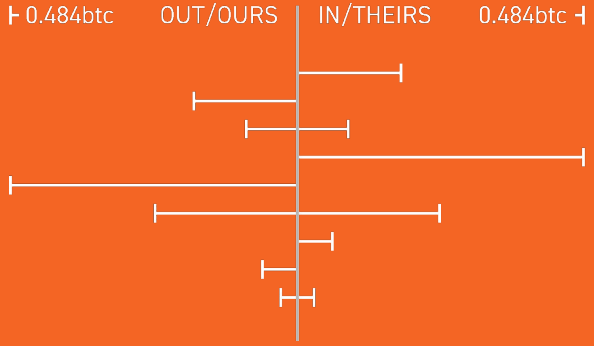
PEERSWAP

Richard Myers • 30.07.2022 • BitDevs LA

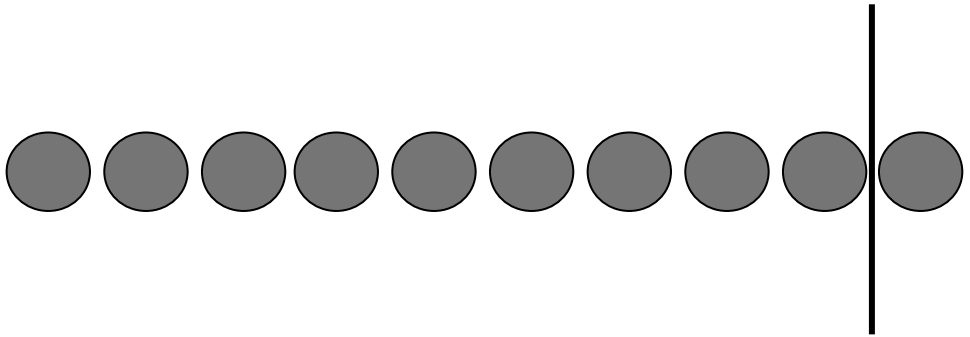

PeerSwap
Decentralized P2P LN Balan ng Protocol

Problem

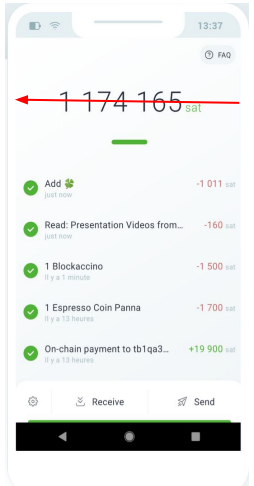


Unbalanced Channels: End User

Their Balance



Our Balance

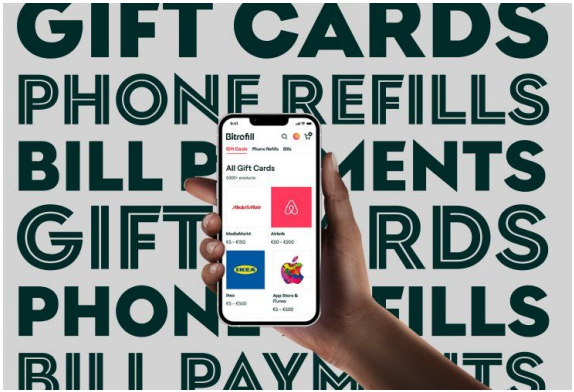


- Spend Only
- No Routing
- No Receiving

Unbalanced Channels: Merchant

Our Balance

Their Balance

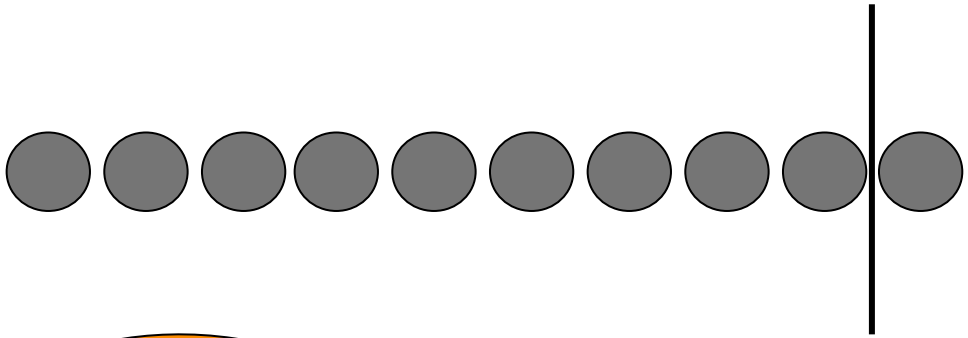


- Receive Only
- No Routing
- No Spending

Unbalanced Channels: Routing Nodes

Our Balance

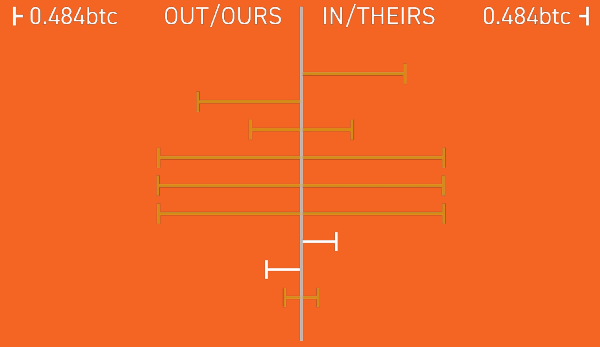
Their Balance



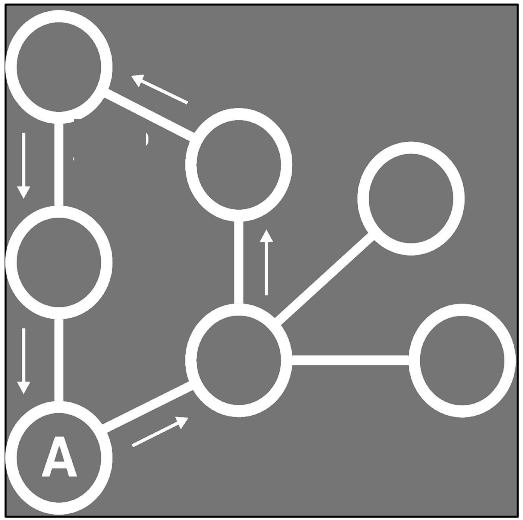
Advertise Total Capacity!

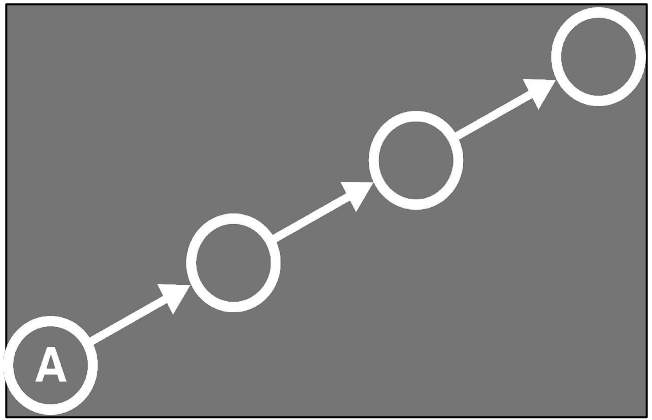
Routing Failures →
Lower Routing Fees +
Unused Liquidity

Solutions

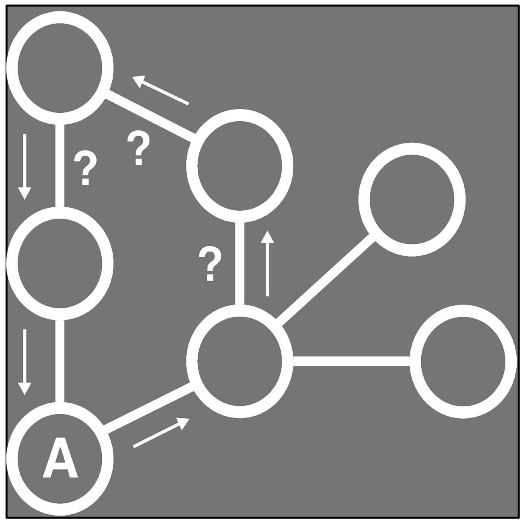


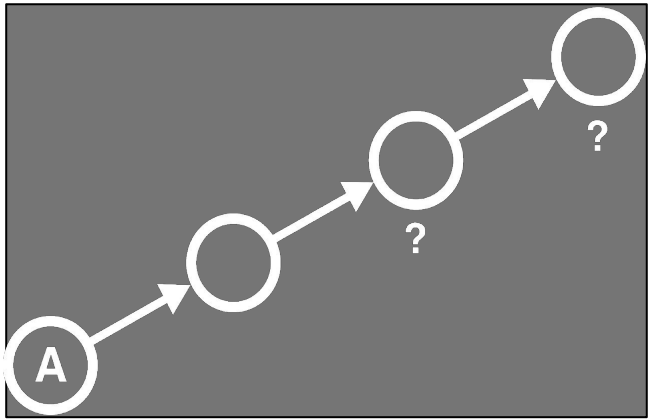
Multihop Rebalancing



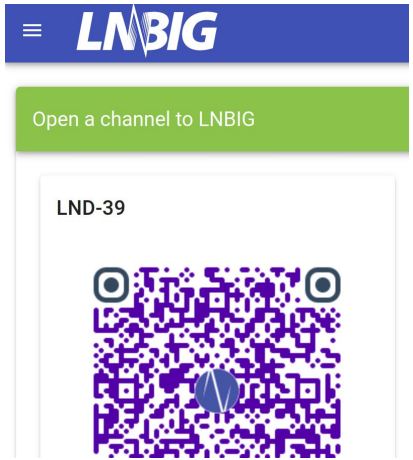


Multihop Rebalancing

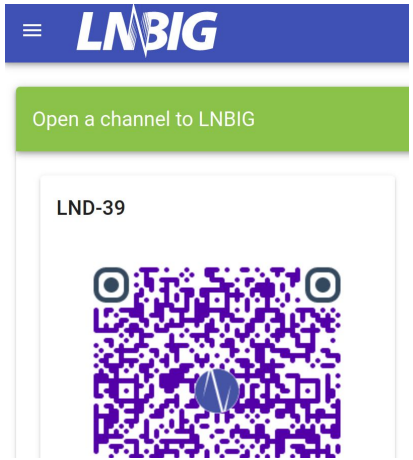




Open New Outbound Channels



Open New Outbound Channels



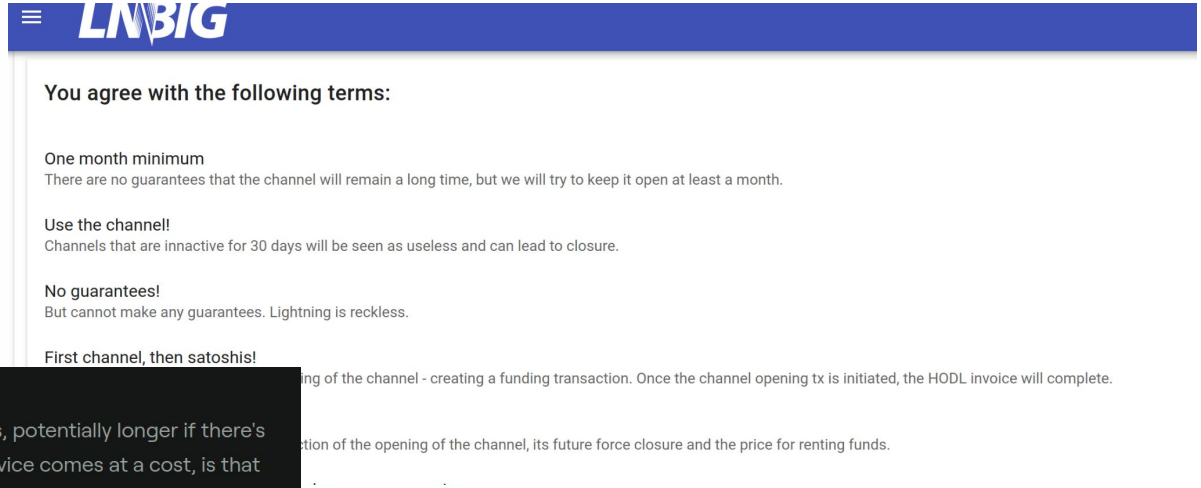
- On-chain tx fees
- Minimize size
- More in hot wallet
- Close old channel
- More tx fees

Buy New Inbound Liquidity

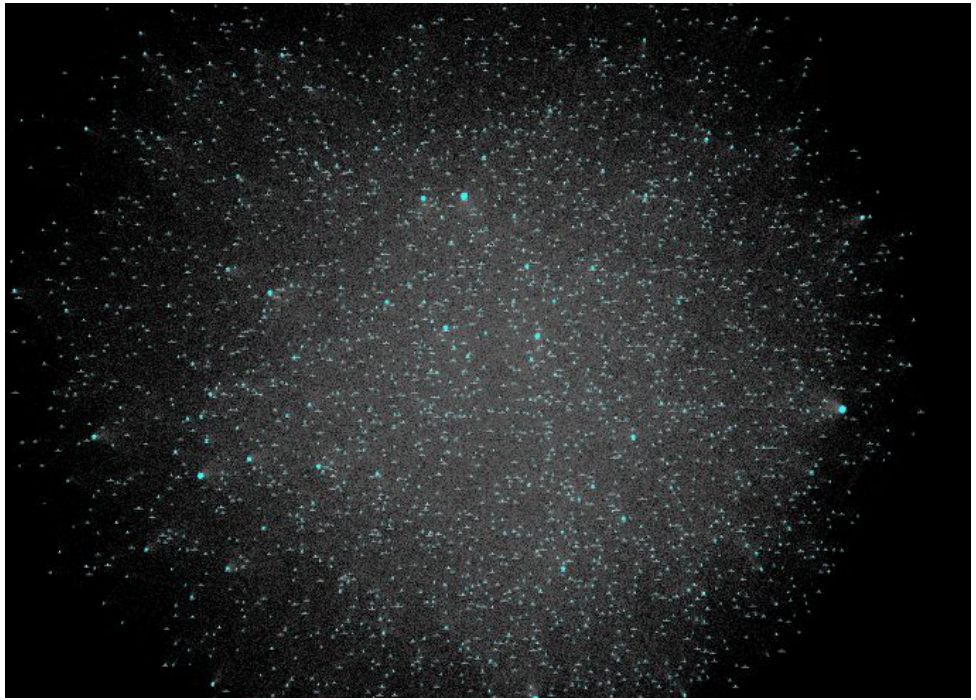
Buy New Inbound Liquidity

What are the limitations?

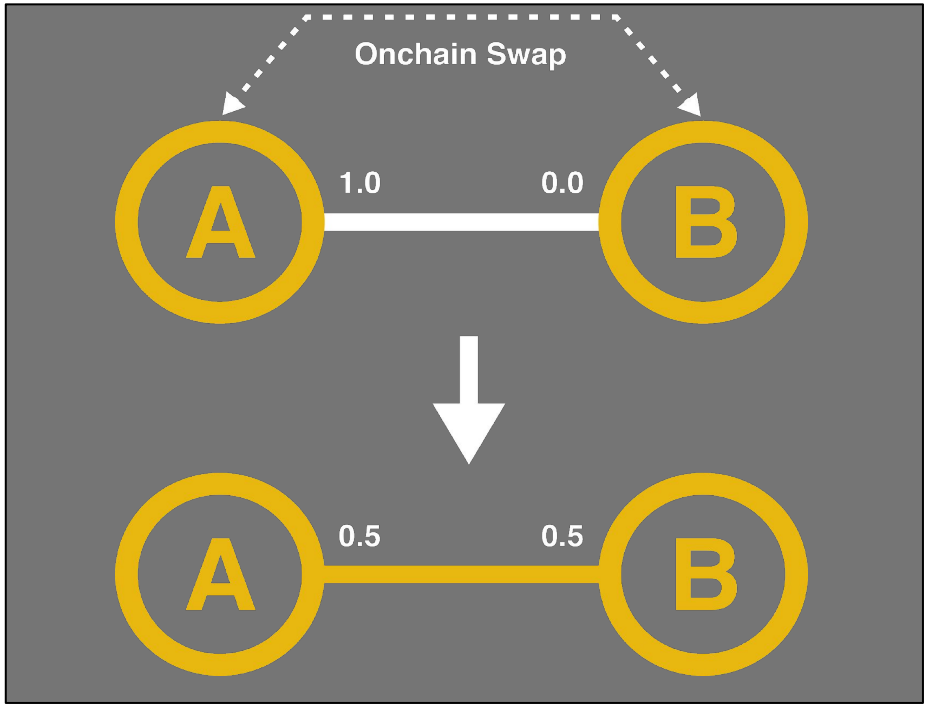
Each Thor channel will be kept open on our side for 30 days, potentially longer if there's activity on it. The reason for this limitation, and why this service comes at a cost, is that opening an empty channel requires us to lock up our bitcoin into your channel and keep them there.



Risks: Centralization, Censorship



PeerSwap



PeerSwap: Reliable

- **Simple - works with existing LN nodes of today.**
- **Lowest cost balancing and rebalancing.**
- **Reliable because of single hop.**
- Fully P2P and decentralized. No coordinator. No 3rd party data collection.
- Don’t need to open yet more channels for balancing
  - Reduces Hot Wallet Risk.
  - Reduces Cost of Capital.
    - More channels == More unproductive
- Reduces need to pay for incoming capacity.
- End-users don’t need to open new channels if they don’t want to!

PeerSwap: Decentralized

- Simple - works with existing LN nodes of today.
- Lowest cost balancing and rebalancing.
- Reliable because of single hop.
- **Fully P2P and decentralized. No coordinator. No 3rd party data collection.**
- Don’t need to open yet more channels for balancing
  - Reduces Hot Wallet Risk.
  - Reduces Cost of Capital.
    - More channels == More unproductive
- Reduces need to pay for incoming capacity.
- End-users don’t need to open new channels if they don’t want to!

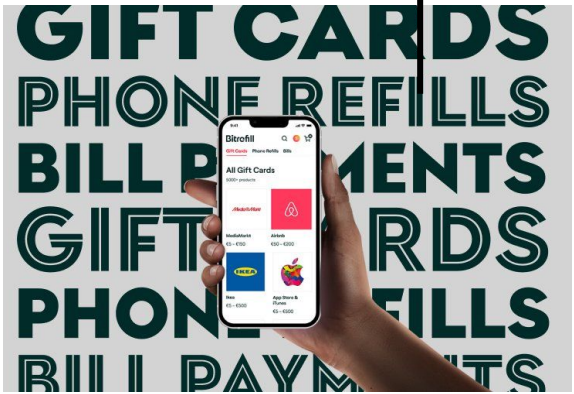
PeerSwap: Lower Cost

- Simple - works with existing LN nodes of today.
- Lowest cost balancing and rebalancing.
- Reliable because of single hop.
- Fully P2P and decentralized. No coordinator. No 3rd party data collection.
- **Don’t need to open yet more channels for balancing**
  - **Reduces Hot Wallet Risk.**
  - **Reduces Cost of Capital.**
    - **More channels == More unproductive**
- **Reduces need to pay for incoming capacity.**
- **End-users don’t need to open new channels if they don’t want to!**

PeerSwap: Merchant Example

Our Balance

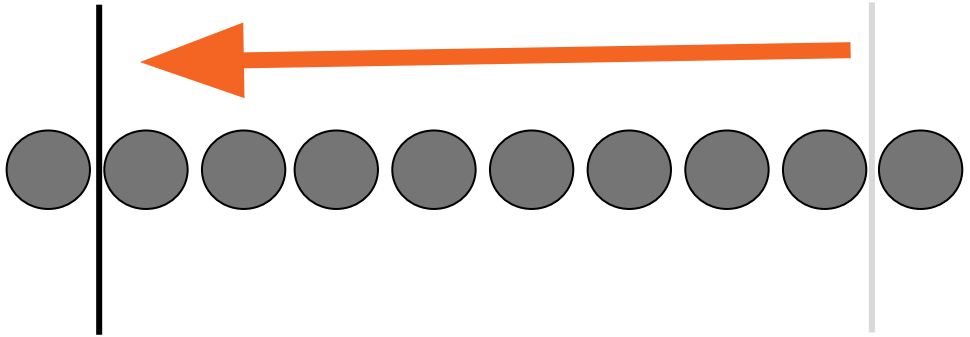
Their Balance



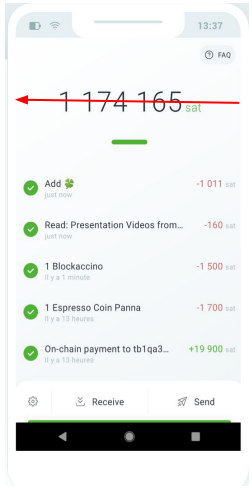
- Create incoming liquidity from peer
- Receive on-chain Bitcoin from peer

PeerSwap: End User Example

Their Balance



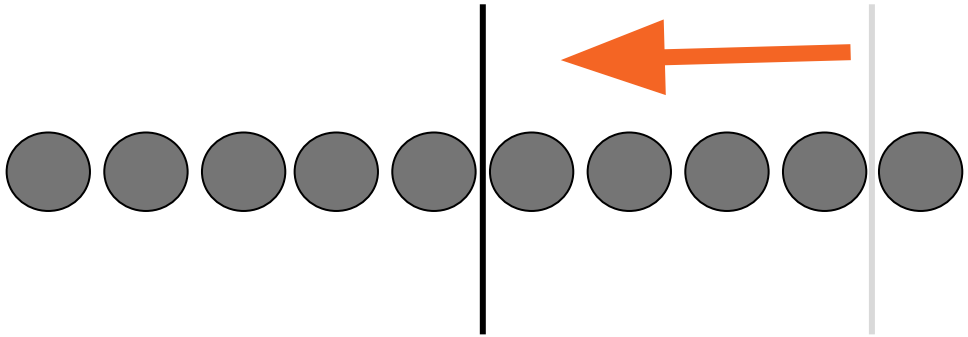
Our Balance



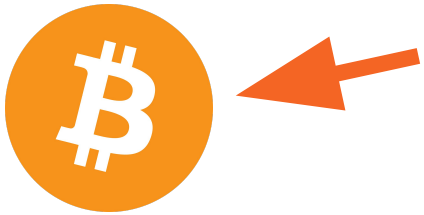
- Create outgoing liquidity to peer
- Send on-chain Bitcoin to peer

PeerSwap: Routing Node Example

Their Balance



Our Balance



- Rebalance liquidity between peers
- Shift balance from hot wallet to offline storage

Current Status

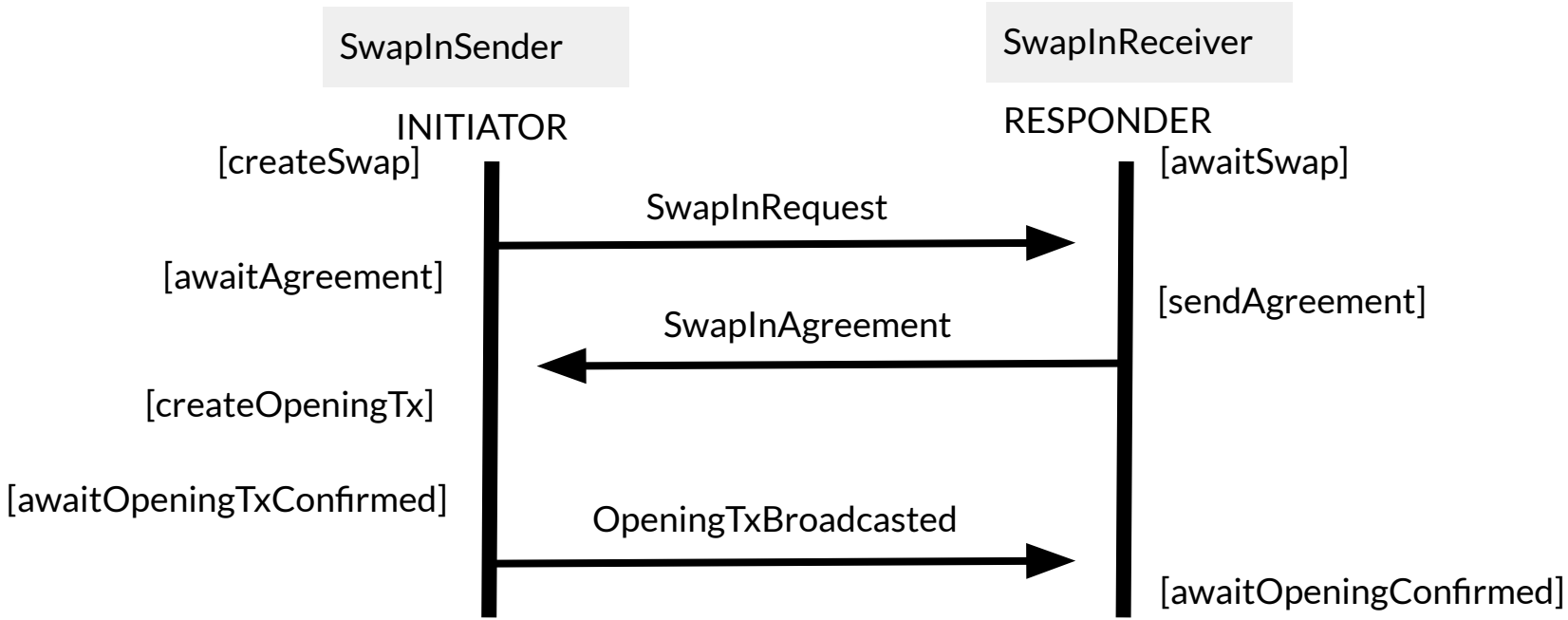
Plugins + Signet

github.com/ElementsProject/peerswap

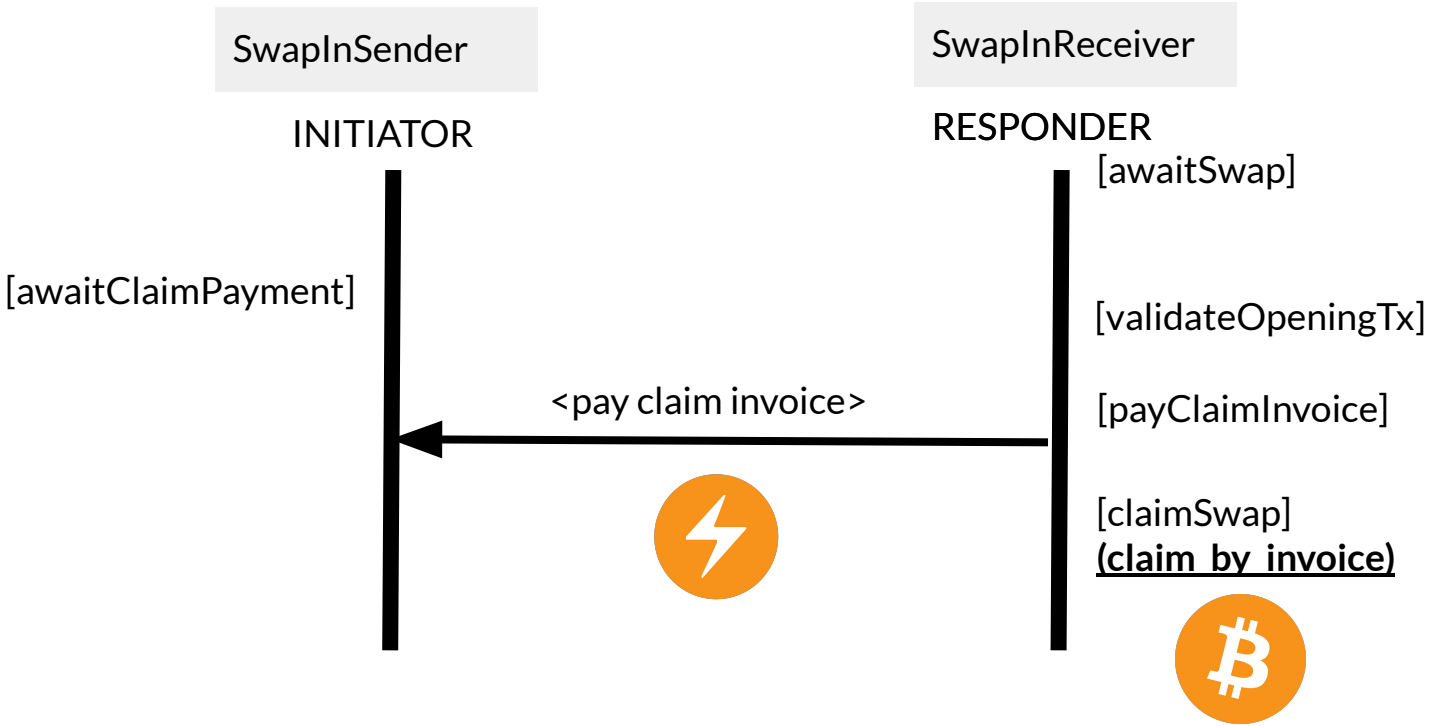
CORE LIGHTNING

How Does it Work

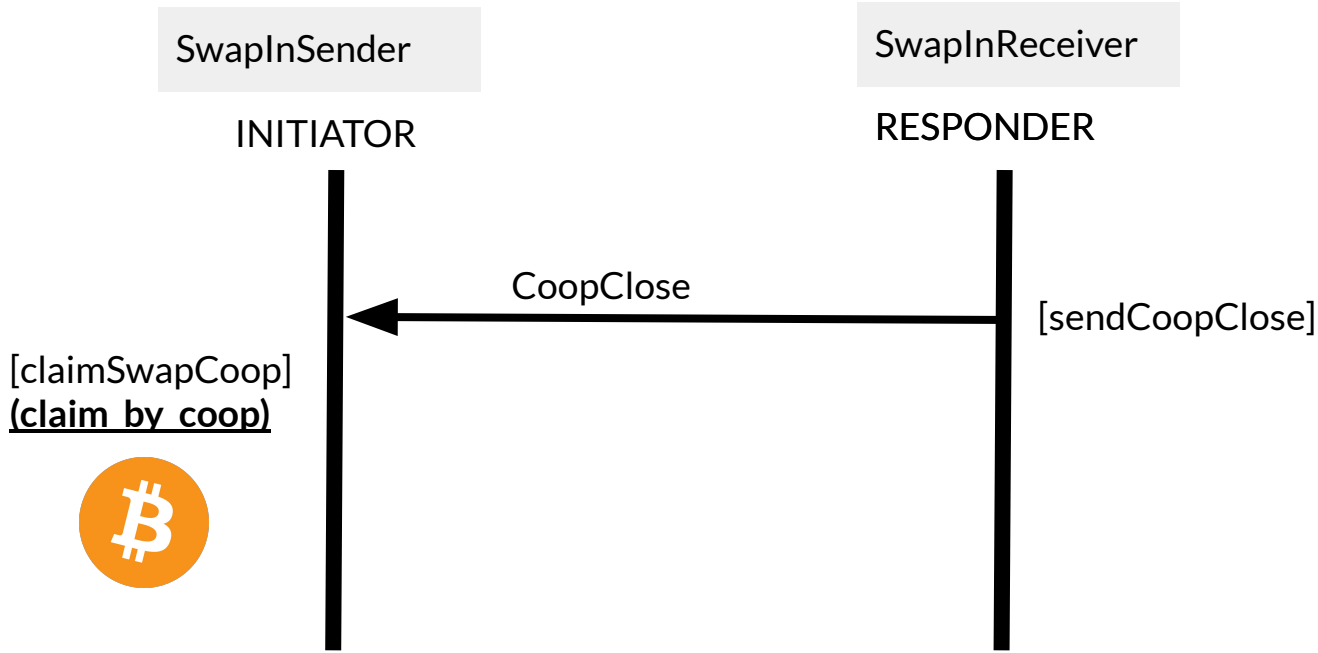
PeerSwap: Initiate Swap-In



PeerSwap: Claim with Preimage



PeerSwap: Refund Cooperatively



PeerSwap: Refund After Timeout

SwapInSender

INITIATOR

[waitCsv]

[claimSwapCsv]
(claim_by_csv)

SwapInReceiver

RESPONDER

Future

- Taproot
- Non-BTC swaps (LUSD-T)
- More implementations (Eclair)

Open Issues

- Security without allow list, DoS ?
- Premium/ pricing

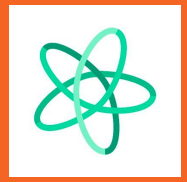
More Information

https://www.peerswap.dev

https://www.youtube.com/watch?v=onMVDsoCniU

Thank You

- Blockstream: Warren Togami, Konstatin Nick
- ACINQ



Questions

PeerSwap helps create a more censorship resistant and robust Lightning Network