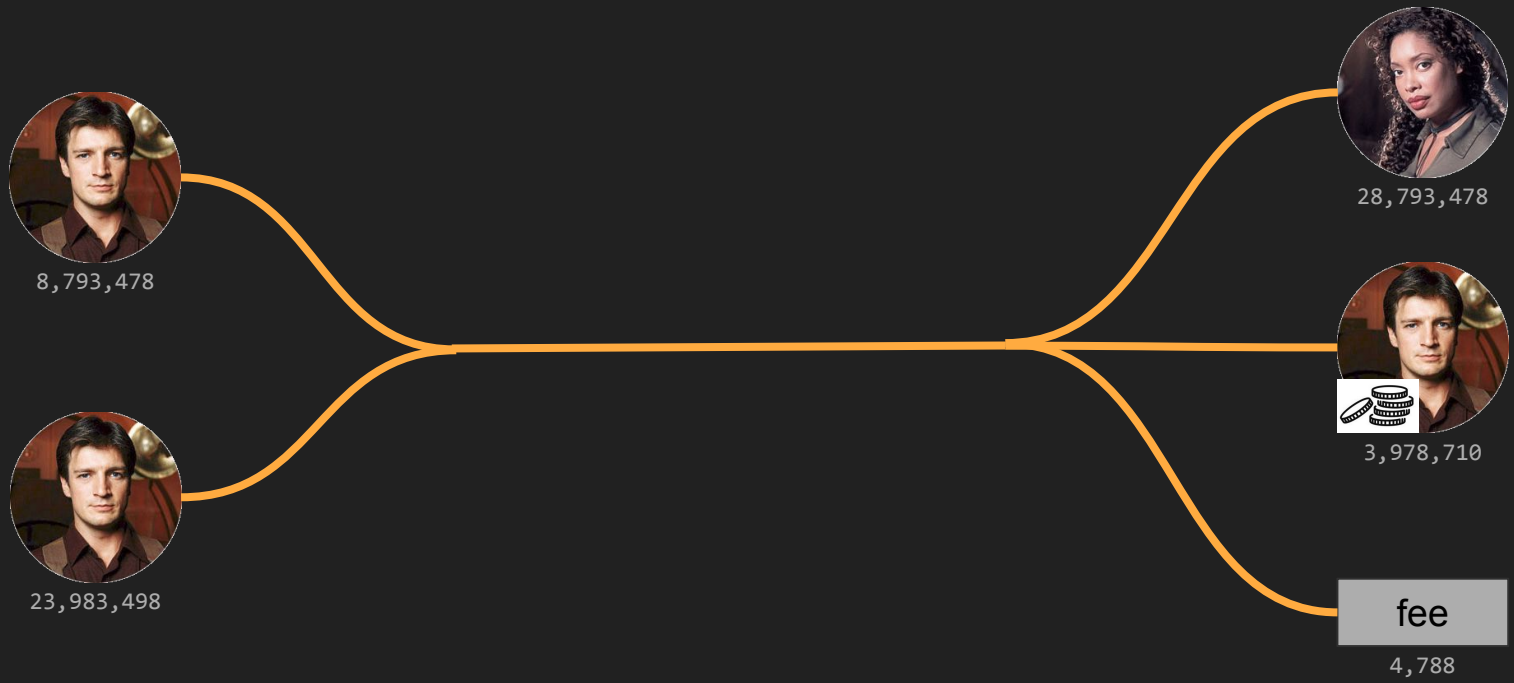
Payjoins & Coinjoins

aka Torturing Signing Devices

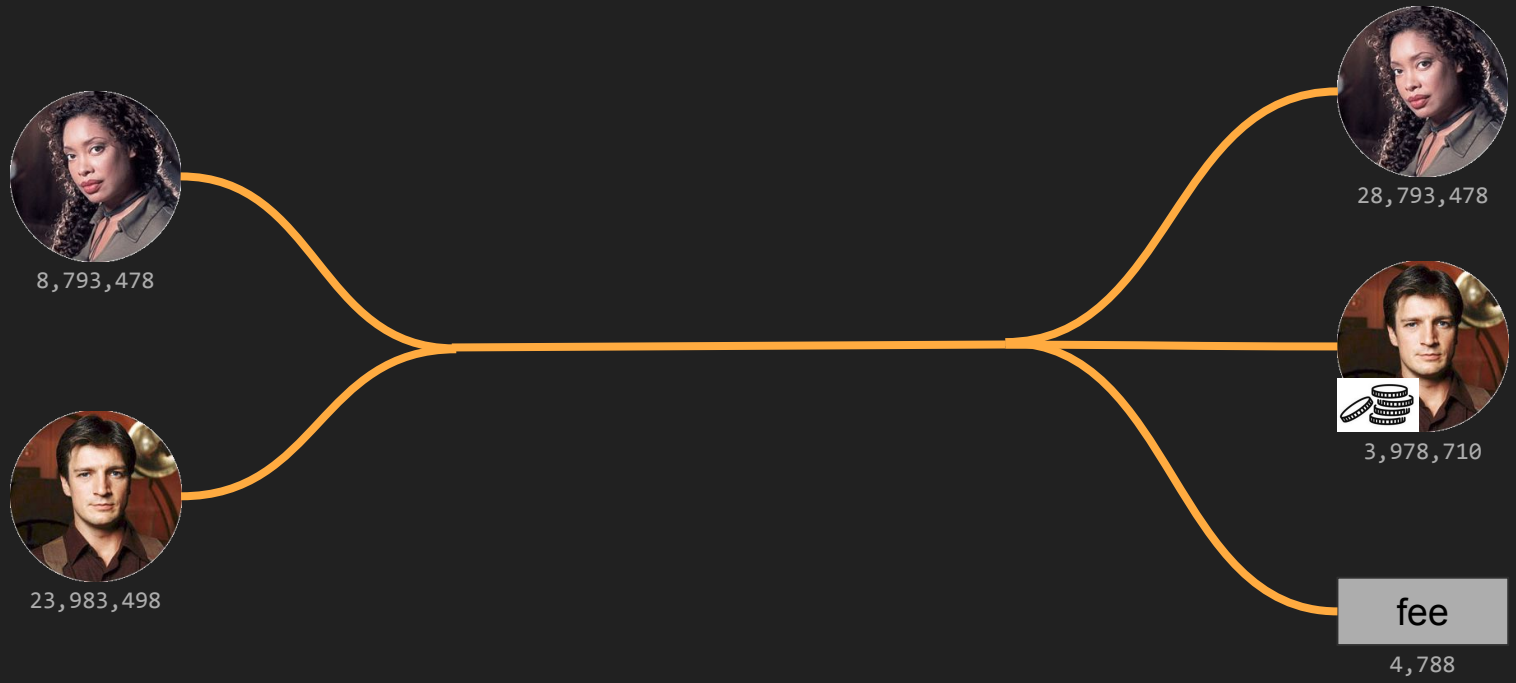
Malcolm pays Zoe 28m sats w/1 utxo



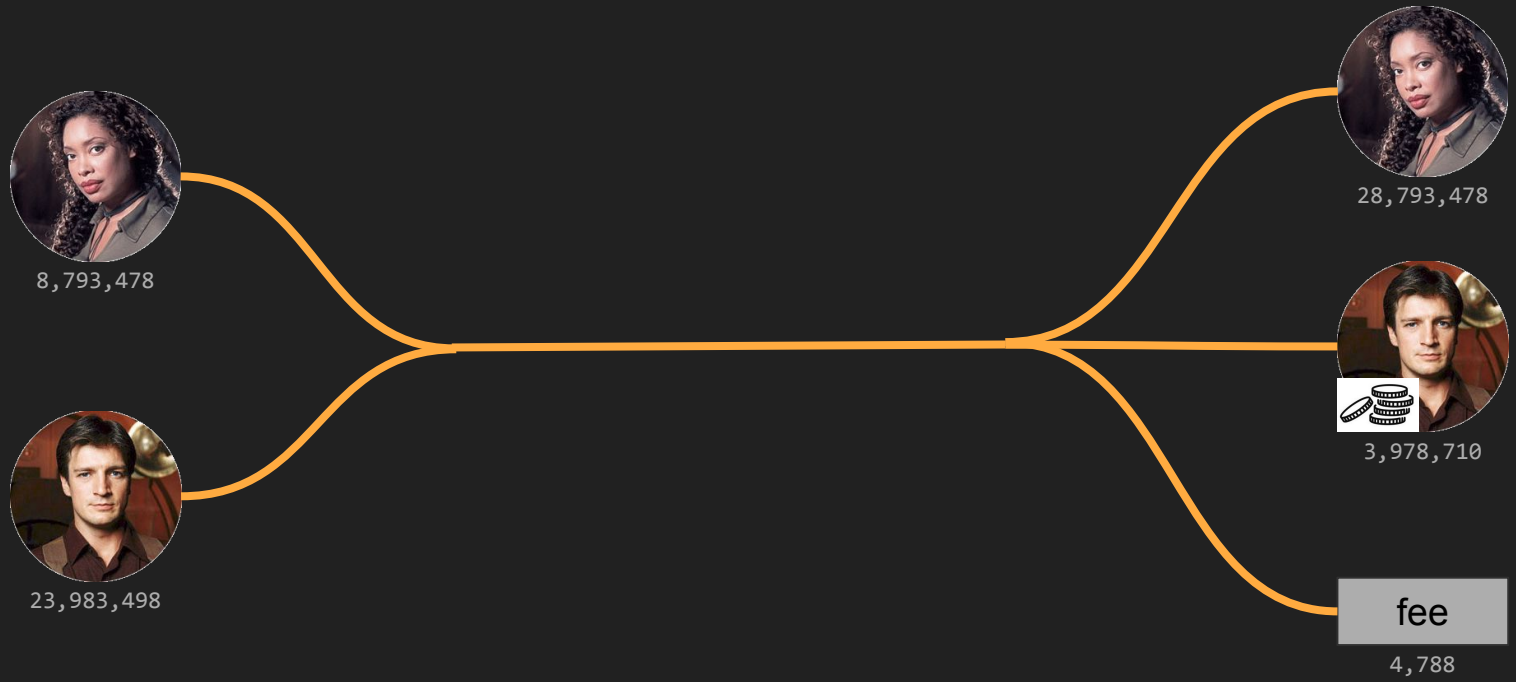
Malcolm pays Zoe 28m sats w/2 utxos



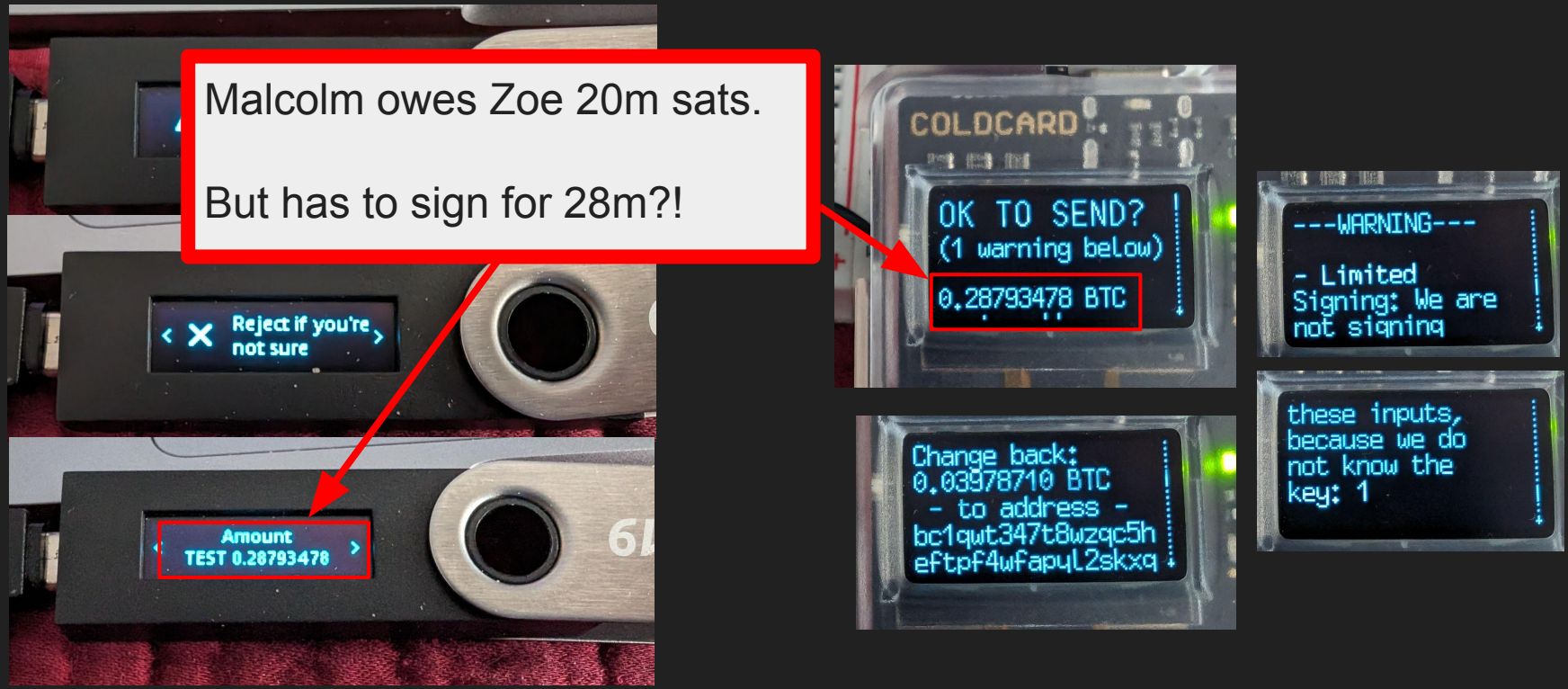
PAYJOIN: Malcolm only actually owes Zoe 20m sats



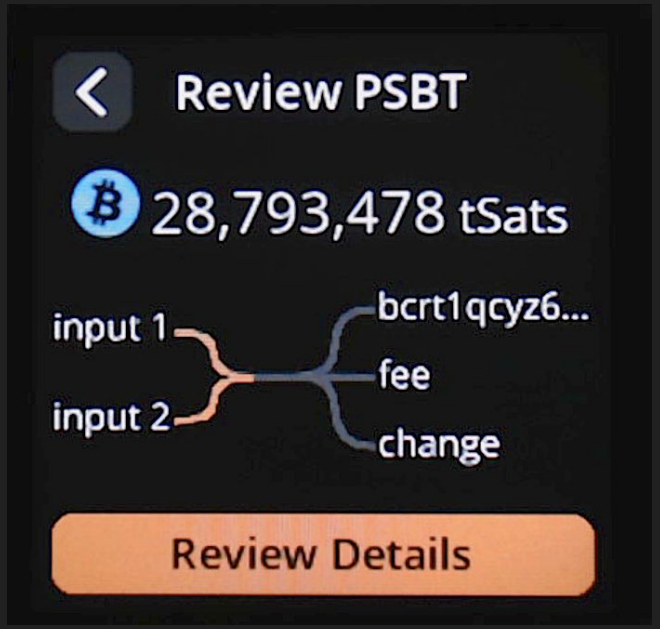
What does a naive signing device display?

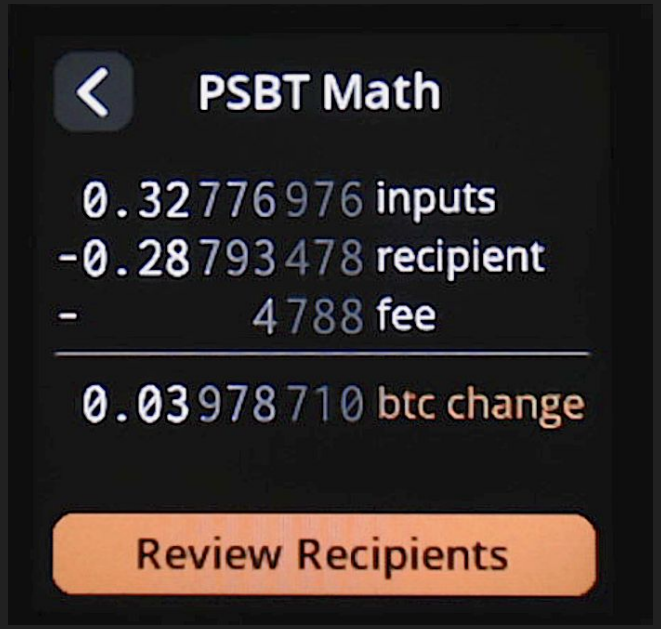


Payjoin: Malcolm's Perspective

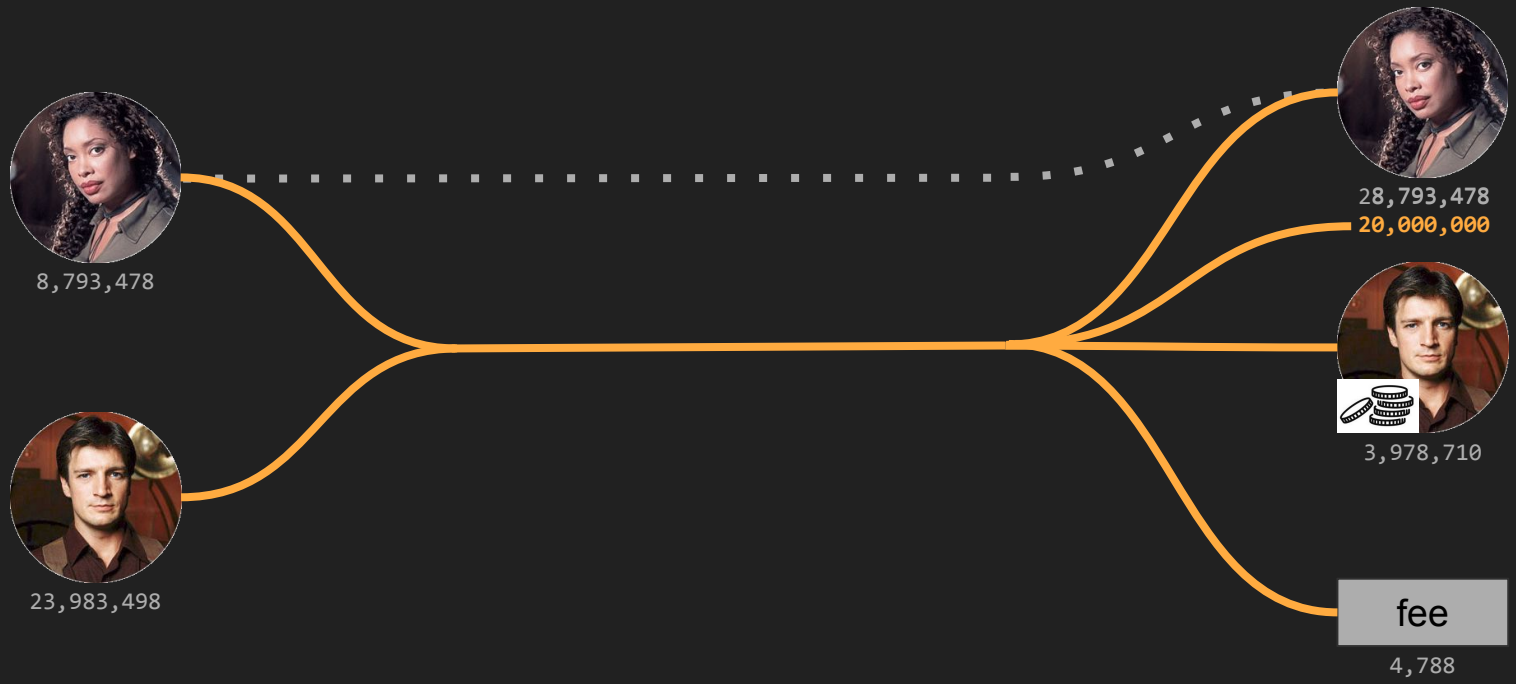


Naive SeedSigner: Womp, Womp… 😢

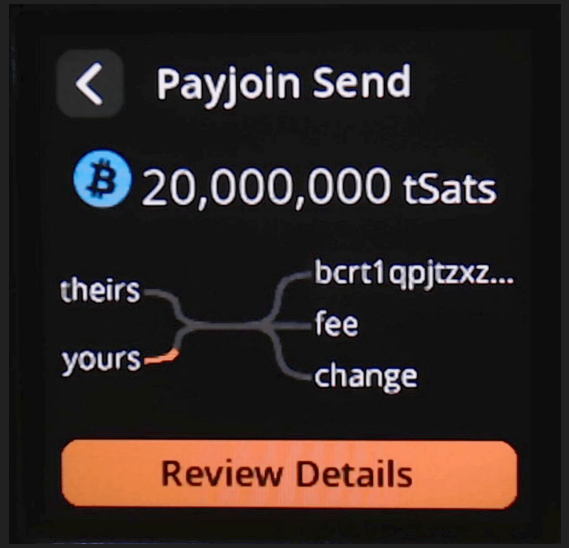




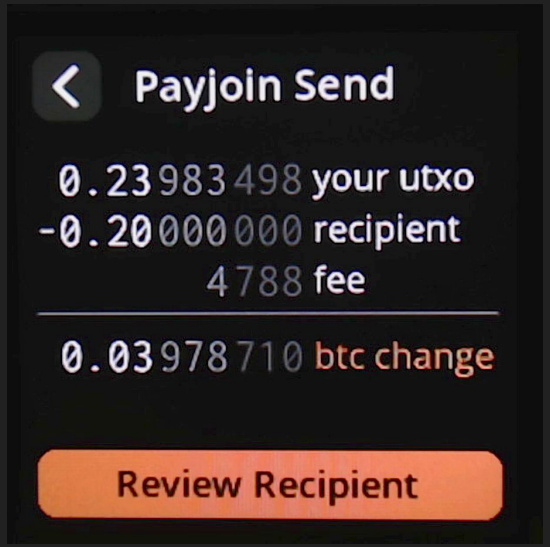
From Malcolm’s perspective



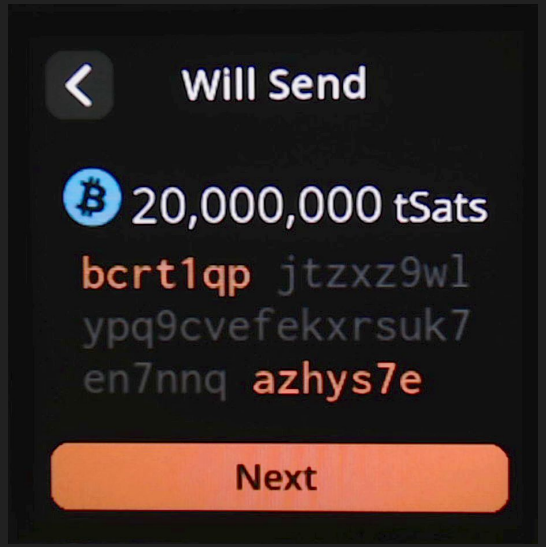
Work-in-Progress: SeedSigner payjoin send



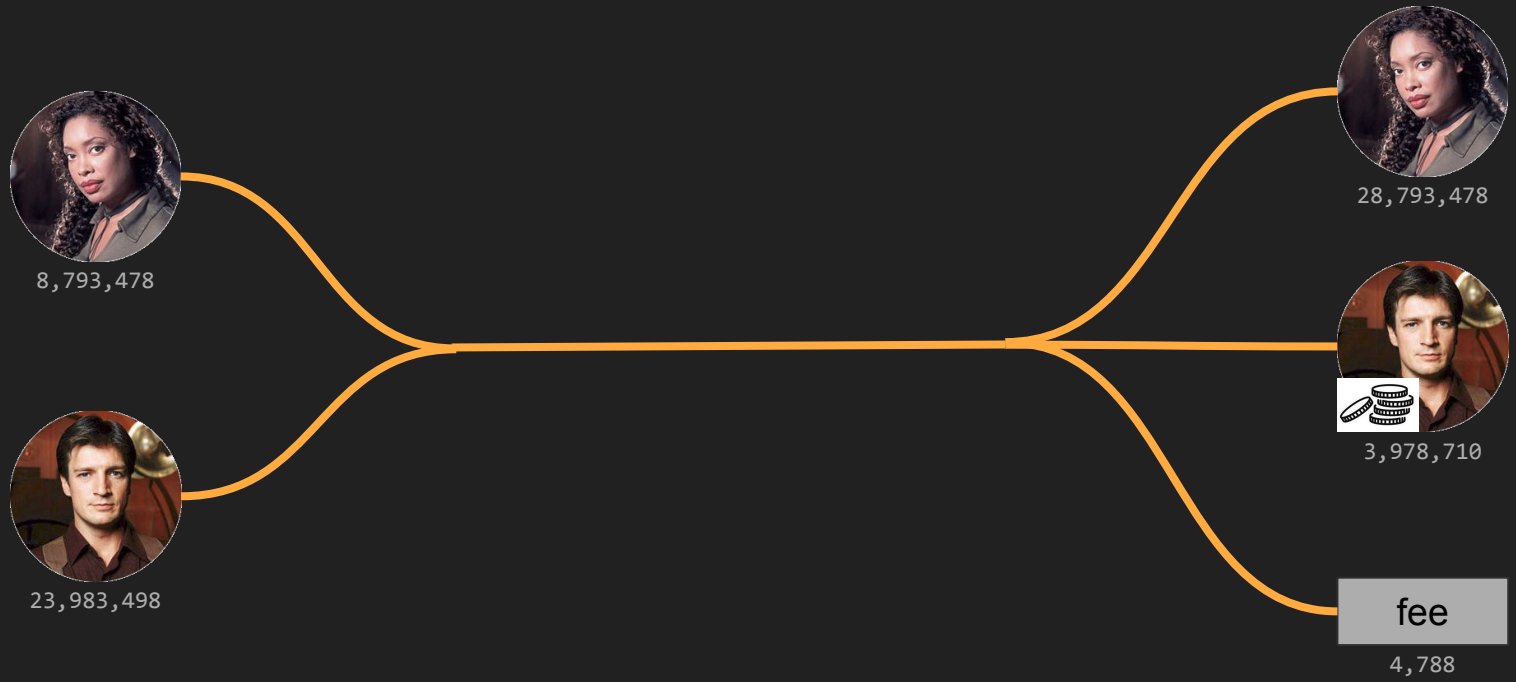
Work-in-Progress: SeedSigner payjoin send



Work-in-Progress: SeedSigner payjoin send



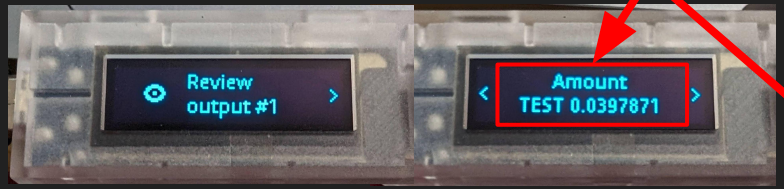
But Zoe has to sign the tx, too!

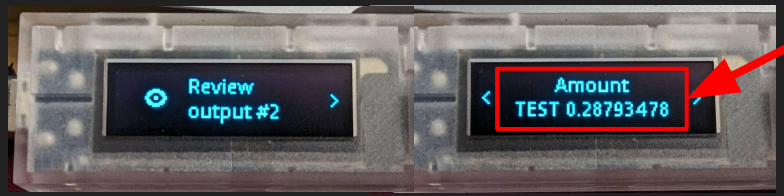


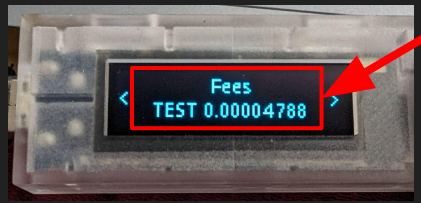
Payjoin: Zoe's Perspective

Is Zoe funding Malcolm's chang

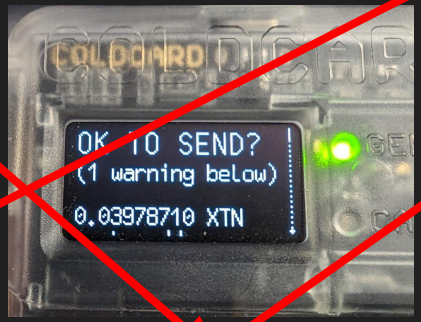
Is Zoe OVERpaying herself?

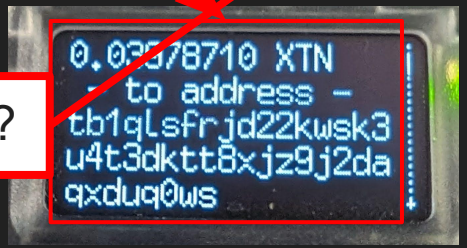


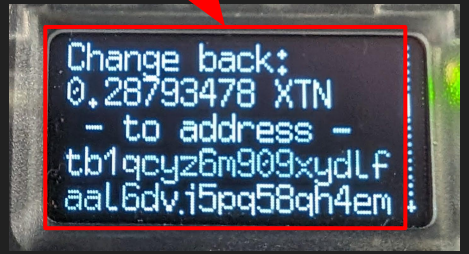




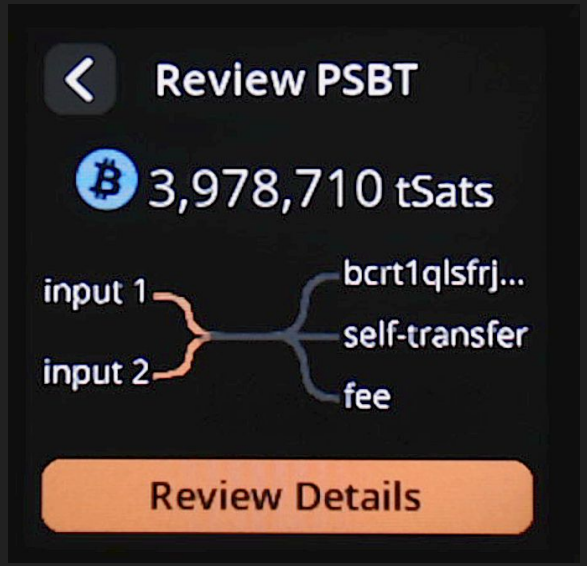
Is Zoe paying fees?

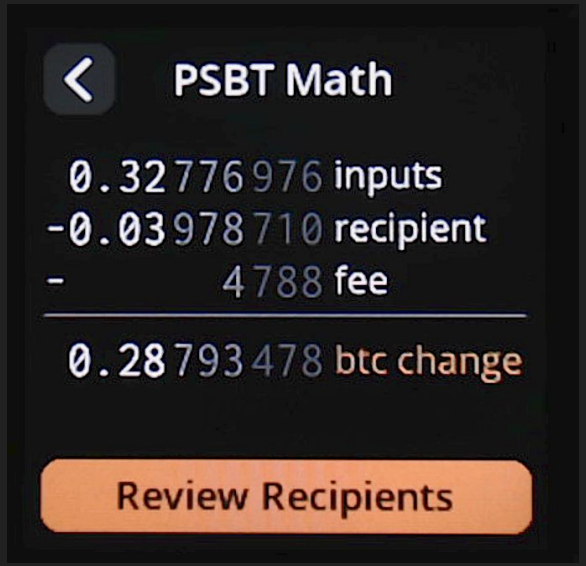




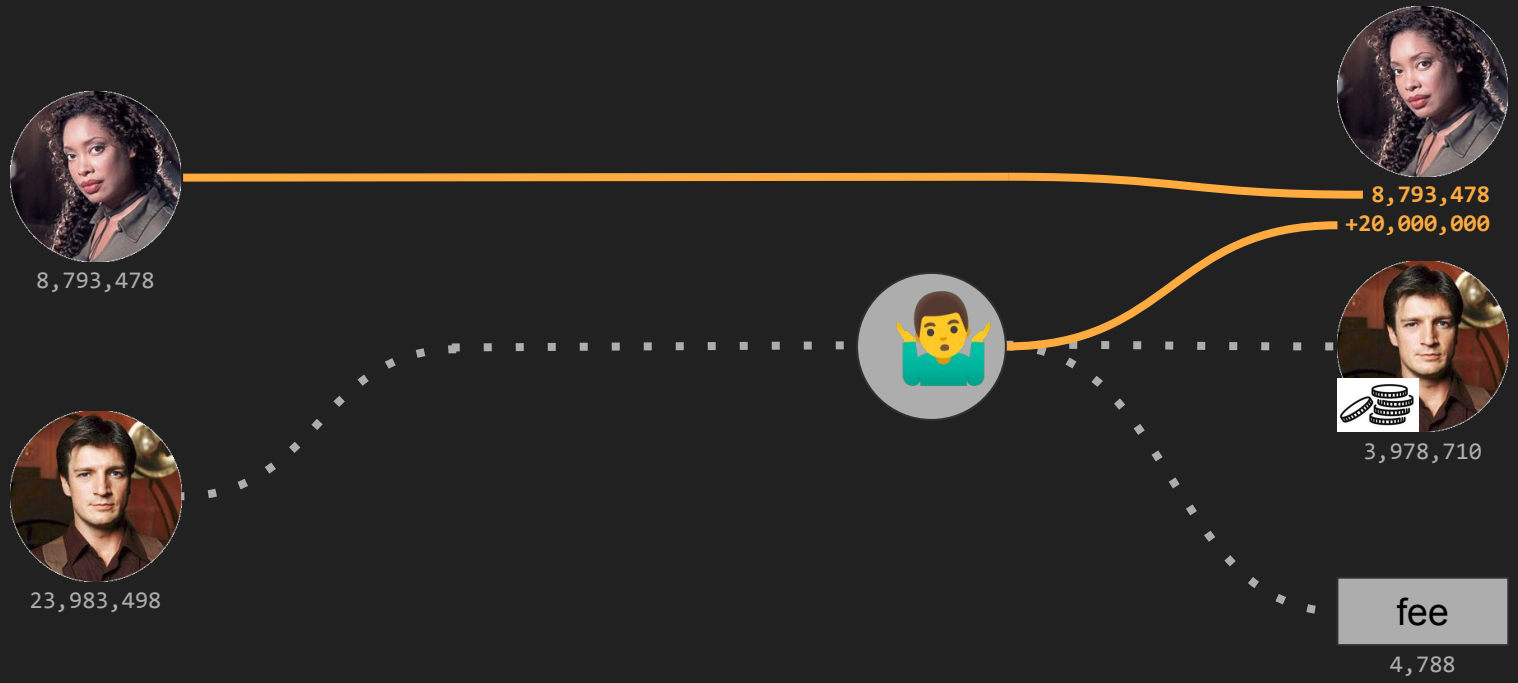


But naive SeedSigner…? Still 😢

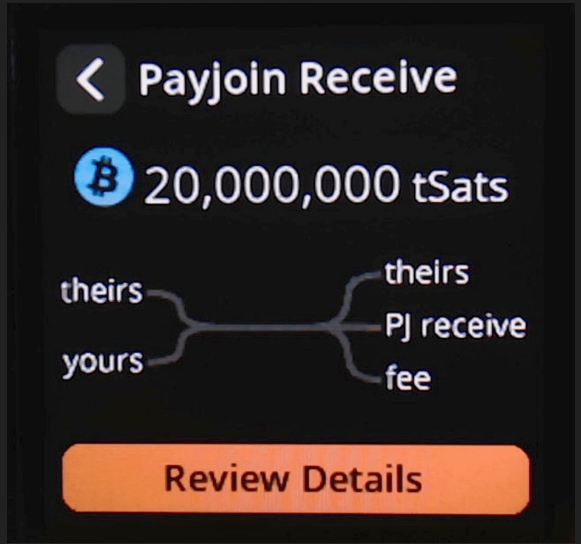




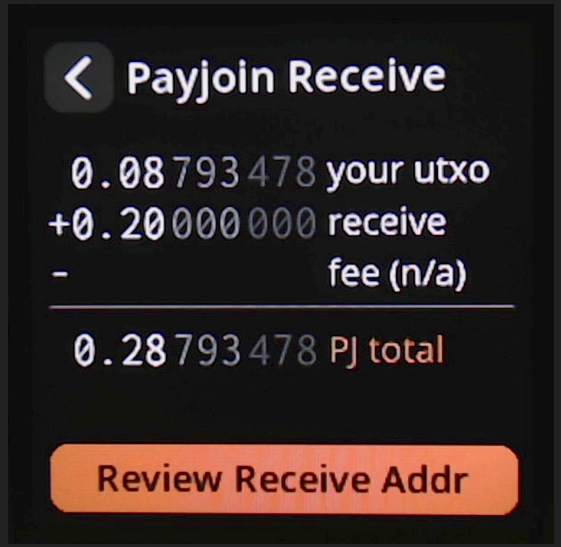
So what does Zoe care about?



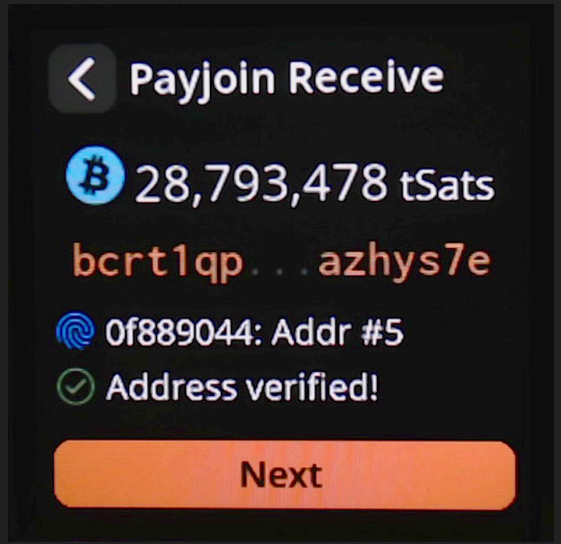
Work-in-Progress: SeedSigner payjoin receive



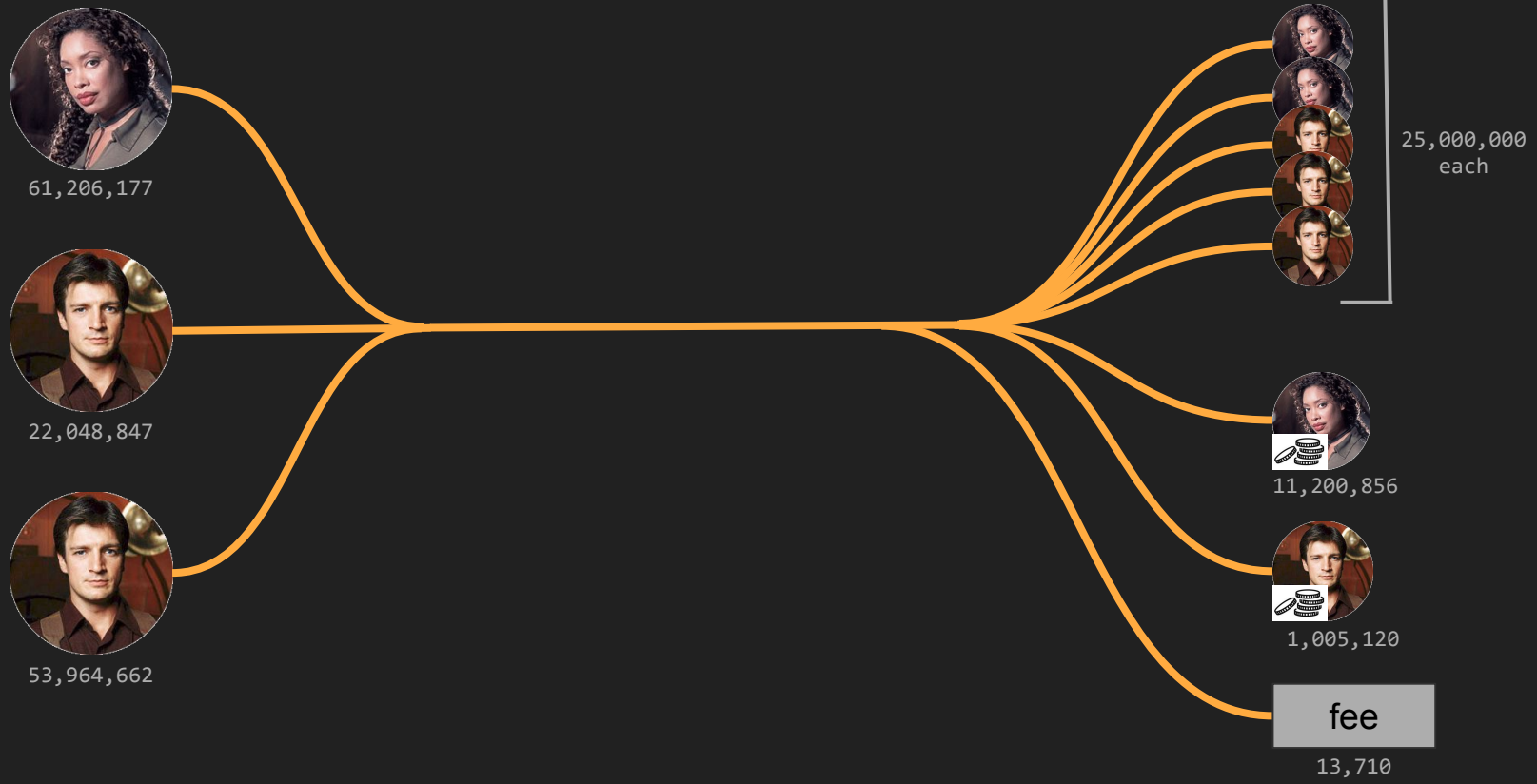
Work-in-Progress: SeedSigner payjoin receive



Work-in-Progress: SeedSigner payjoin receive

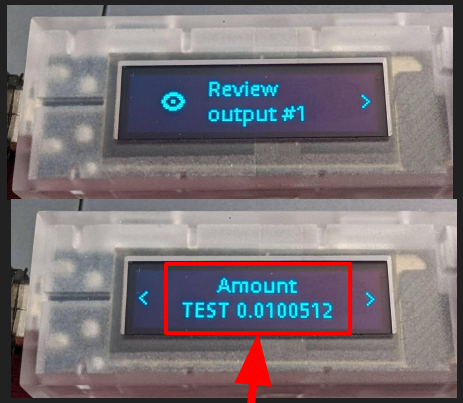


How about a coinjoin?

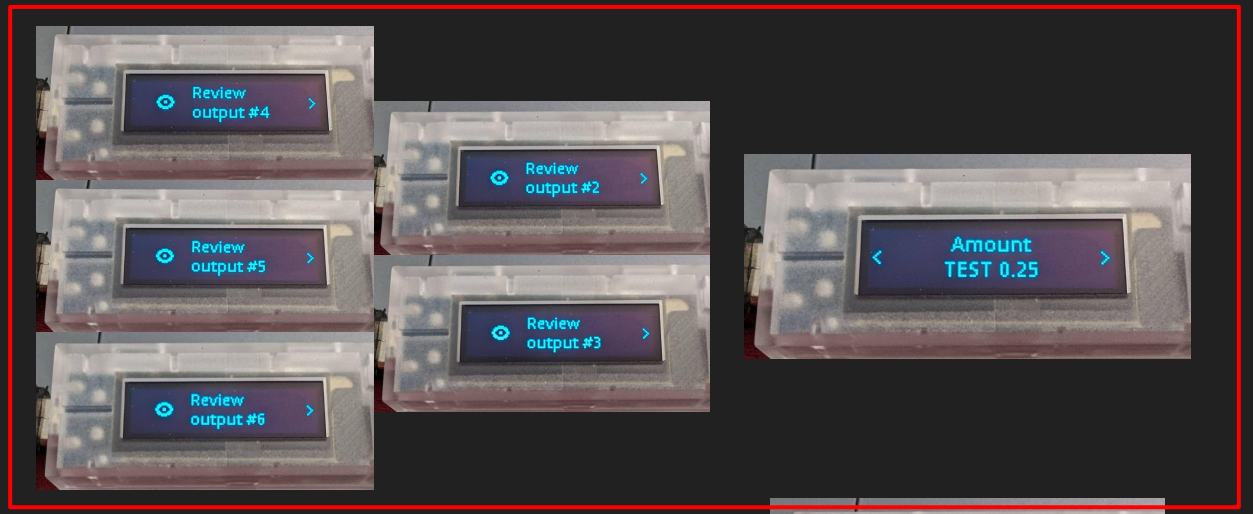


Coinjoin: Zoe's perspective

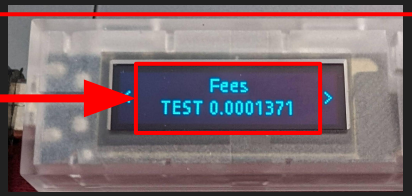
Review ALL 5 equal-size output addrs



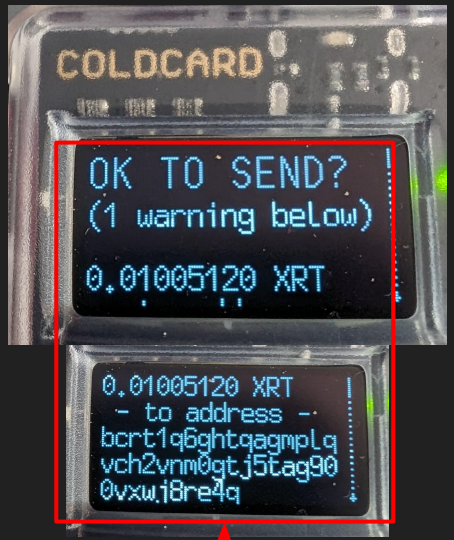
Malcolm's change



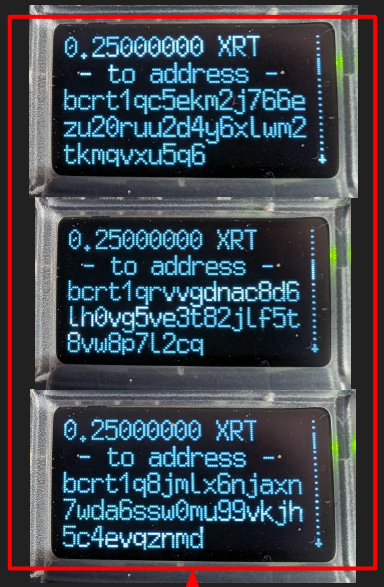
Is Zoe paying all the fees?



Coinjoin: Zoe's perspective

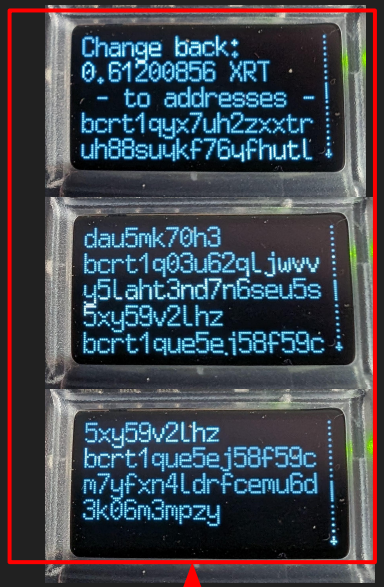


Malcolm's change



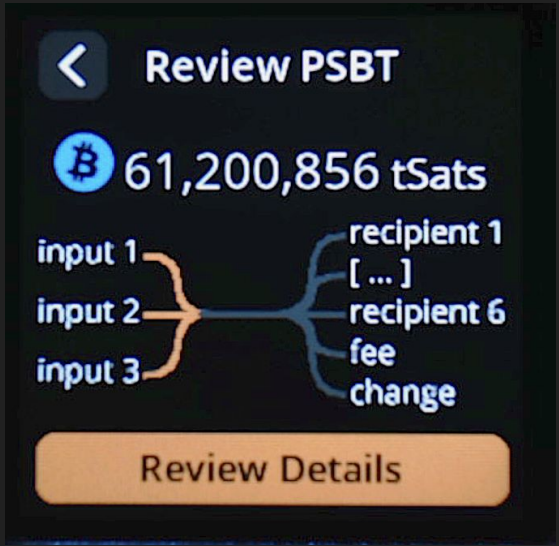
Malcolm's equal-size outputs

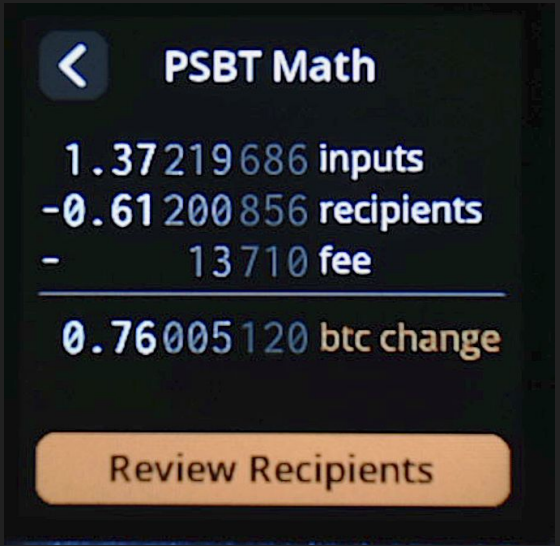
Is Zoe paying all the fees?



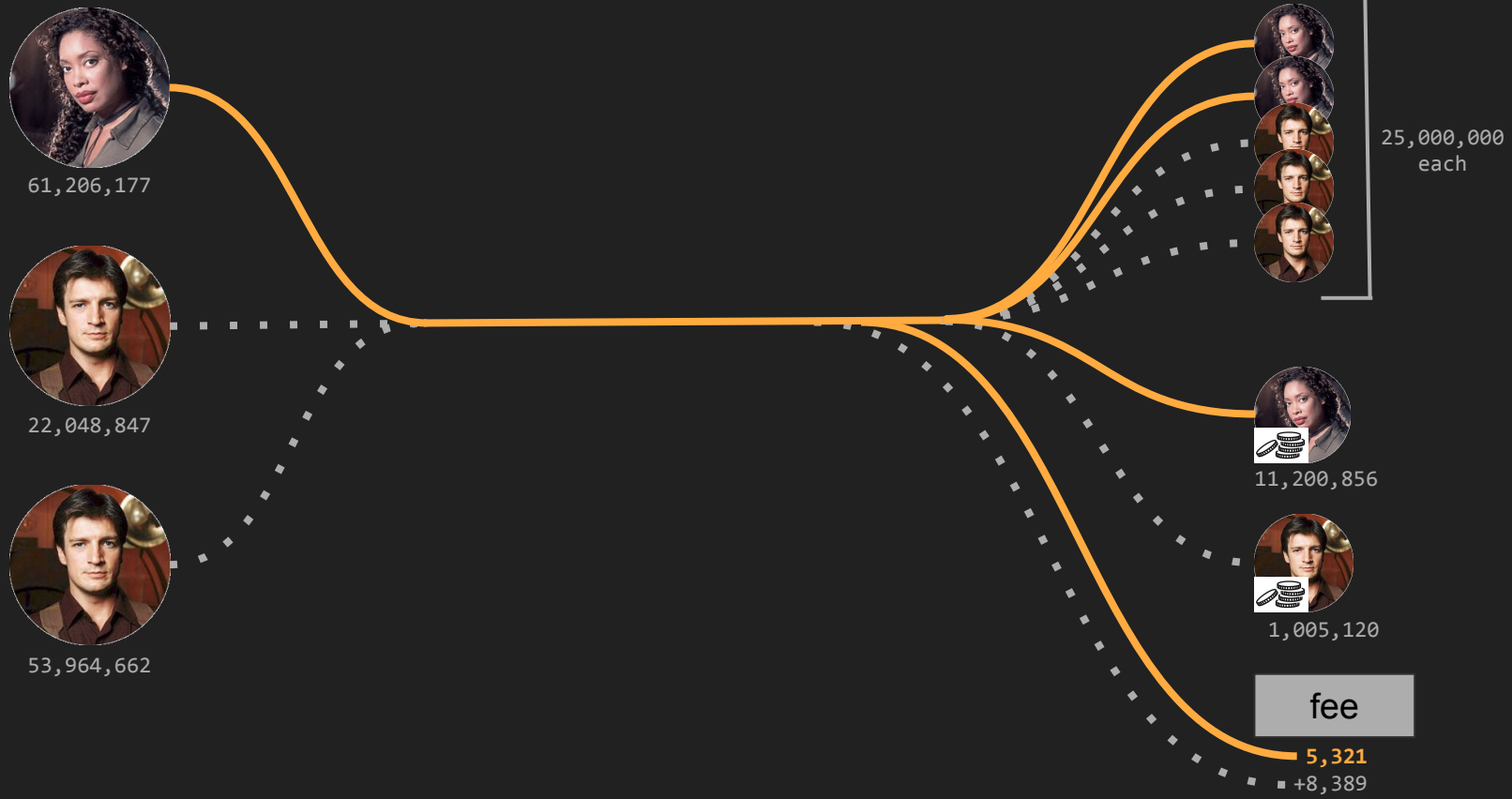
Zoe's equal-size outputs + change

…Womp, Womp… 😢😢😢

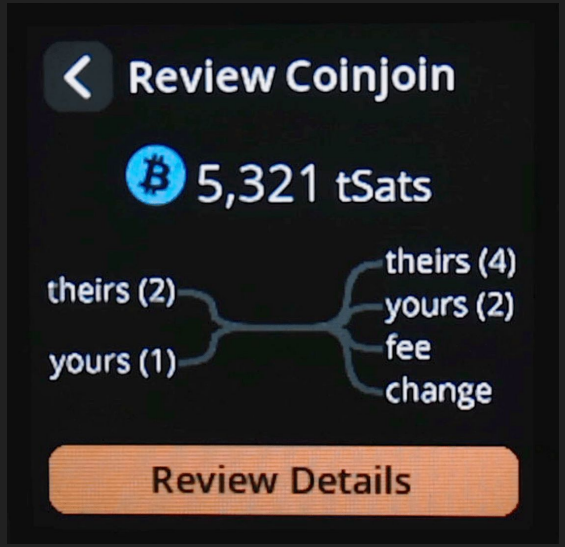

Review PSBT
61,200,856 tSats
input 1
input 2
input 3
recipient 1
[...]
recipient 6
fee
change
Review Details


PSBT Math
1.37219686 inputs
-0.61200856 recipients
- 13710 fee
0.76005120 btc change
Review Recipients

Zoe’s Perspective

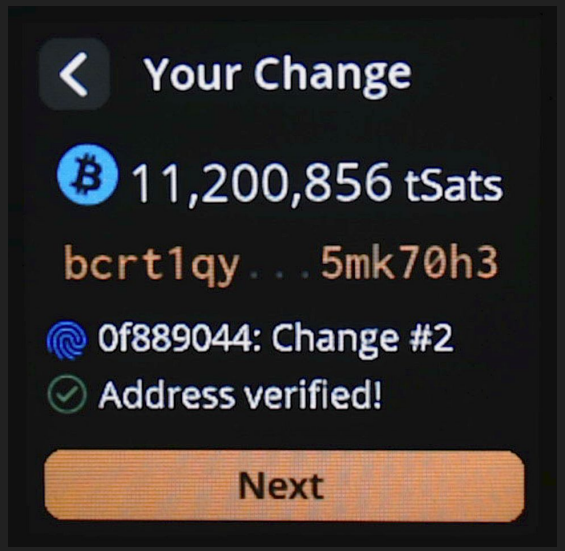


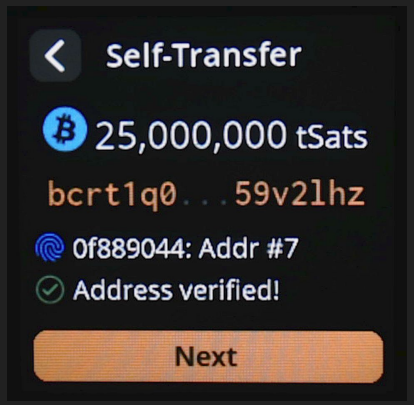
Work-in-Progress: SeedSigner coinjoin

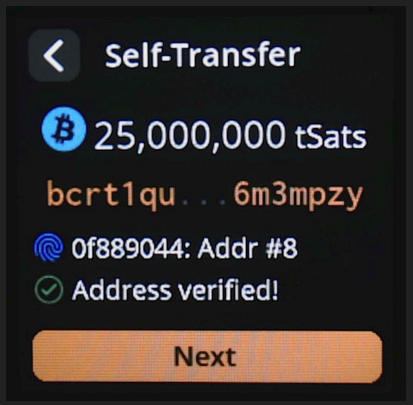


Work-in-Progress: SeedSigner coinjoin

Work-in-Progress: SeedSigner coinjoin







Some tx contexts are unknowable

Work-in-Progress: SeedSigner complex cooperative spend

Cooperative spend cheat sheet

Given a tx with 1+ input from you and 1+ external input…

- Payjoin receive: your outputs > your inputs
- Payjoin send: your inputs = (their outputs - their inputs) + fee
- Coinjoin(?): your inputs - your outputs* <= fee
  - **(where 1+ of your outputs is the same size as 1+ "their" outputs)*
- Complex / Ambiguous(???): your inputs - your outputs > fee

Payjoin / Coinjoin support

Via hot wallets

- Payjoin
  - Samourai
  - BlueWallet
  - btcpay server
- Coinjoin
  - Samourai
  - Wasabi
  - Sparrow
  - JoinMarket/JAM

Via HWWs / signers

- Software:
  - 😢
- Hardware:
  - SeedSigner (R&D branch)
  - 😢