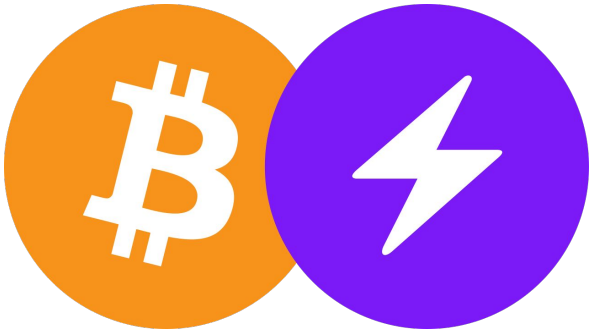
Basic Bitcoin Tech: The Lightning Network

Host - Simplest Bitcoin Book w/ Portland.HODL

- Overview -

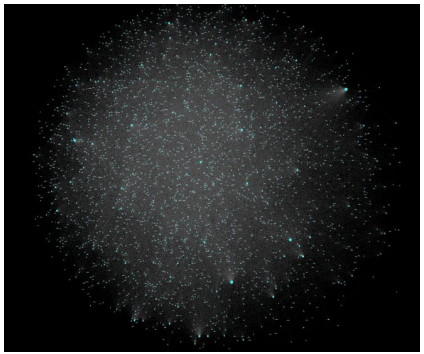


Topics

- What is a ‘Layer 2’ on Bitcoin?
- The Lightning Network as an L2
  - Lightning as a means of payment
  - Is lightning still bitcoin?
  - Channels
  - Instant Settlement & Fees
  - Final Layer 1 Settlement
- Wallets
  - Custodial
  - Non-Custodal
- Nodes
  - Types
  - Liquidity

What is a Bitcoin Layer 2?

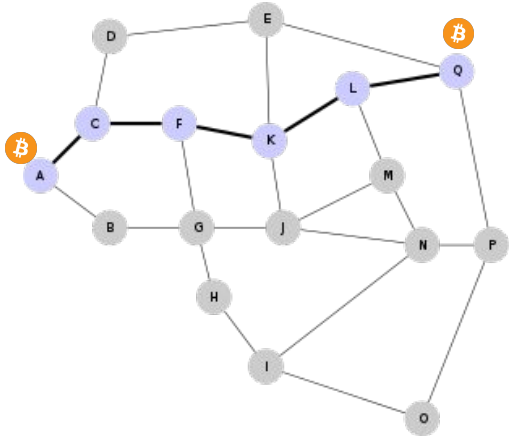
Definition



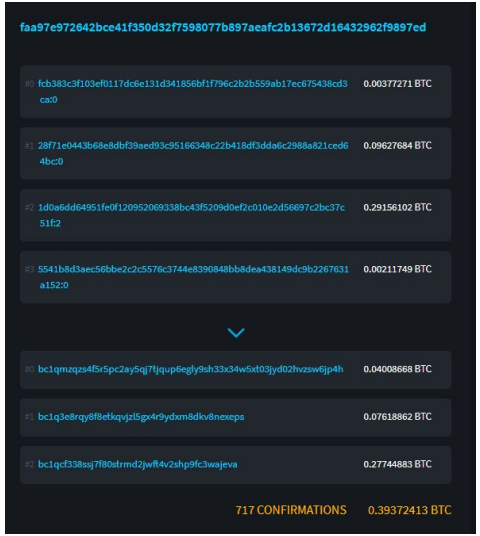
The lightning network of nodes! Over 19K of them right now.

- Layer 2 solutions refer to various protocols that are built on top of the Bitcoin layer 1 protocol to improve functionality.
- **These layer 2 solutions do not change the rules of Bitcoin.**
- A layer 2 is analogous to an extension. An example are Google Chrome extensions. They do not change the way chrome works, but do add features to the browser.
- You can build anything on top of Bitcoin's foundation, but the foundation itself can't be changed.

The Lightning Network as a Layer 2



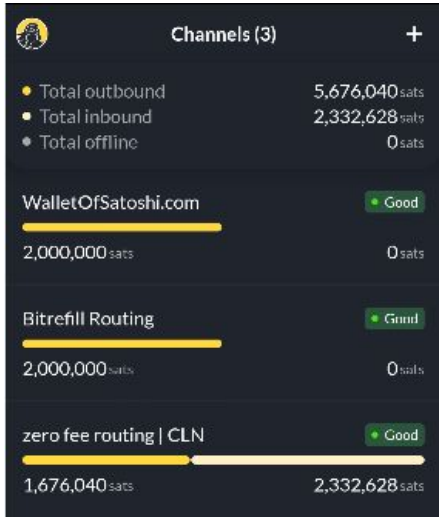
- The Lightning network is built on top of Bitcoin
- The heart of the Lightning Network is the way computers send messages and transactions, so that instant settlement of a transaction is possible.
- Computers on the Lightning network form connections though channels that contain bitcoin.
- Multiple channels can be chained together to form a payment route, such that even if you don’t have a direct connection to the other party. Your payment can be pushed through multiple channels (hops) to get to the payee.



A funding transaction of mine that will be updated again and again until the channel is closed. This was a coordinated dual funded channel. On closure the latest version of this is broadcast.

Is Lightning still Bitcoin?

- Lightning is still Bitcoin since the participants are just passing back and forth a valid bitcoin transaction that can be broadcast at any moment.
- The Bitcoin transactions between participants (peers) update each time a transaction is made. This creates a consensus between all peers involved.
- There are mechanisms to prevent dishonest peers from broadcasting transactions that would double spend funds.



3 Lightning channels on my node.

Channels - Pipes made of Bitcoin*

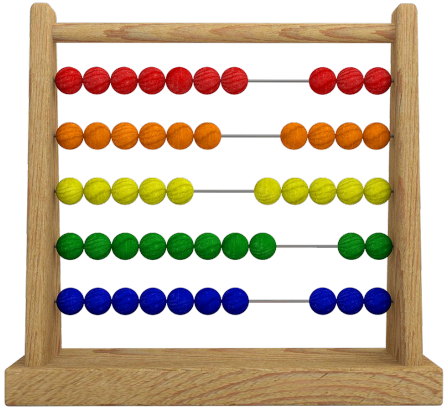
- Channels are connections that your lightning node makes to peers on the network.
- Channels are always created by an initial (funding) bitcoin transaction.
- Essentially these channels are pipes between your lightning node and it's peers made of bitcoin transactions.
- You must authorize channel opens from your node.
- Other nodes may create channels with your node without permission.
- Channels can be closed at any point.

Using chips avoids the disruption of needing to go to the bank after each round of poker to settle up balances.

The Poker Game Analogy - PortlandHODL

- Opening channels is when players go to the bank and get money to buy into the poker game. The players open a channel when they exchange their money for chips.
- Once channels are open, players play poker and in the process they are winning (receiving) and losing (spending) money each round. THERE IS NO NEED TO CASH IN THE CHIPS EACH ROUND, the amount of money each player has is represented by the number of chips they hold.
- At any point after a round a player can cash out their chips and receive money, and then take that money to bank for final settlement. (Closing a channel)
- THERE IS A BAR TAB ANALOGY THAT IS USED COMMONLY AS WELL.

Instant Settlement and fees!



- Since the peers on the lightning network are just passing around valid bitcoin transactions the settlement is instant. - No need to wait for blocks
- E.G. If you spend 5000 sats; you and the other party create a transaction immediately that updates the balance that you each have. This would subtract 5000 sats from your balance and your peer would get 5000 stats.
- It's possible to push a payment across multiple nodes by having a node that is in the middle receive bitcoins, but then immediately spend them to the next link along the chain. Link pushing beads though an abacus,
- Each node imposes a small fee to pass a transaction through it. This is how nodes can use their bitcoin to generate *yield* through fees.

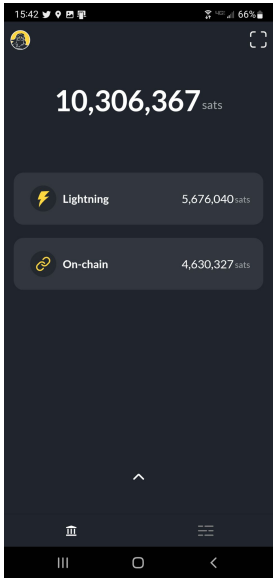
Settlement in finality on the timechain.

Broadcast the transaction and put the bitcoins back into your full custody.

- This is when a lightning channel is closed. This means that a participant broadcasts the latest transaction they have to the network so that it can get mined into a block.
- At this point the funds each person has on their side of the channel are returned to their wallets.
- In terms of the poker example, closing a channel is like cashing the chips out, then taking the money to the bank so that your bank account balance reflects how much money you have.

  Note: Once you cash out, you can't play poker until you get more chips again.

Mobile Lightning Wallets - Lightning is for payments!



E.G. Zeus Wallet

There are 2 types of lightning wallets

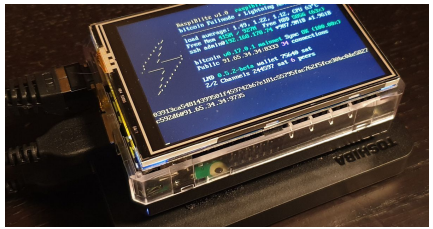
- **Custodial** : The wallet software provider manages and has custody of the bitcoins (sats)
- **Non Custodial**: (Self Custody) The user has full custody of their funds.

Some Examples of mobile lightning wallets are…

- **Custodial** : Wallet of Satoshi, Blue Wallet
- **Non Custodial**: ZEUS, ZAP, Muun, Breeze, Phoenix

All mobile wallets are capable of sending and receiving sats.
Note: Receiving sats requires liquidity.

Lightning Nodes



Raspberry Pi Based Nodes

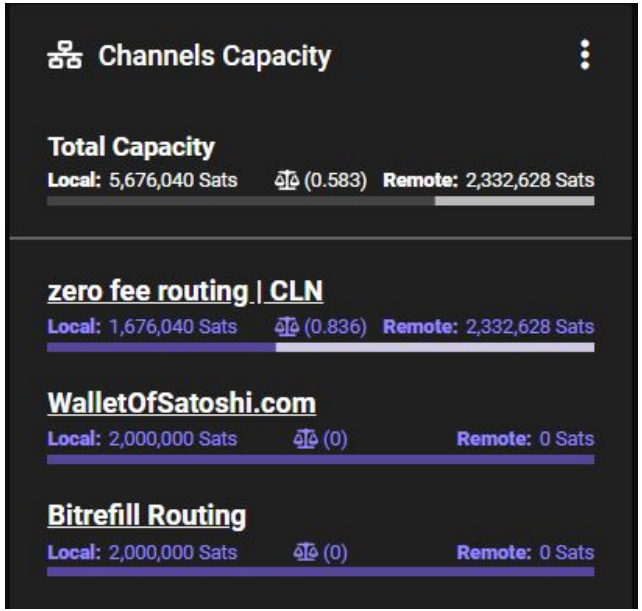
A lightning node is software that runs on top of Bitcoin Core and utilizes the rules of the lightning network to send, receive and route payments.

A lightning node can run on many different devices and there are many software packages to start up a node - A lightning node needs a Bitcoin core full node to operate on top of.

- Popular turn key solutions are Umbrel and Citadel
- Standalone node software packages are Core Lightning and LND

Note: Any funds deposited to lightning node are funds stored in a hot wallet. As such don't use your lightning node like a cold storage solution.

Lightning Liquidity



Liquidity ratios of various channels.

- ‘Liquidity’ on the lightning network is how much bitcoin is able to be sent or received
- There are two types of liquidity; inbound (receiving) and outbound (spending)
- When a new channel is opened it’s inbound is 0% and outbound is 100% of the sats in the channel.
- Getting inbound liquidity is one of the harder things for people getting started with lightning to obtain and/or understand.
- Voltage is working to make it easier and much quicker.

Thanks For Listening.

1. Questions or Comments? Please ask to come on stage.
2. Anything incorrect please comment on the slide in question.