Could anyone advise me if you know “How to aggregate sigs for swapTx on Plasma Cashflow”?

My insights are below.

PatternA) I’ve considered an “unsigned Tx sharing scheme” via libp2p/whisper. This swap Tx is completely same form with Cashflow’s swap. Then Alice shares it with her sign only. Then Bob receive it via p2p channel, and sign it. But for initial phase of the plapp(plasma app), libp2p’s nodes would be almost centralized by the op, in this case I’m still not sure what this centralization causes.

PatternB) This is a bit different Tx form from Cashflow’s swap. Alice build LockedOrderTXO. In other words, Alice can create signed Tx which includes coinA inside, plus, needs coinB + Bob’s sig to unlock coinA. And it’ll be included to block. Then Bob can confirm&sign to the Alice-initiated-swap-Tx(unlock coinA and send coinB). Now sigs are filled to Tx. But still there’s a scenario which enable Bob(op) to game the “force include”, but I won’t dig further because my concern is concrete preparation process of two inputs for swapTx.

Relevant Part

[

IMG_20181112_083814

1080×1195 94.5 KB

](https://ethresear.ch/uploads/default/original/2X/e/e1ea2155e1f1de2001ecff0b090cc7faf7f84805.jpeg)

https://hackmd.io/DgzmJIRjSzCYvl4lUjZXNQ?view