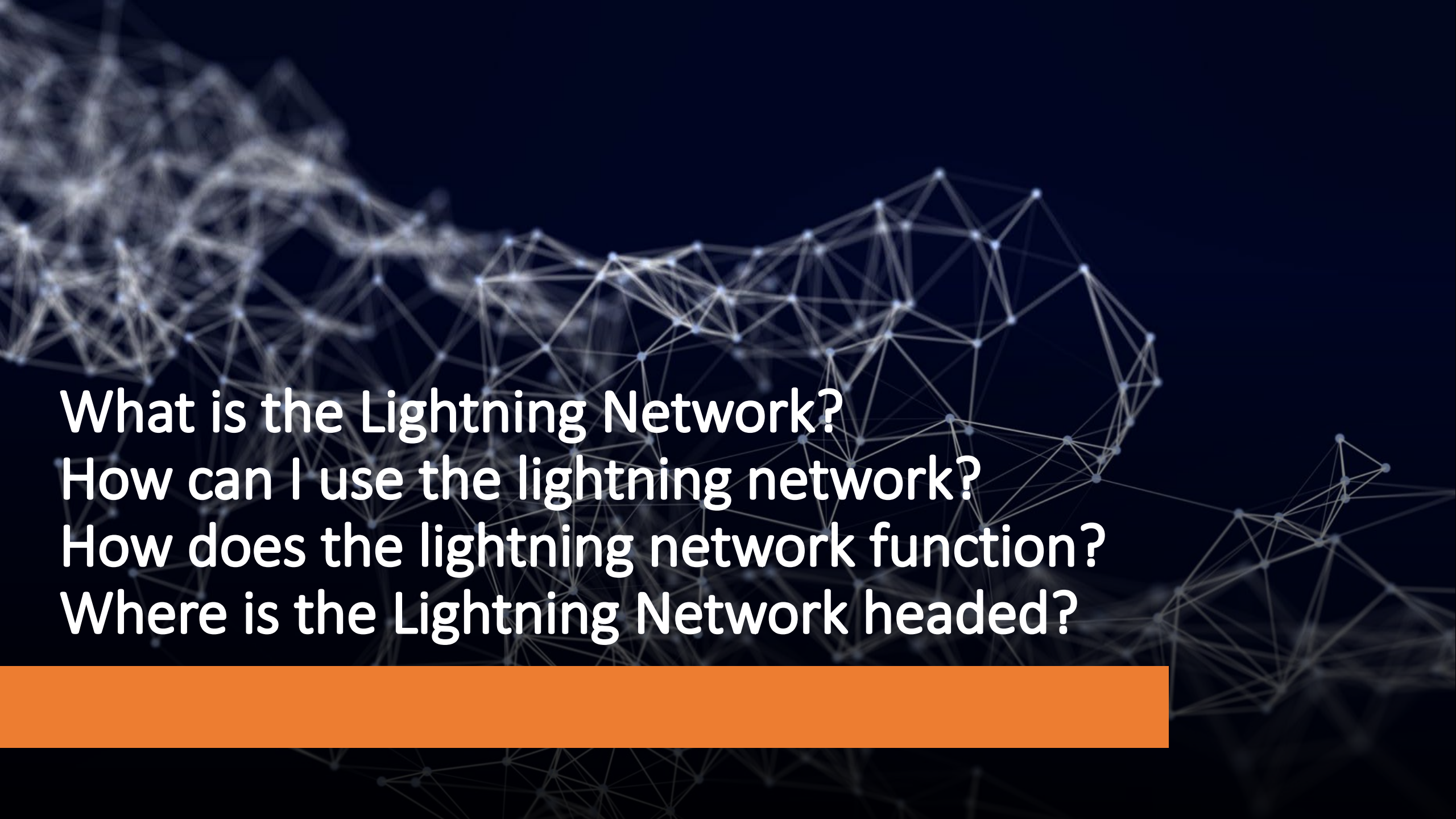
Plugging in to the Lightning Network


What is the Lightning Network?
How can I use the lightning network?
How does the lightning network function?
Where is the Lightning Network headed?

DISCLAIMER

- High level functional overview, not technical.
- DO YOUR OWN RESEARCH.
- DON’T TRUST, VERIFY.
- Lightning is still #RECKLESS (but it’s getting better).
- Lightning is changing rapidly, and all of this may change.

What is the Lightning Network?

- A possible scaling solution
- Increased divisibility
- A rapid settlement solution
- A privacy improvement
- A smart contract layer for Bitcoin

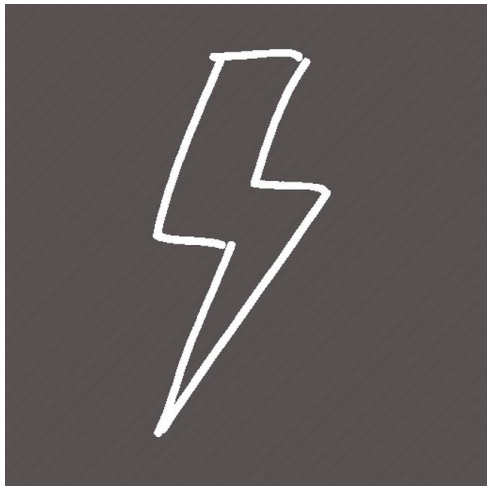
How can I use the Lightning Network?

1. Custodial Lightning Wallets (most user friendly)
2. Non-custodial mobile Wallets (user friendly)
3. Full Control Lightning Wallets – Routing Nodes
   - Non-Custodial
   - Channel Management
4. Lightning Backend

Custodial Lightning Wallets

- Custodial = Not Your Keys, Not Your Coin.
  - DO NOT STORE LARGE AMOUNTS!
- Extremely User Friendly

- Blue Wallet
- LNtxbot in Telegram
- Wallet of Satoshi



Non-Custodial Mobile Wallets

- User Friendly
- No Channel Management
- Single balance – BTC/LN (Muun)

- Muun Wallet
- Phoenix Wallet
- Breez Wallet

Routing Nodes

- Channel Management
- Non-custodial
- Can participate in Liquidity Marketplaces

- Raspiblitz
- Raspibolt
- NODL
- Umbrel

RASPI BLITZ

How does LN function?

1. Channels
2. Routing

How does LN function?

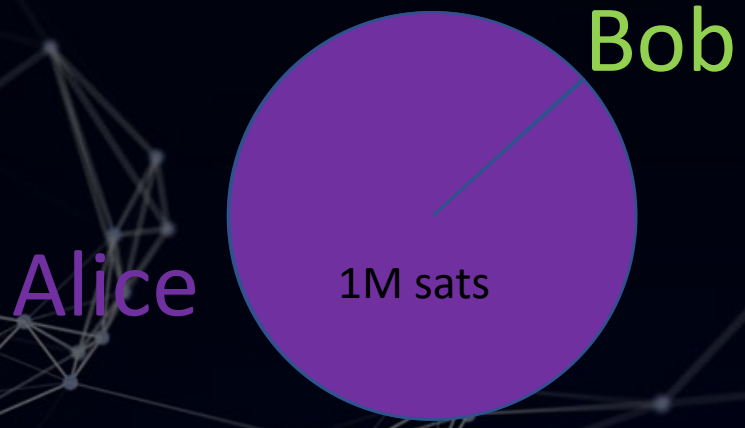
- Agreements are made between users called “Channels”
  - Channels are formed in an on-chain transaction
  - Channels are closed in an on-chain transaction
  - Unlimited transactions can occur between open and close outside the blockchain

Channels

Alice opens a channel with Bob.

Alice pays 1M sats to a wallet that Alice *and* Bob control.

(2 of 2 multisig)

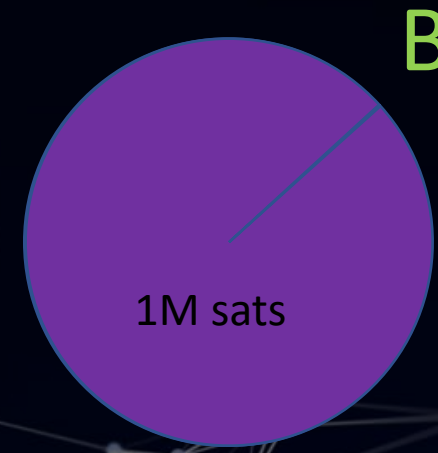


Capacity = 1M sats

Channels

Alice and Bob both sign a payout:

- Alice gets 1M sats
- Bob gets 0 sats
- Can be broadcast at any time (force close)

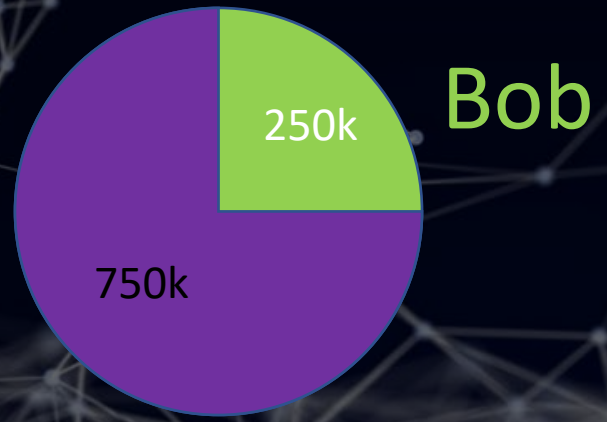


Capacity = 1M sats

Channels

- Lightning payments are updates of the payout.

Alice pays Bob 250k sats.



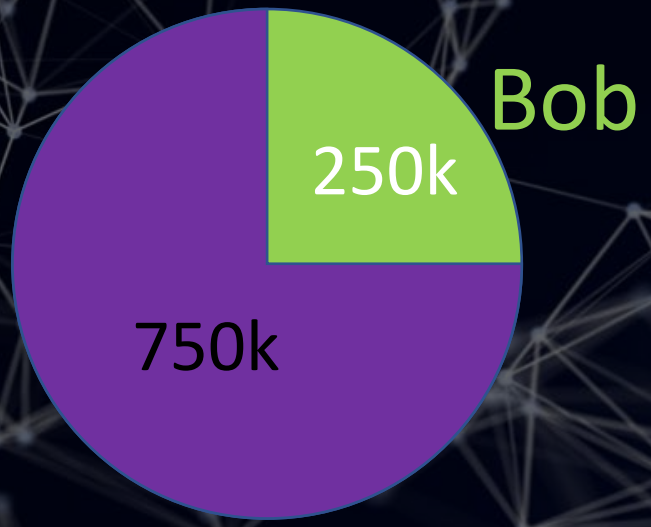
Capacity = 1M sats

- Local + Remote Balance = Channel Capacity

*ignoring the *commit* which reserves some balance to pay a next block force close

Channels

- Q: What is the maximum lightning payment that Bob can pay to Alice?

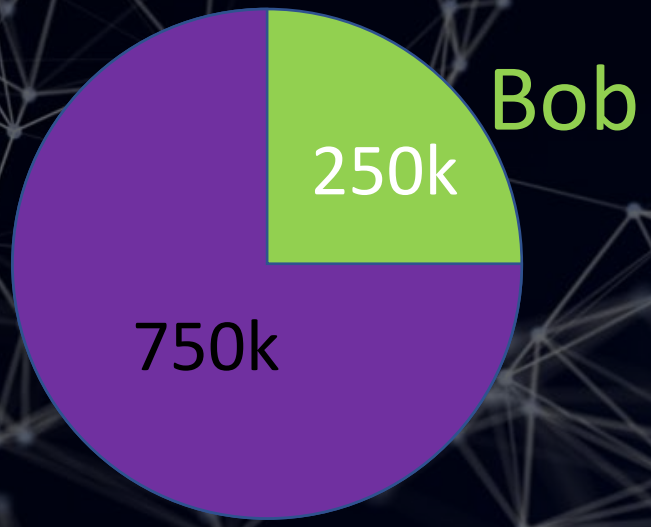


Capacity = 1M sats

Channels

- Q: What is the maximum lightning payment that Bob can pay to Alice?

- Answer: 250k sats



Capacity = 1M sats

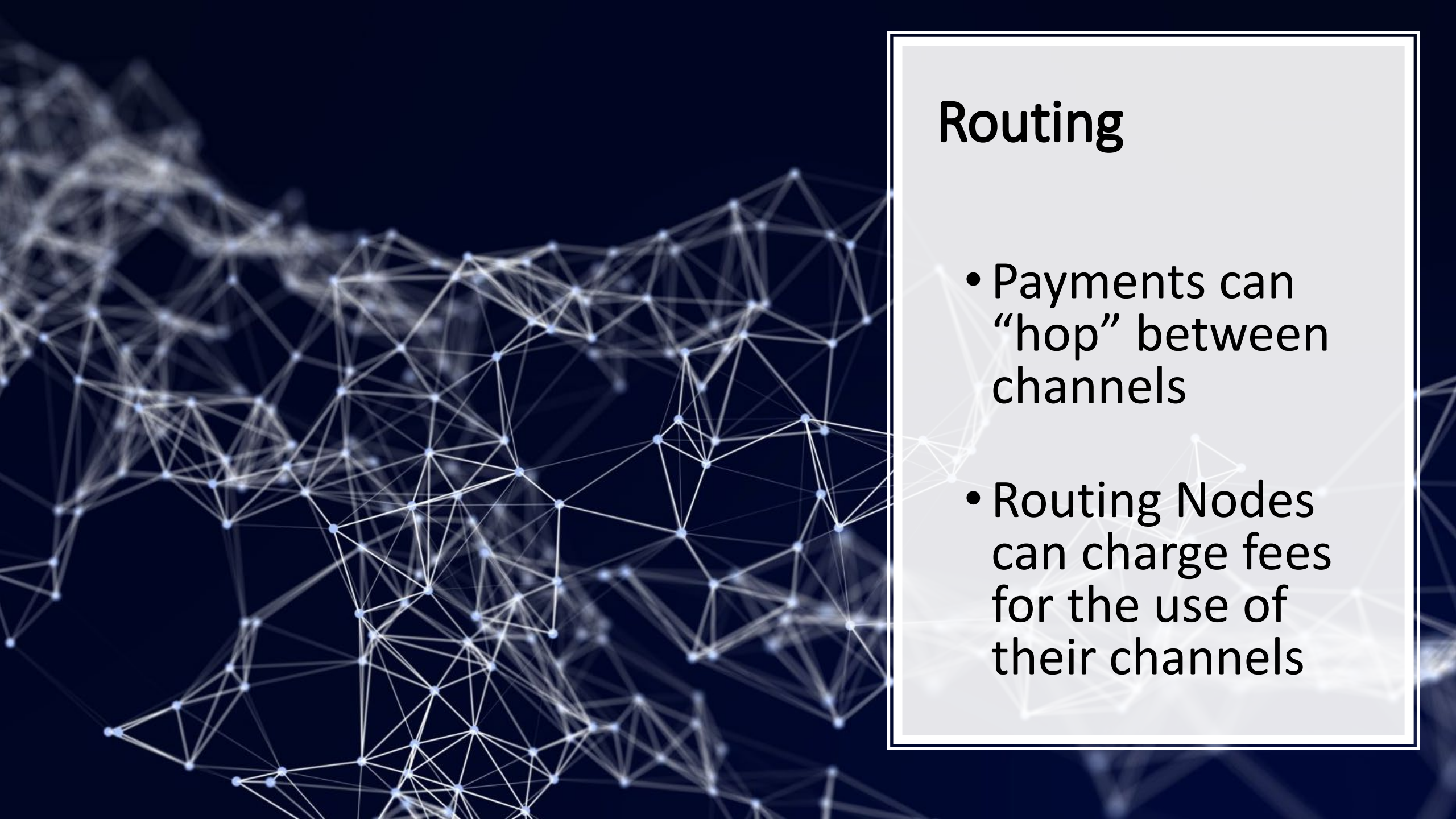
Channels

- Alice and Bob’s nodes must be online to send/receive.
- Payout updates in a channel cost zero fees.
- WARNING: Offline nodes may be stolen from by publishing old channel states (learn about *Watchtowers* to penalize).

Channels

- Alice and Bob’s nodes must be online to send/receive.
- Payout updates in a channel cost zero fees.
- WARNING: Offline nodes may be stolen from by publishing old channel states (learn about *Watchtowers* to penalize).

Any questions before Routing? →



Routing

- Payments can “hop” between channels
- Routing Nodes can charge fees for the use of their channels

Routing

- Bob has another 1M sat channel open with Carol.
- Alice can pay Carol via Bob's channel.
- Bob can charge a ⚡ routing fee for this service.

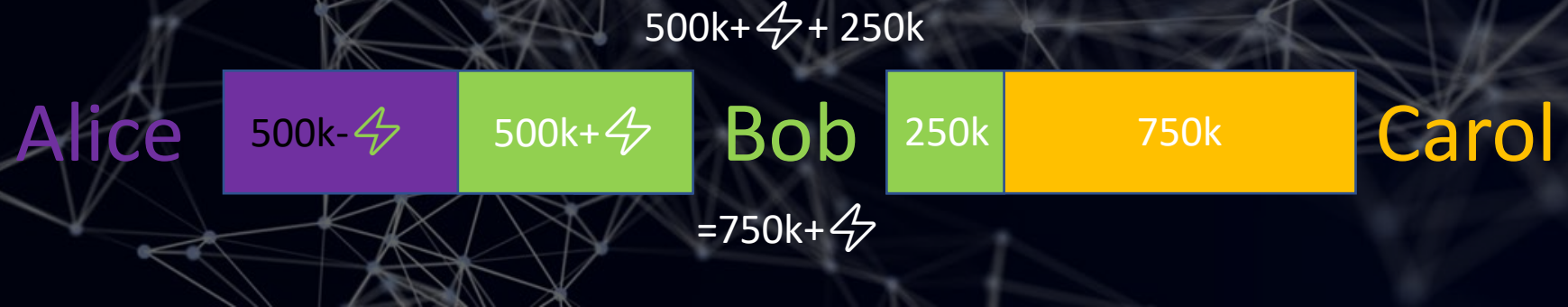
Routing

Routing

Alice pays Carol 250k sats and a ⚡ fee to Bob

Routing

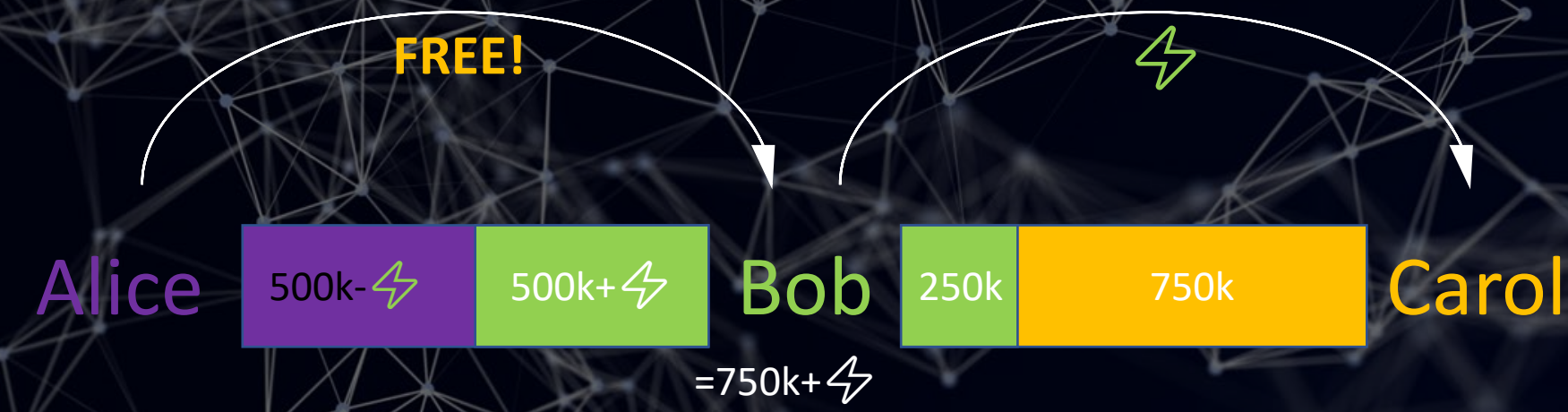
Alice pays Carol 250k sats and a ⚡ fee to Bob



Routing

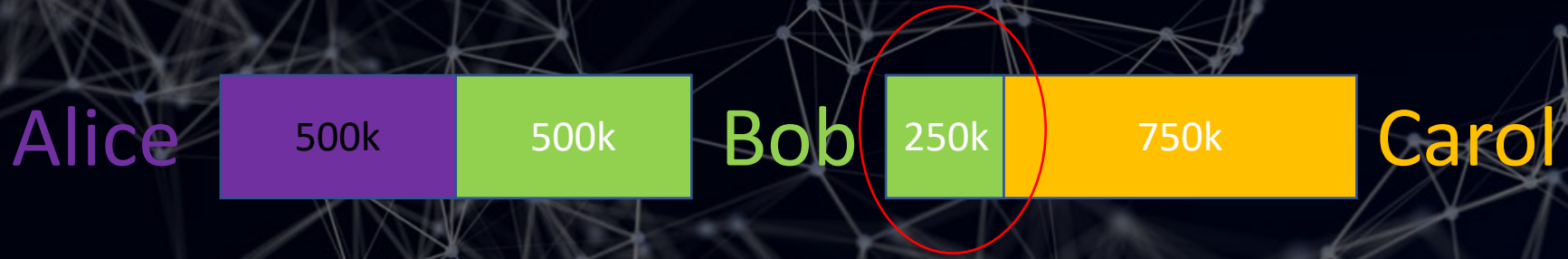
Bob charges Alice ⚡ based on the hop to Carol

The fee rate on Bob's channel to Carol is the cost.



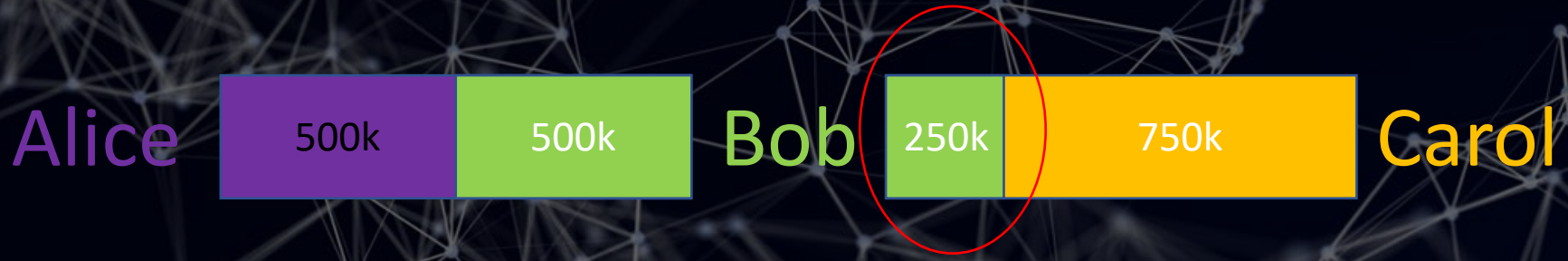
Routing

Q: What is the maximum* that Alice can pay Carol?
*(ignore fees)



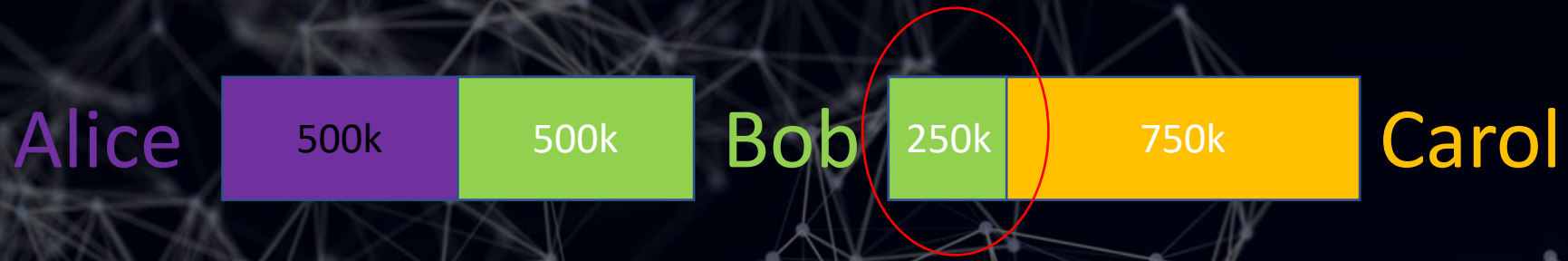
Routing

Q: What is the maximum* that Alice can pay Carol?
*(ignore fees)



A: Carol's *inbound liquidity* from Bob is limiting.
A maximum of 250k sats can be paid.

Routing



- Alice can't see the balance of Bob's channel to Carol.
- Alice will experience a payment failure for payments larger than 250k.

Routing

Additional Notes:

- Fees are public (see 1ml.com)
- Flat fee and a ppm fee rate (sometimes msat/sat)
    - 1 sat + 100 ppm payment, for example
- May be changed at any time

Routing

- Routing Nodes are getting passive bitcoin income
  - Must maintain inbound & outbound capacity to route

$$$$$

- Routing Nodes don't know the ultimate origin/destination
  - TOR routed, they only know adjacent channel details
- Incentives are for *high uptime*, *long-lasting channels.*

Routing

- Routing Nodes are getting passive bitcoin income
  - Must maintain inbound & outbound capacity to route

$$$$$

- Routing Nodes don't know the ultimate origin/destination
  - TOR routed, they only know adjacent channel details
- Incentives are for *high uptime*, *long-lasting channels.*

Where is the Lightning Network headed?

Liquidity Marketplaces

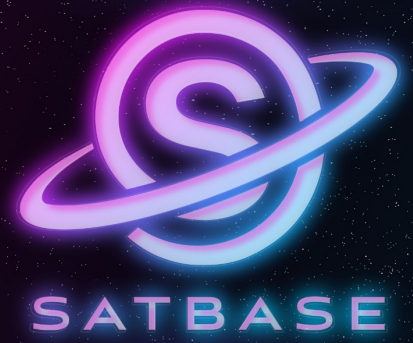
- Inbound Liquidity is a valuable commodity
  - Inbound = The sats that others have pointed to your node

- Buy Inbound
  - Lightning Pool (blind auction, command line)
  - Lightning Liquidity Bot (on Telegram)
- Sell Inbound
  - Lightning Loop

Strike

- Zero fee transactions
- Basically Venmo, but lightning compatible
- International Settlement Layer
  1. Remittances
  2. High Frequency Trading (?)

Thank You!



BITKO.CC