PeerSwap

Decentralized P2P LN Balancing Protocol

Blockstream

WARREN TOGAMI

VP Solutions @ **Blockstream**

Founder @ **Fedora Linux**

Former Engineer @ **Red Hat**

Twitter @**wtogami**

KONSTANTIN NICK

Lead Developer of **PeerSwap**

Founder @ **Donnerlab**

Contractor @ **Blockstream**

Twitter @**sputn1ck**

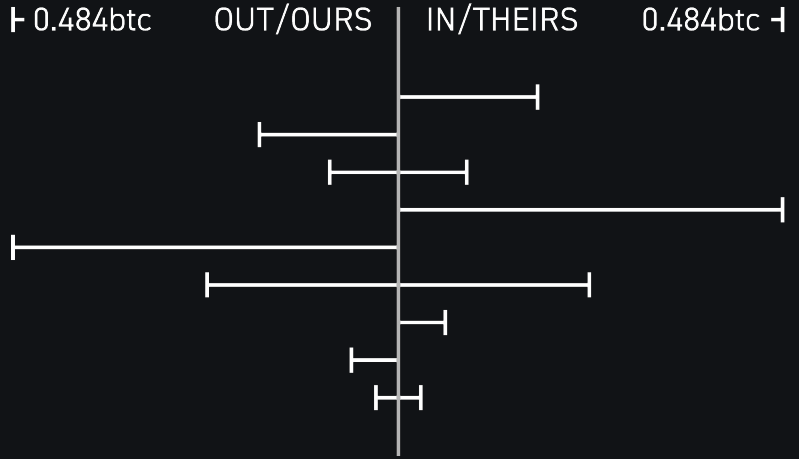
PEERSWAP

Contents

PEERSWAP

Most Difficult Problem: LN Channel Balancing

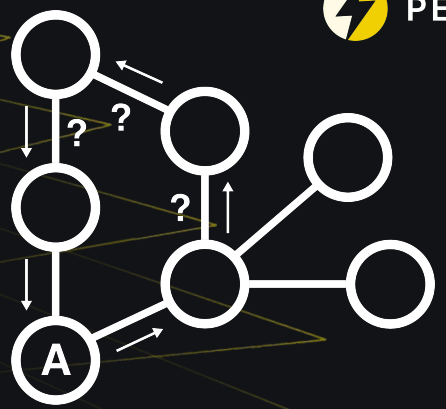
- Most capital tied up in LN channels is stuck forever in unbalanced channels.
- Unbalanced channels are significantly less productive. Routing algorithms remember failures and try them less often.
- Most people want channels to be balanced at 50%.
- Most existing guides encourage opening more channels as the “solution”.
- Most existing solutions utilize multi-hop routes.



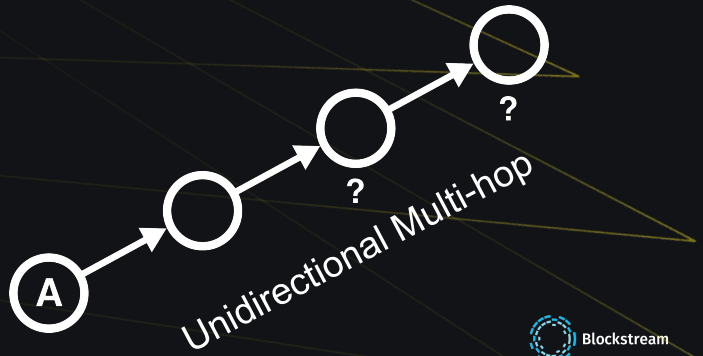
Blockstream

Multi-Hop Balancing Considered Harmful

- Most existing solutions utilize multi-hop routes to balance your immediate channels.
- Multi-hop is very unreliable because …
  - By design you don't know what the capacity is of other nodes.
  - Often balancing your own channel causes other node's channels to become unbalanced.
  - Cooperative circular balancing can be zero cost and beneficial - but this is rare and labor intensive.
  - Unsolicited (normal) circular balancing is parasitic.
    - Nodes who charge a higher proportional feerate prey upon any available liquidity of lesser priced competitors - otherwise known as victims.
- Ultimately can't escape the zero sum game.
  - Need some other method that does not add to the overall problem.



Parasitic Circular Multi-hop

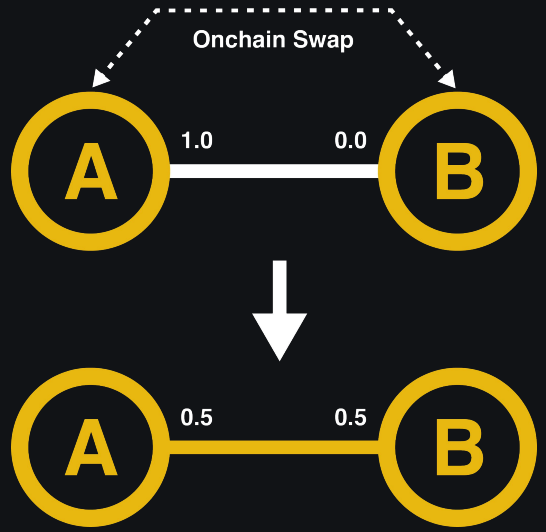


Unidirectional Multi-hop

PEERSWAP

What does PeerSwap do?

- On-chain atomic swap negotiated over custommessage with direct peers.
- Opposite approach to most existing balancing methods.
  - Balance channel only with direct peers - reliable.
  - Rather than opening more and bigger channels, you can cheaply refill channels you already have to the desired balance.
  - Fixes balance without harming other nodes.
- Opening new channels is recommended not for the purpose of balancing, but if you want a more direct connection with a frequent source/destination node.
- Multiple optional swap types.
  - Currently BTC & L-BTC onchain swaps.
  - Additional wallet options coming.

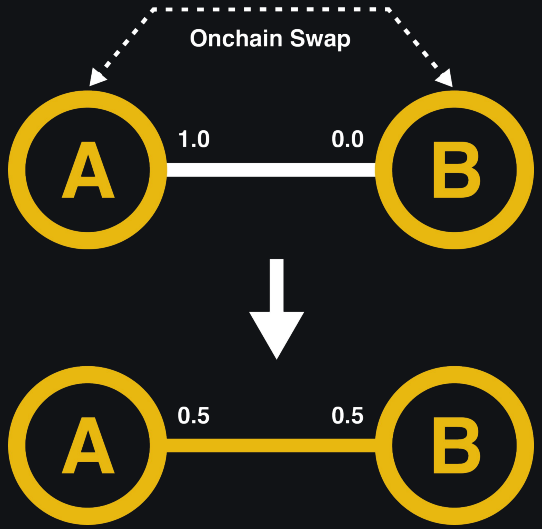


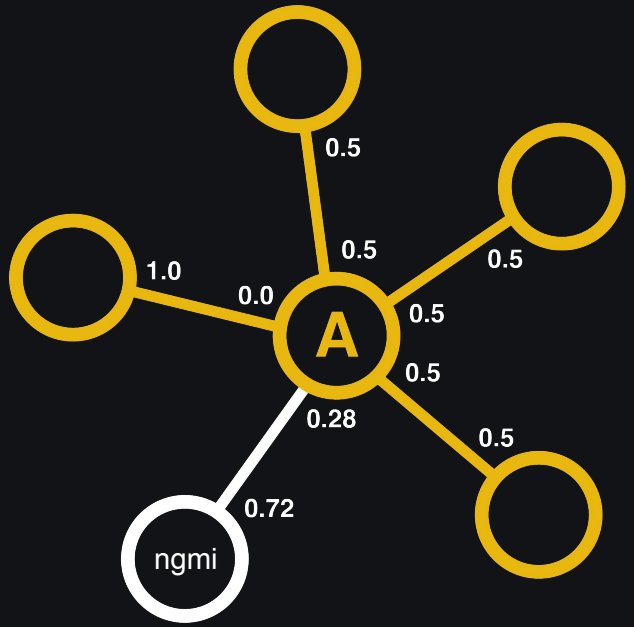
Blockstream

PEERSWAP

WHAT DOES PEERSWAP DO?

- Balance channels only with direct peers.
- Repeatedly refill channels to the desired balance.

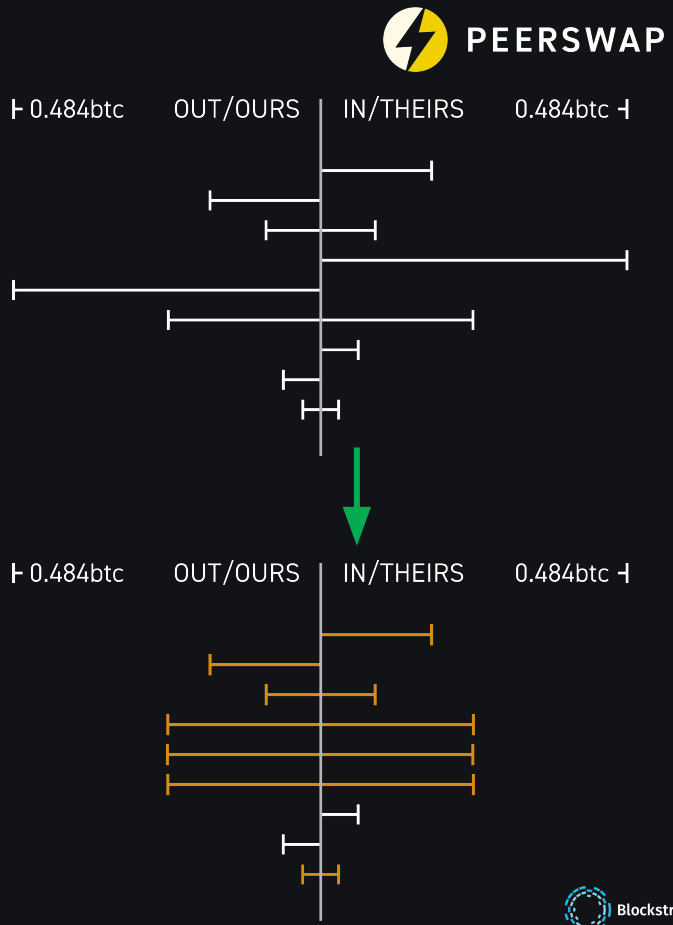




Blockstream

Benefits of PeerSwap

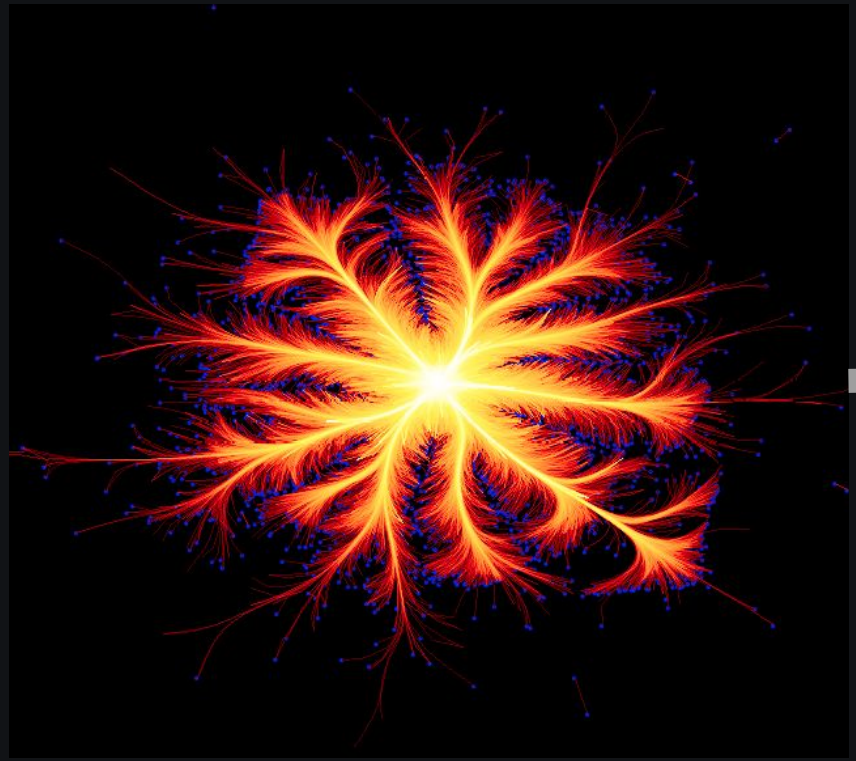
- Simple - works with existing LN nodes of today.
- Lowest cost balancing and rebalancing.
- Reliable because of single hop.
- Fully P2P and decentralized. No coordinator.
- Don’t need to open channels for balancing
  - Reduces Hot Wallet Risk.
  - Reduces Cost of Capital.
    - More channels == More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



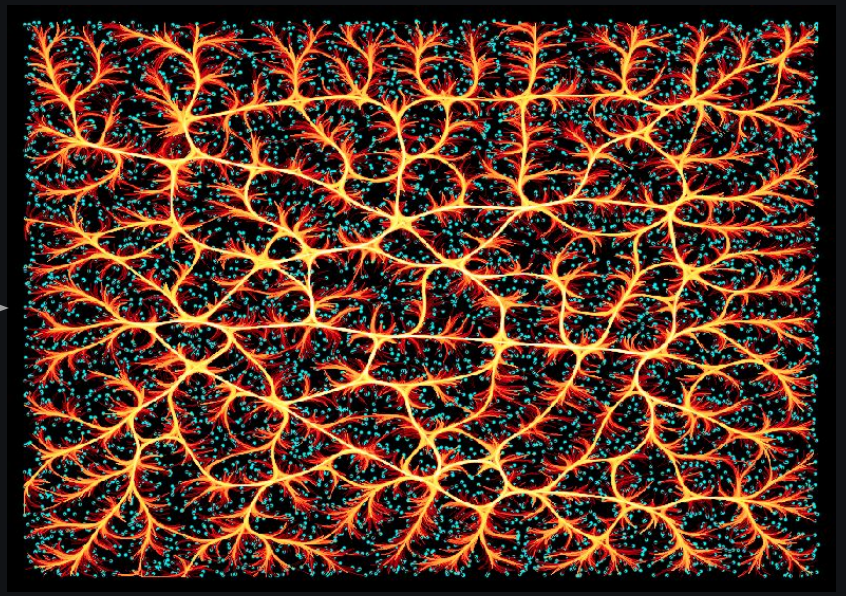
Blockstream

Benefit: Decentralize Topology of the Lightning Network

PEERSWAP



Force Directed Layout - Weighted by channel size



Random Layout

Credit: Twitter @pymoment November 3rd, 2021
https://twitter.com/pymoment/status/1456099385411084288

Blockstream

Balancing Solutions Comparison

PEERSWAP

	Decentralized	Reliability	Cost	Ease of Use	Privity	UTXO Privacy	Status
Circular Route	✓	multihop ✗	$	Manual ✗	✓	✓	Requires multi-human intervention ✗
Lightning Loop	✗	multihop ✗	$$	✓	✓	😐	Production service ✓
Lightning Pool	✗	✓	$$$	✓	😐	😐	Production service ✓
Liquidity Ads	✓	✓	$$$	Needs UX 😐	✓	✓	C-Lightning deployed draft specification
Boltz.exchange	✗	multihop ✗	$$$	✓	😐	😐	Production service ✓
Dual Funding	✓	✓	$	Needs UX 😐	✓	✗	Balanced only once at opening
Splicing	✓	?	$$	Needs UX ?	✓	✗	High Complexity, Not yet implemented ✗
PeerSwap	✓	✓	$	Needs UX 😐	✓	✓	CLN/LND prototype and draft specification

PeerSwap Swaps

or(and(pk(A), or(pk(B),sha256(H))),and(pk(B),after(N)))

and(pk(A), sha256(H))
Signature of Alice and revealing Preimage

and(pk(A), pk(B))
Signature of Alice and Bob
Future Taproot Keypath

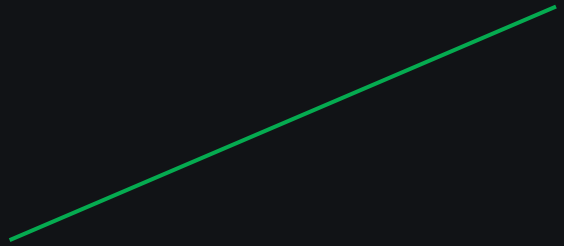
and(pk(B), after(N))
Signature of Bob, N Blocks after confirmation

PeerSwap Swaps

or(and(pk(A), or(pk(B),sha256(H))),and(pk(B),after(N)))

PeerSwap Swaps

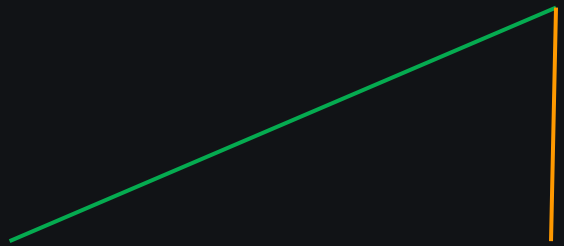
or(and(pk(A), or(pk(B),sha256(H))),and(pk(B),after(N)))



and(pk(A), sha256(H))
Signature of Alice and revealing Preimage

PeerSwap Swaps

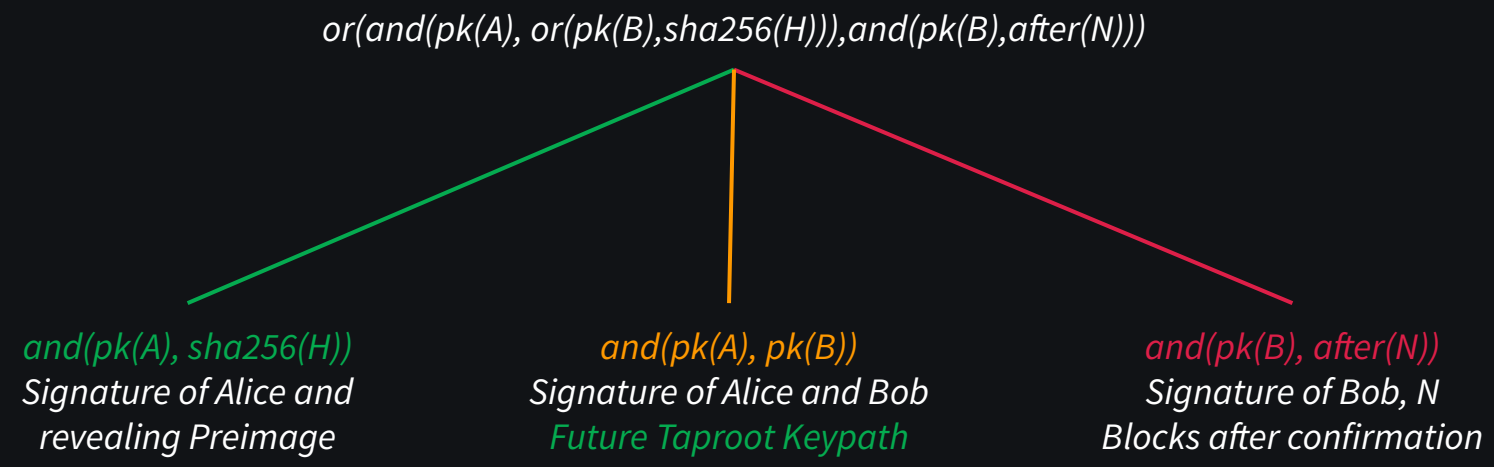
or(and(pk(A), or(pk(B),sha256(H))),and(pk(B),after(N)))



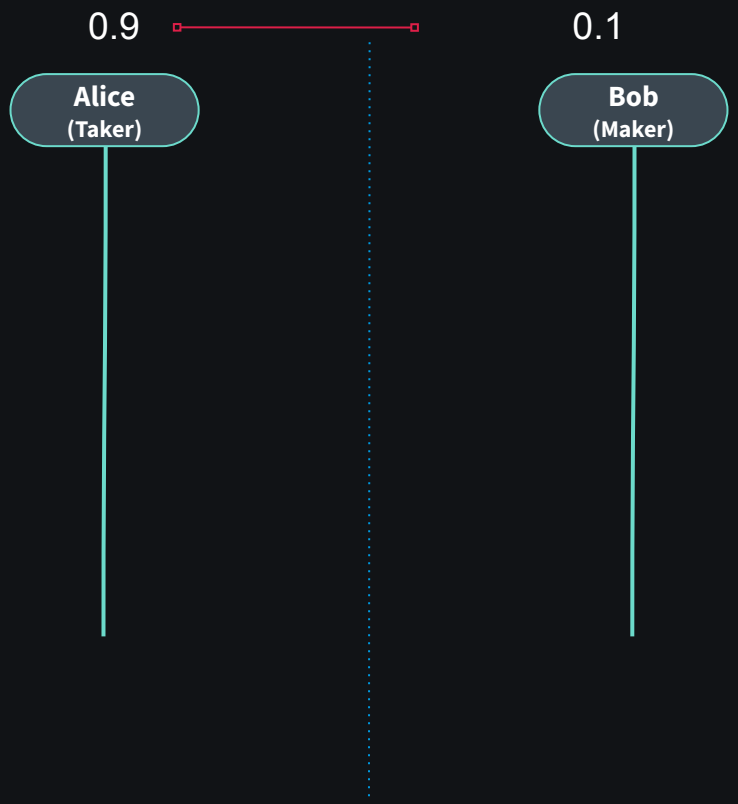
and(pk(A), sha256(H))
Signature of Alice and revealing Preimage

and(pk(A), pk(B))
Signature of Alice and Bob
Future Taproot Keypath

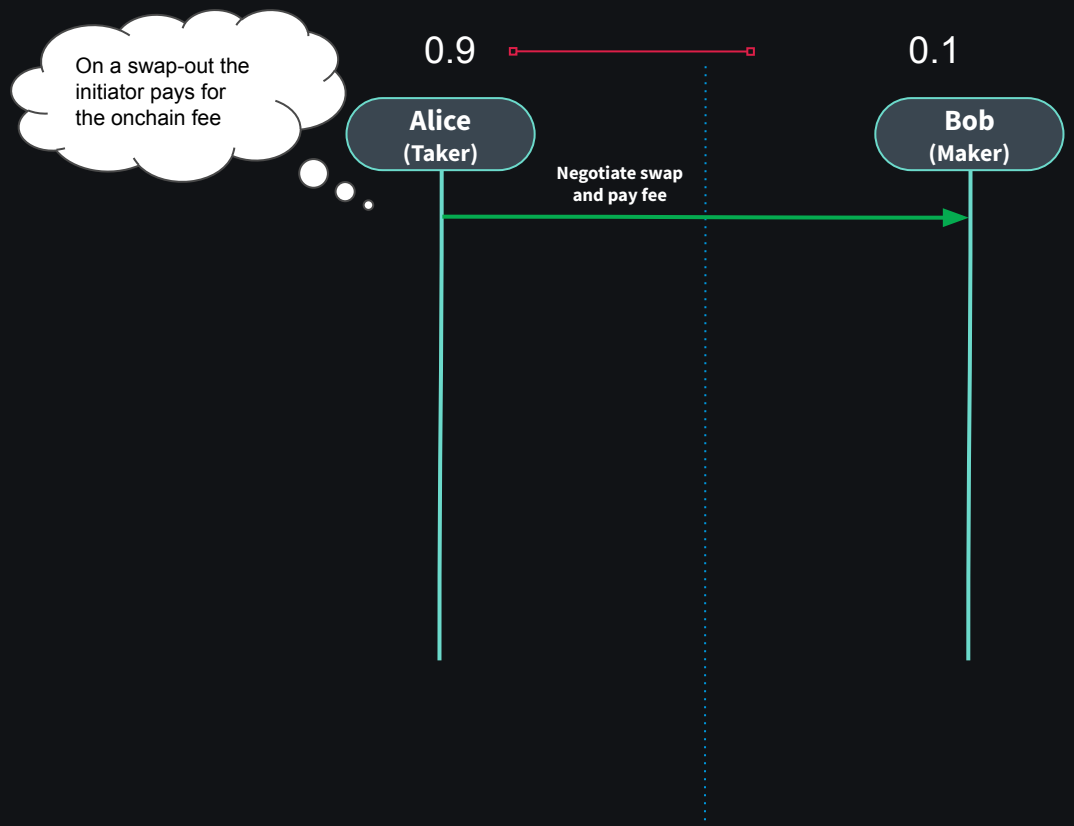
PeerSwap Swaps



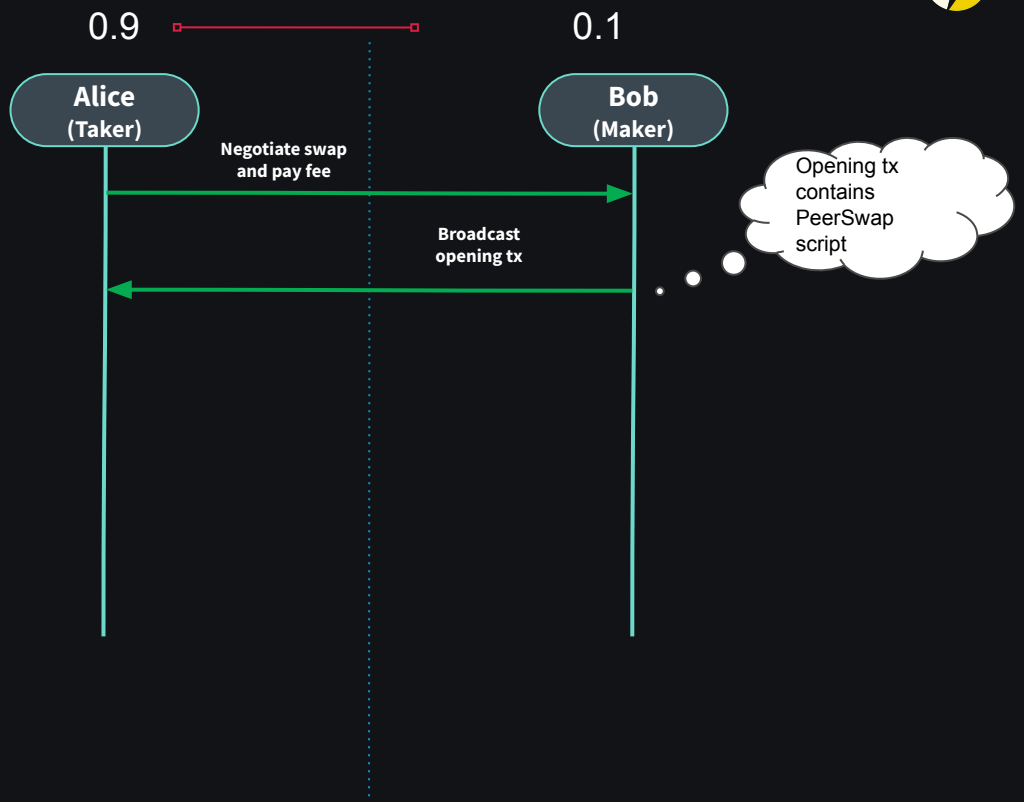
Swap-Out



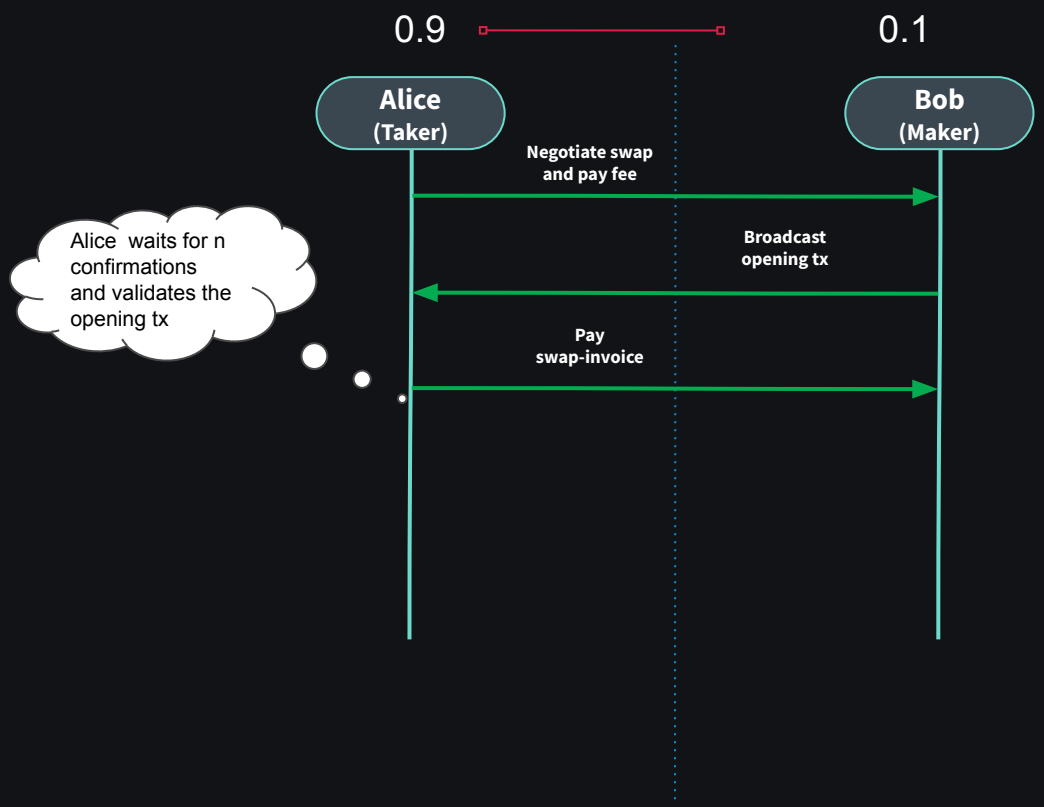
Swap-Out


On a swap-out the initiator pays for the onchain fee
0.9
0.1
Alice
(Taker)
Bob
(Maker)
Negotiate swap and pay fee

Swap-Out

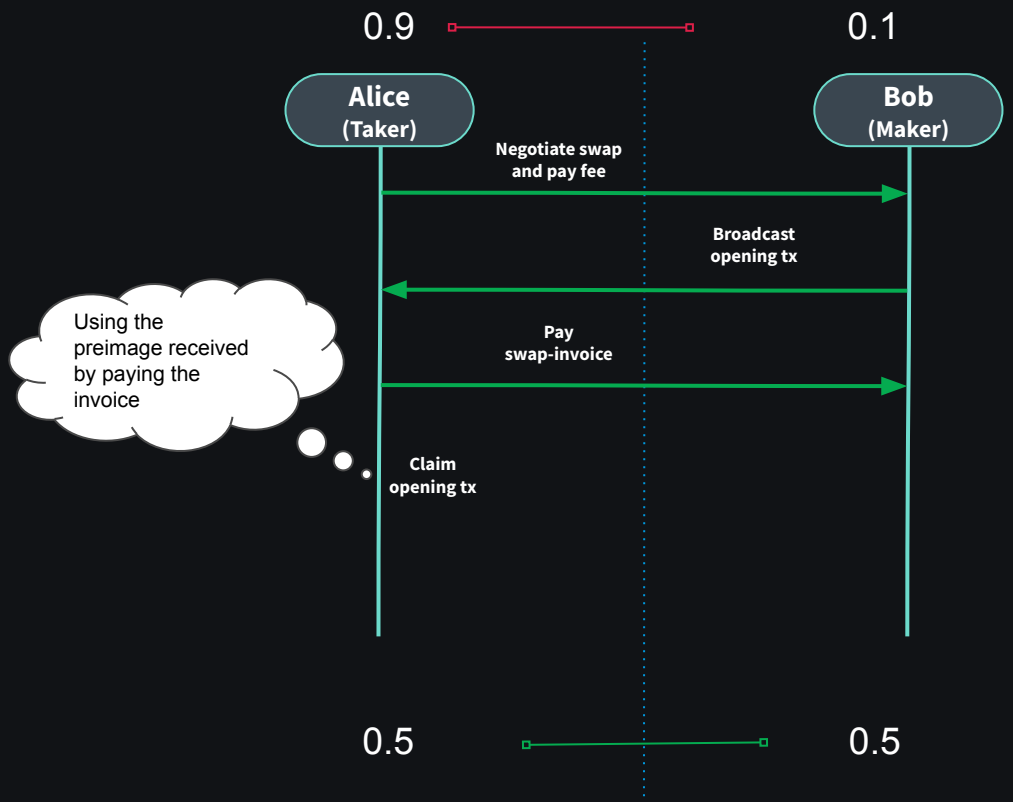

0.9
0.1
Alice
(Taker)
Bob
(Maker)
Negotiate swap
and pay fee
Broadcast
opening tx
Opening tx
contains
PeerSwap
script

Swap-Out


0.9
0.1
Alice
(Taker)
Bob
(Maker)
Negotiate swap
and pay fee
Broadcast
opening tx
Pay
swap-invoice
Alice waits for n
confirmations
and validates the
opening tx

Swap-Out

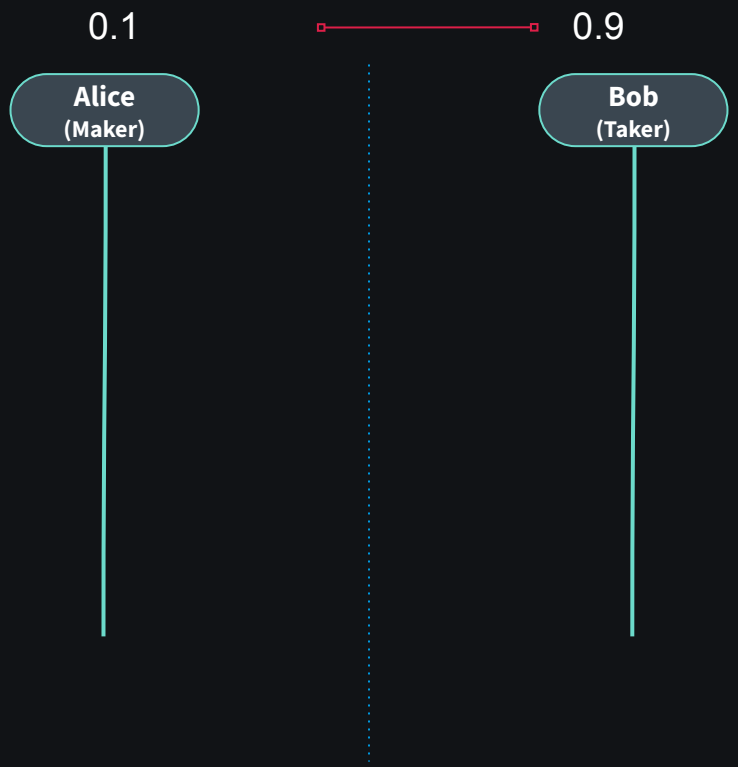
PEERSWAP



Blockstream

Swap-In

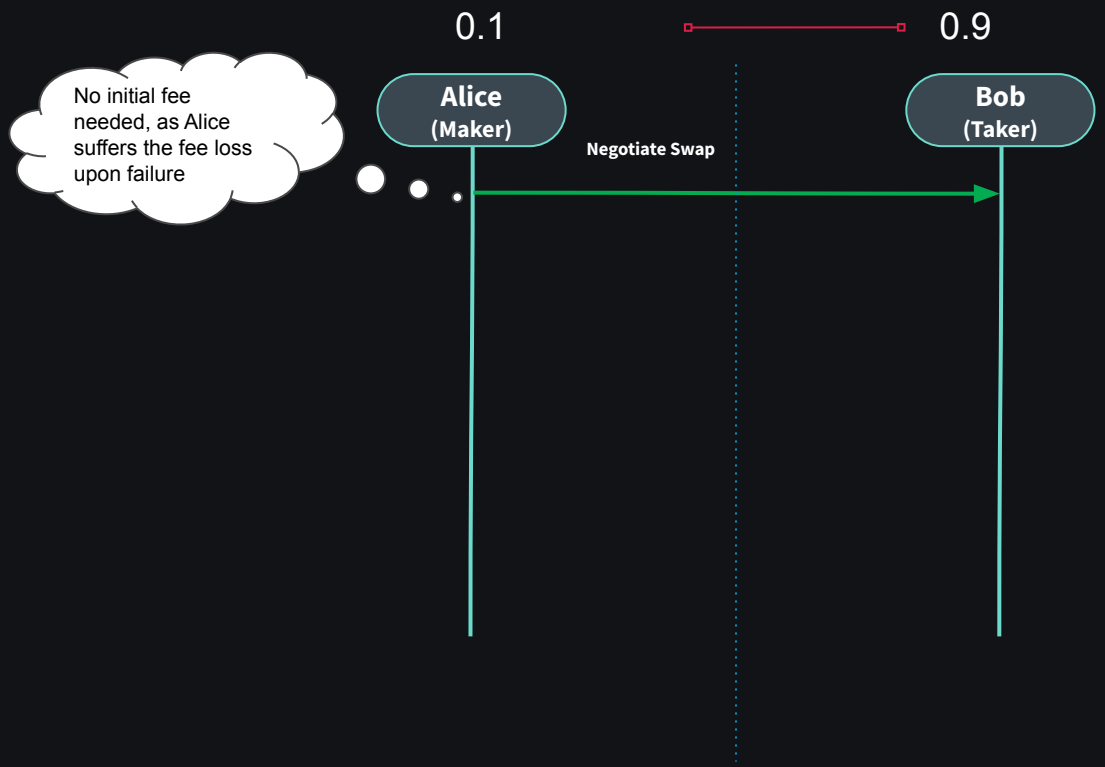
PEERSWAP



Blockstream

Swap-In

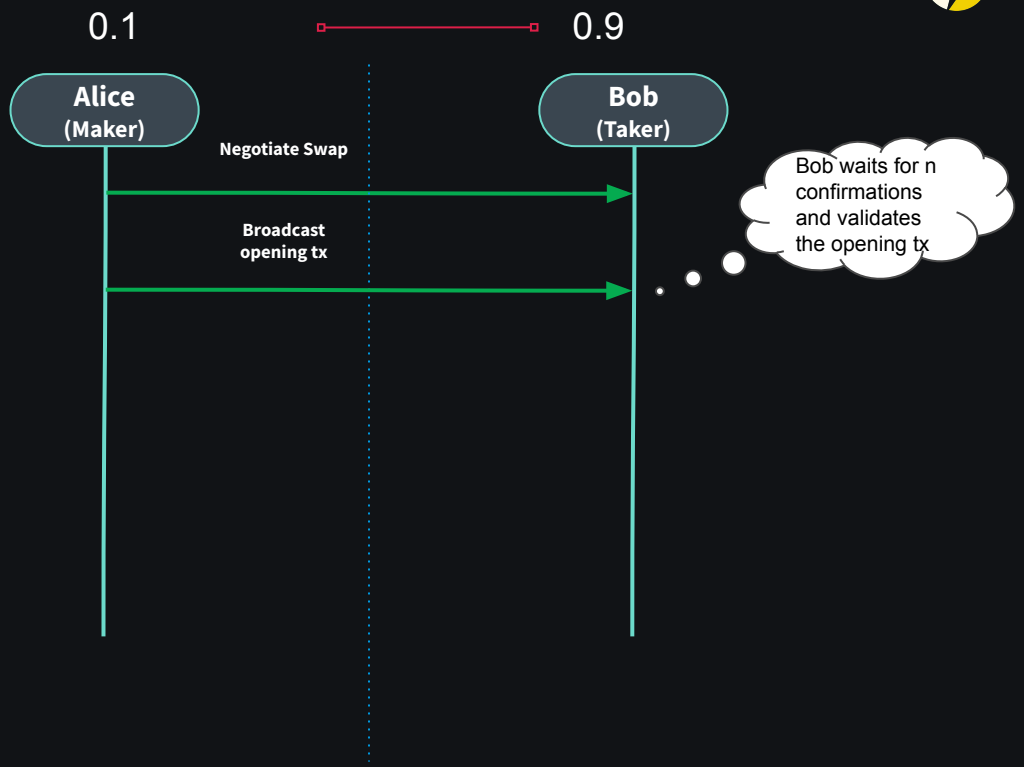
PEERSWAP



Blockstream

Swap-In

PEERSWAP



Blockstream

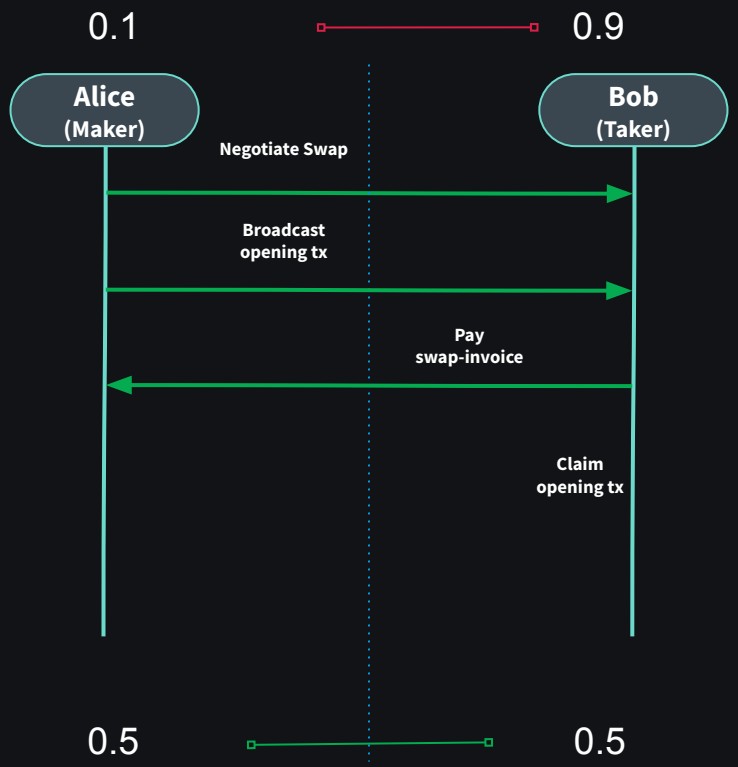
Swap-In

PEERSWAP

Blockstream

Swap-In

PEERSWAP



Blockstream

Types of Swaps

PEERSWAP

LIQUID NETWORK

	Bitcoin chain	Liquid chain	Other chains*
Asset	BTC	L-BTC	?
Time until Swap	3 Confirmations(~30+ min)	2 Confirmations(2+ min)	?
Amount Privacy	Public	Blinded	?
Wallet	LN-Node Native Wallet	Elementsd Wallet, GDK	?
Benefits	Totally trustless	Predictable time to completion	?
Drawbacks	Variable time until swap	Federated custody	?

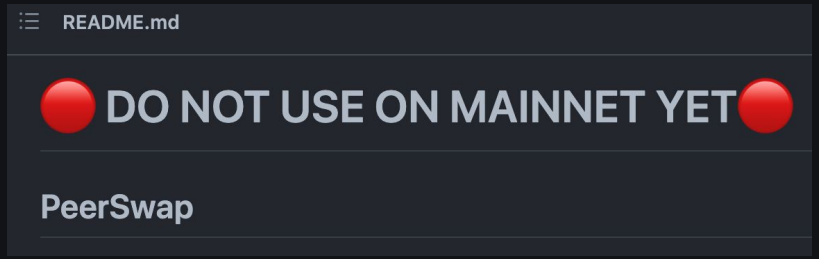
**Anything that can spend while revealing preimage*

Blockstream

PEERSWAP

Status of PeerSwap

- Prototype
- Supports LND and clightning
  - Node-native Onchain Wallet for BTC swaps
- Peer Allowlist required (until we figure out incentives/anti-griefing design)
- Can we get rid of the allowlist?

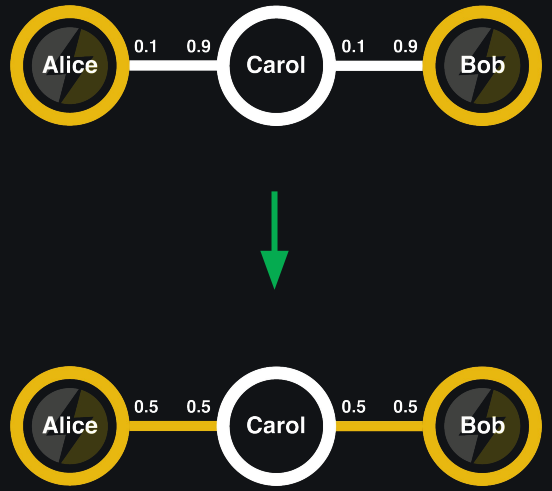


Blockstream

PEERSWAP

Roadmap

- Open Source Release soon-ish™
- Standardization for spec
- Could this become part of the LN spec?
- Implement Optional Light Liquid Wallet
- 2-Hop swap negotiation via onionmessage?
- Call to Action:
  - https://www.peerswap.dev
  - Join our Discord
  - Get involved with specification
  - Implement in node managers and UIs
  - Future swap options with additional chains or other L2's (e.g. fedimint)



Blockstream

WARREN TOGAMI

VP Solutions @ **Blockstream**

Founder @ **Fedora Linux**

Former Engineer @ **Red Hat**

Twitter @**wtogami**

KONSTANTIN NICK

Lead Developer of **PeerSwap**

Founder @ **Donnerlab**

Contractor @ **Blockstream**

Twitter @**sputn1ck**