Lightning Network Topologies

Joseph Poon
joseph@lightning.network

Quick Review

Multisignature payment channels

Real bitcoin transactions

No custodial delegation

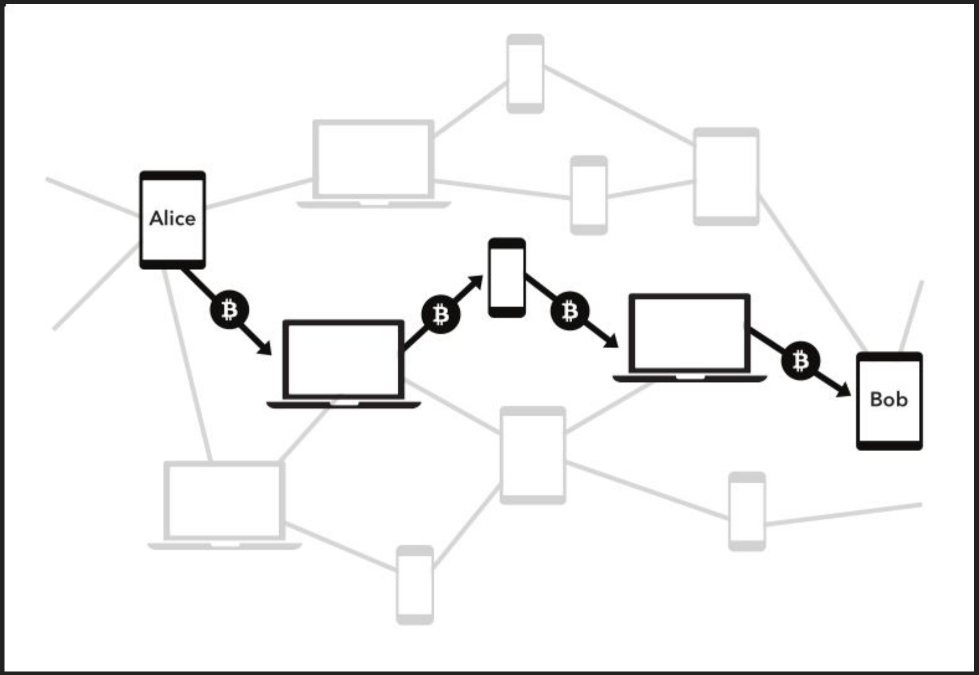
A network of channels

Atomic payments

Cheap transactions

Instant

Micropayments



Detour… Let’s talk about long-term incentives

What happens when block rewards go down?

Transaction fees can pay for miners

However, fees operate in a market

If you don’t include a higher-fee transaction, another miner will

If block sizes are unconstrained, fees approach zero

If block sizes are constrained, fees become large and it’s possible that fees would be too large to make many kinds of on-chain payments

Lightning is about solving long-term mining incentives

One of the greatest values in Lightning is in resolving this tension of transaction fees to pay for miner security, and the fees being too high to pay for transactions

Higher fees (to pay for mining security), we need to be able to make micropayments and everyday purchases using real Bitcoin

Real Bitcoin and real transactions means people will be making on-chain transactions. Net settlement, many users making a few transactions

Miners can have higher fees but everyday users can still transact cheaply

Desirable Network Topologies

As Lightning is a network, it implies different kinds of topologies

Core promise of Bitcoin: decentralized payments

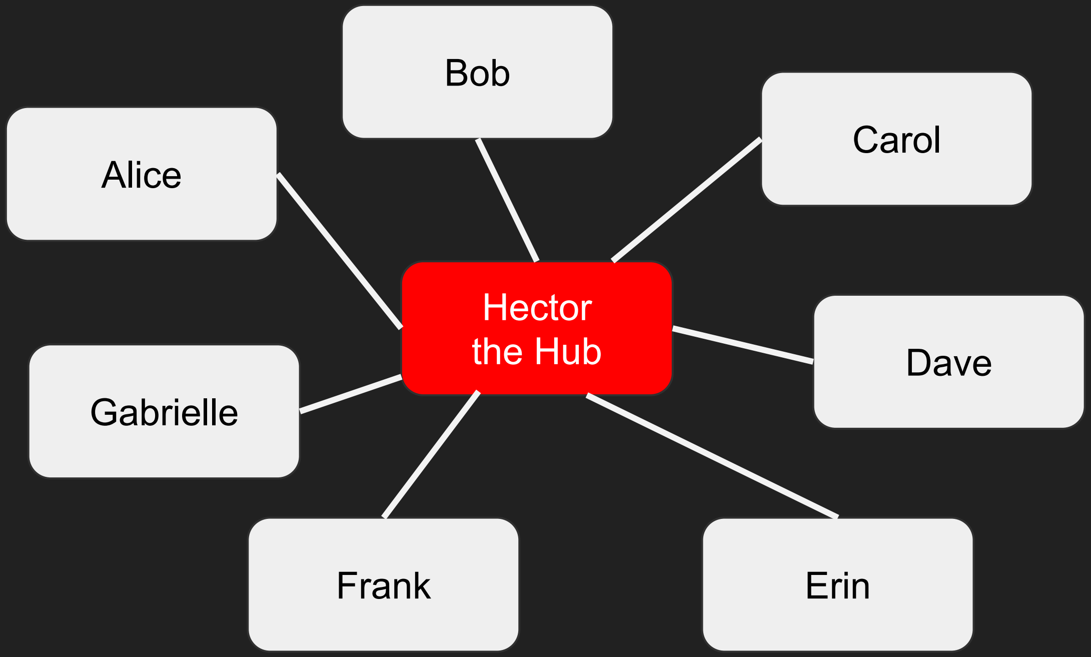
Everyone connect to a single processor (Visa, MC, UnionPay) is undesirable

We all want the network to be decentralized, but the primary criteria is more nuanced

Node incentives is what matters, we need to understand the cause for centralization

Network Effects

What really matters: Are there significant network effects gained from having a single (or handful) of nodes, a “hub and spoke model”? Does the hub provide significantly more value?



You can't stop highly connected nodes

Power law distributions are a fact of life, there will be supernodes with a high amount of channels

Everyone will not have the same amount of channels open

Highly-connected network is cheap and a function of transaction fees

This is not like Internet routing: nearly zero infrastructure costs

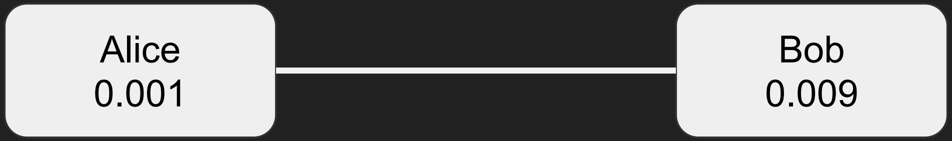
However, is it more efficient to organize with a single hub? How do you bootstrap a distributed system?

Bootstrapping Lightning

If you have a channel open and route, pay over Lightning Network

If you have no channels (e.g. early on), and want to pay someone who accepts Lightning payments, just open a channel directly with them and add some money (bramc)

Alice wants to pay Bob 0.001, but opens a channel with 0.01



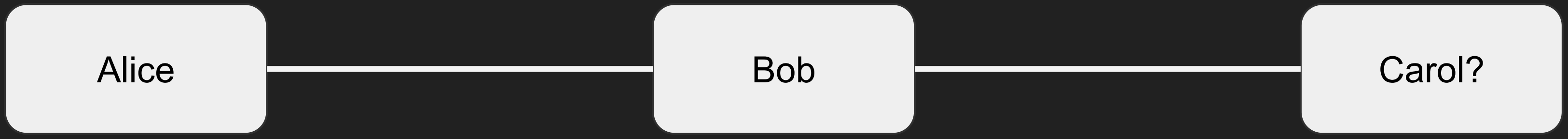
Bootstrapping Lightning

Easy when transaction fees are low, cheap on-chain transactions means you can be lazy and open more channels

Optimizes for very decentralized networks, while making bootstrapping easy

Higher amount of transactions earlier on, match on-chain scalability with its transaction fee costs

Everything is a dumb-channel first, Lightning Network routing is preferred but not necessary



“Hubs” have, at best, marginal network effects

It is improbable to have a single hub willing to open channels with anyone, dominating the market

Hubs require a huge amount of funds. It is not possible to construct one without having a lot of money to enable payment flows

Hub-and-spoke models have lower Velocity

A major factor for network effects resulting in relative centralization is Velocity within a channel

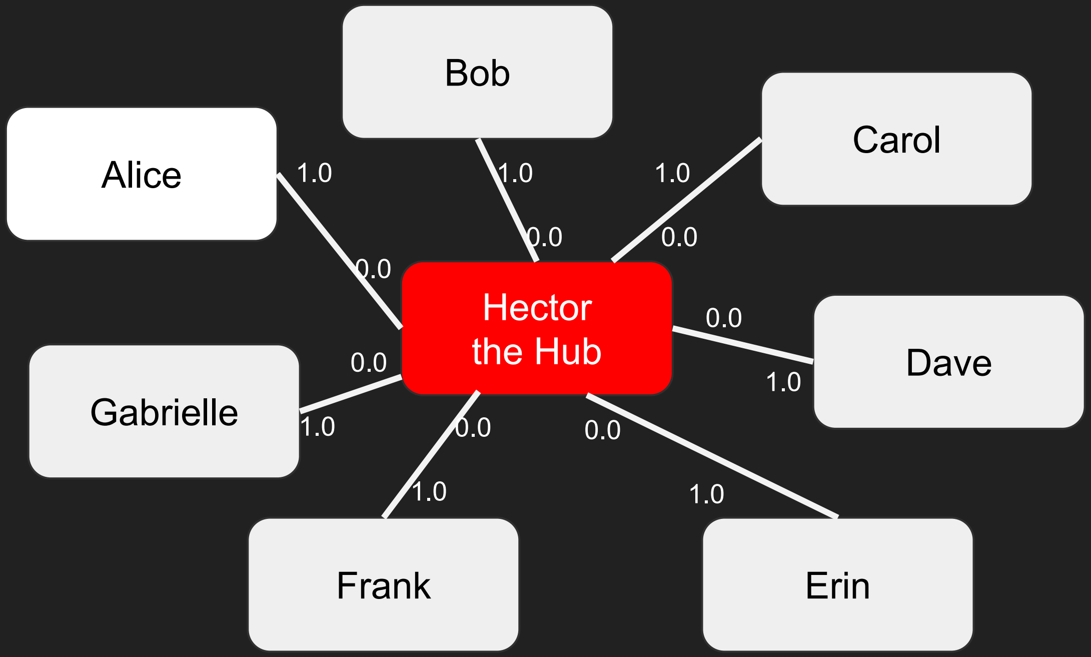
(Amount of funds transferred relative to money supply per time period, e.g. year; how fast money moves)

Large hubs willing to accept channels from anyone result in locking up all their funds in low-velocity channels

Hubs must optimistically add lots of coins to channels to be able to route

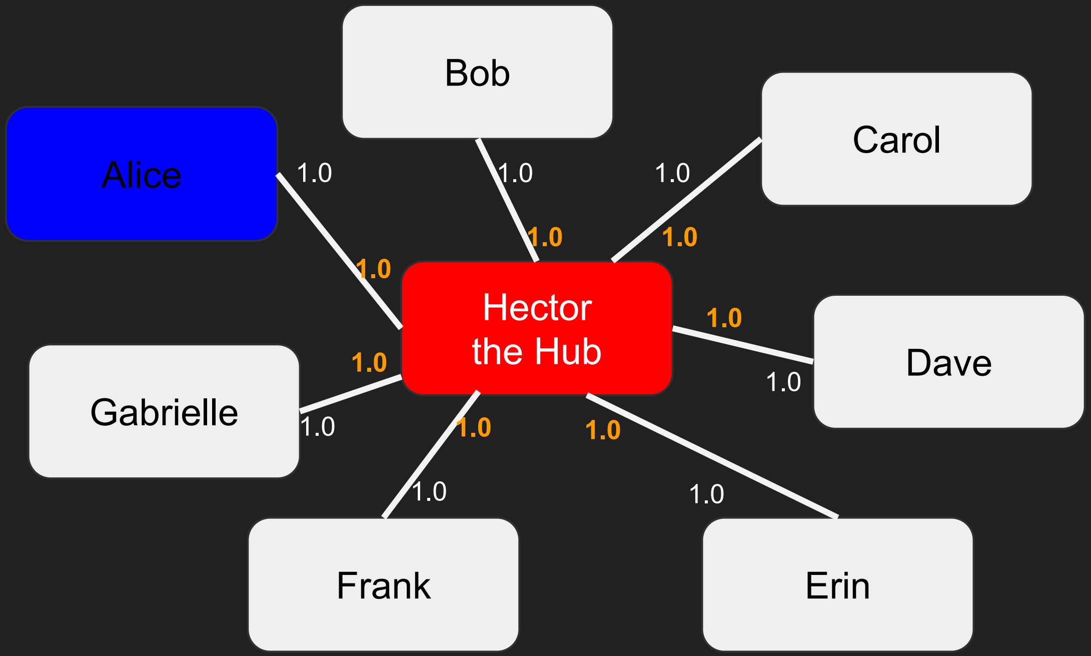
Take a look at the network below. This is what would happen if users open channels to link up to Hector the Hub by putting 1.0 coin in.

This graph can't route at all! Nobody can tell Hector to push funds, because hector doesn't have any to push. Even if Alice pushes 0.1, Hector can't forward it to Bob.



Hubs put up lots of coins with uncertain returns

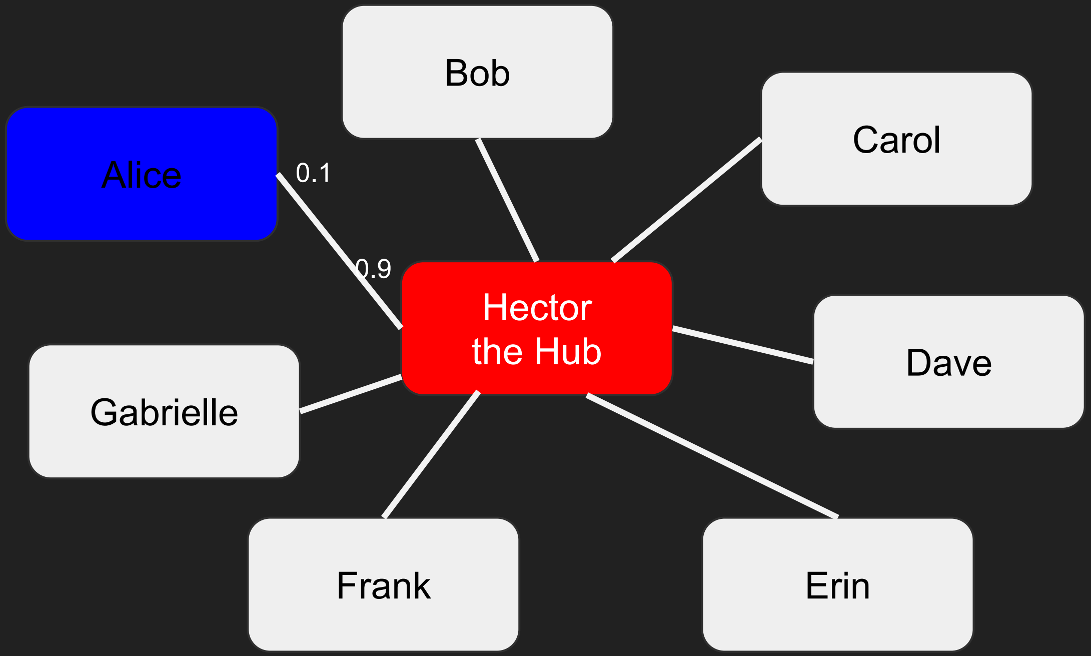
In this case Hector matches each channel funding. Hector needs to lock up 7 coins, and the more people join, the more coins he needs. It gets expensive fast!



Hubs will have lots of money stuck in low-velocity channels

If Alice has a channel with most coins being Hector’s, he is losing out on a lot of time-value

The mitigation is charging periodic fee for channel size, which is cost-uncompetitive with a bootstrapping model which matches payment flows and supply chains



Unclear how things will play out, but a single-hub is unlikely to impossible.

There are still cases where highly connected star topologies (hubs) make sense, but they are not clear money-makers and cost-competitive. Accepting more channel requests results in lower velocity, this is a massive counterweight to any possible network effects

Single hubs have greater on-chain efficiency, but higher costs for the hub off-chain

Direct connections within a particular supply chain or geographic area increases the chance that one is connected to a high-velocity channel, but there are implications for information leakage

Thank you!