



Blockstream

# Lightning $\approx$ Bitcoin

Dr. Christian Decker

Core Tech Engineer

1

The Good

# Lightning = Bitcoin

- Payments on Lightning are denominated in bitcoins
- Bitcoins on Lightning are fungible with on-chain bitcoins
- Lightning is complementary to on-chain payments

# Lightning > Bitcoin

- More private
- More scalable
- Fewer fees
- Real-Time payments
- Invoices that actually work (with on-chain fallback)

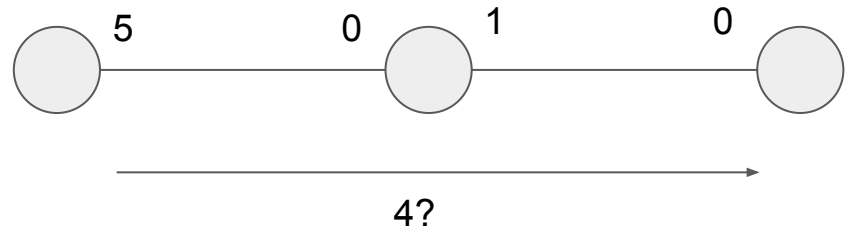
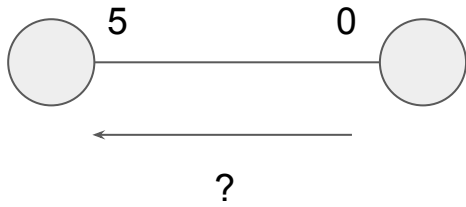
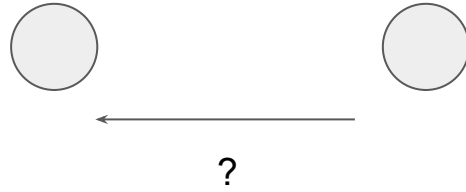
**2**

The Bad

# Lightning < Bitcoin

- Funds allocation is not trivial
- Routing can be difficult
  - Relies on remote channels and their capacities
  - Relies on peers being online
- Need to be online to receive
- Funds are in hot wallets
- Payments may drop on-chain
- Not all funds are spendable (reserve)

# Routing is hard



**3**

The Ugly (but temporary)



# Specification Meeting November 2018

---



## Splice-in / Splice-out

Add and remove funds from an existing channel



## Multipath Routing

Split larger payments onto multiple paths



## Spontaneous / Streamed Payments

Perform multiple payments based on a single invoice



## Payment Decorrelation

Make it harder to correlate payment hops



## Dual-funded channels

Both parties contribute funds to a channel



## Fee Hooks

Decide fees at the time we broadcast



## Watchtower Protocol

Have third-parties monitor the blockchain



## Bitcoin Information Relay

Notify peers about block headers and channel closes



Blockstream

**Thanks!**  
**Questions?**