

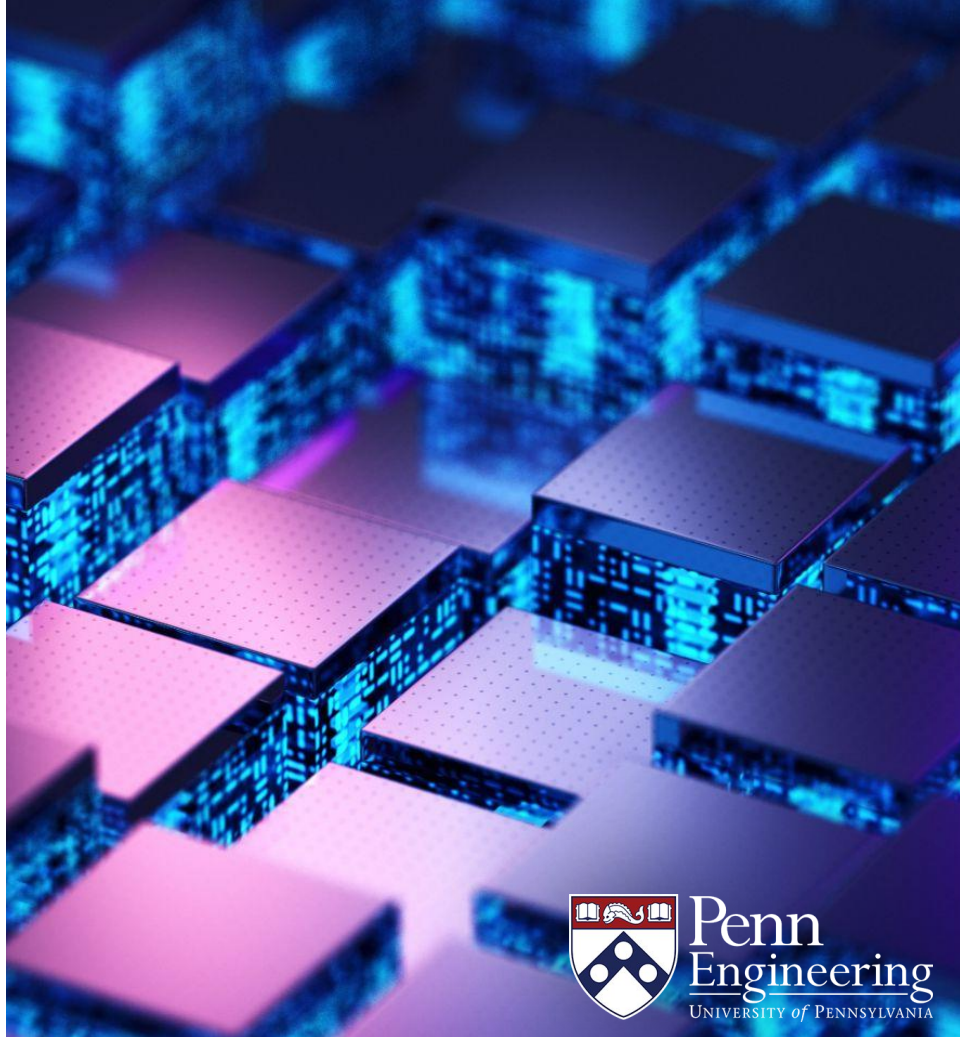
EAS 5830: BLOCKCHAINS

# The Lightning Network

Professor Brett Hemenway Falk



Penn  
Engineering  
UNIVERSITY of PENNSYLVANIA



# Why Lightning?

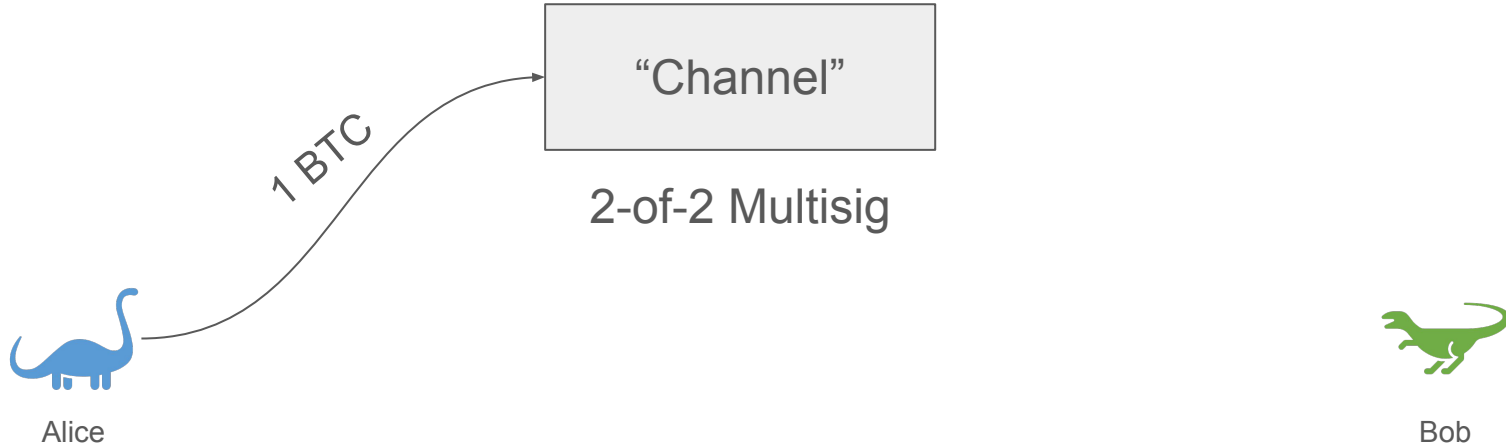
- El Salvador adopted Bitcoin as a national currency in [September 2021](#)
- The Bitcoin blockchain can handle about [6 TPS](#)
- There are [6.6 Million people in El Salvador](#)
- There is about enough Bitcoin blockspace to allow them to each make one transaction every two weeks (assuming no one else used the blockchain)
  - [Typical transactions](#) cost around \$4, so you can't use Bitcoin to buy coffee anyway
- Can't use a faster blockchain because they want the sovereignty of Bitcoin

# Lightning Overview



- Lightning is a layer-2 “payment channel network” on top of Bitcoin
- Any pair of participants can open a “channel”
  - Each user deposits funds in a 2-of-2 multisig account
    - Channel “openings” are on-chain transactions
    - Users can deposit different amounts (even zero for a unidirectional channel)
    - User deposit is maximum (net) payment they can make to the other party
- Payments are done off-chain
  - To make a payment, spender signs a TX to close the multisig account with updated balances
  - Either participant may send these transactions to the blockchain at any time to close the channel (but they don’t, they just hold the signed transaction)
  - Penalty system ensures that participants don’t broadcast “stale” transactions

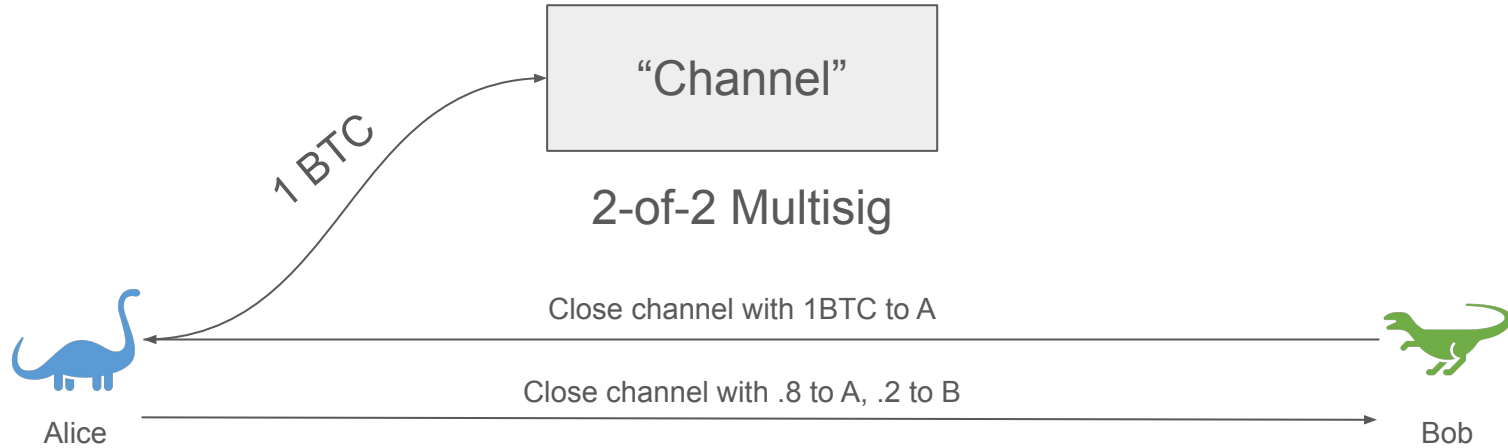
# Lightning Channels



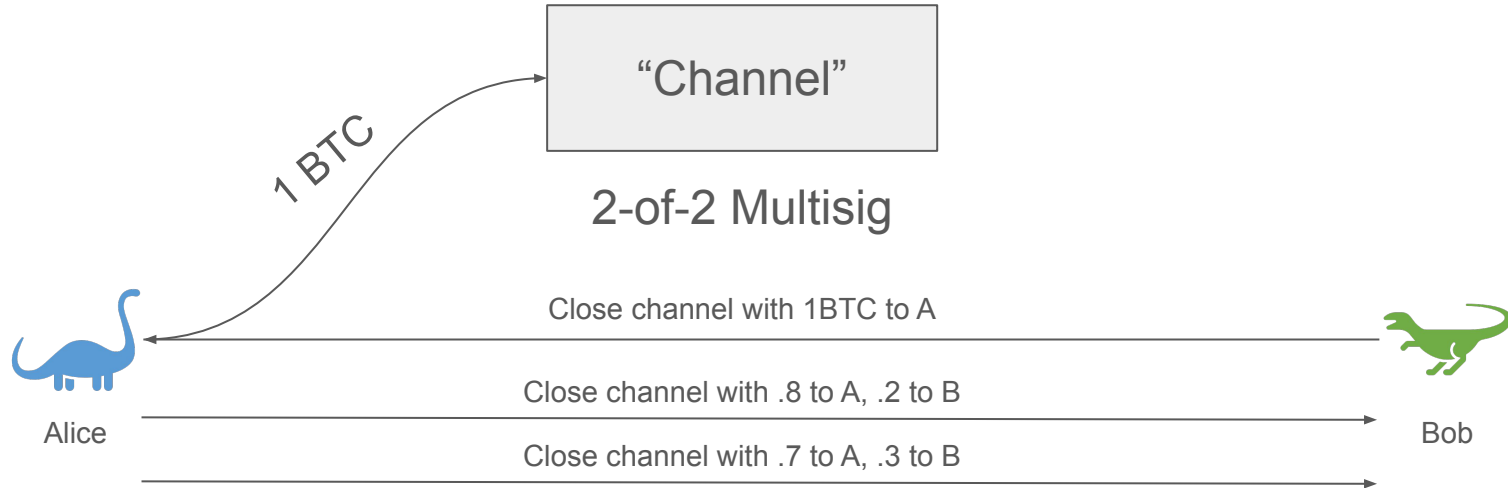
# Lightning Channels



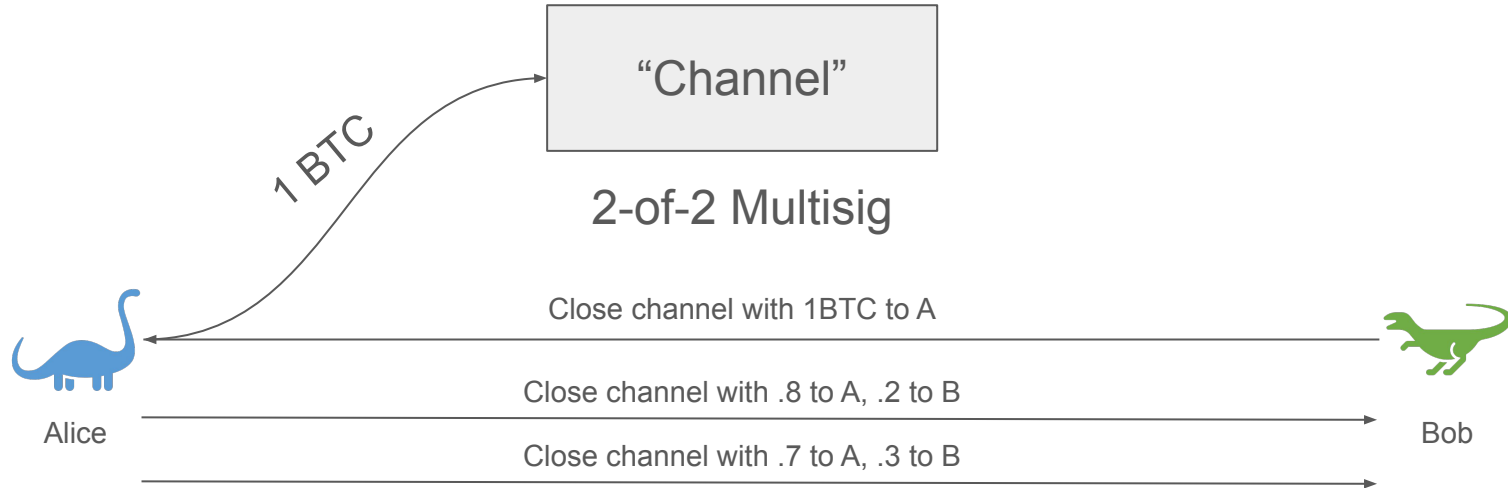
# Lightning Channels



# Lightning Channels



# Lightning Channels



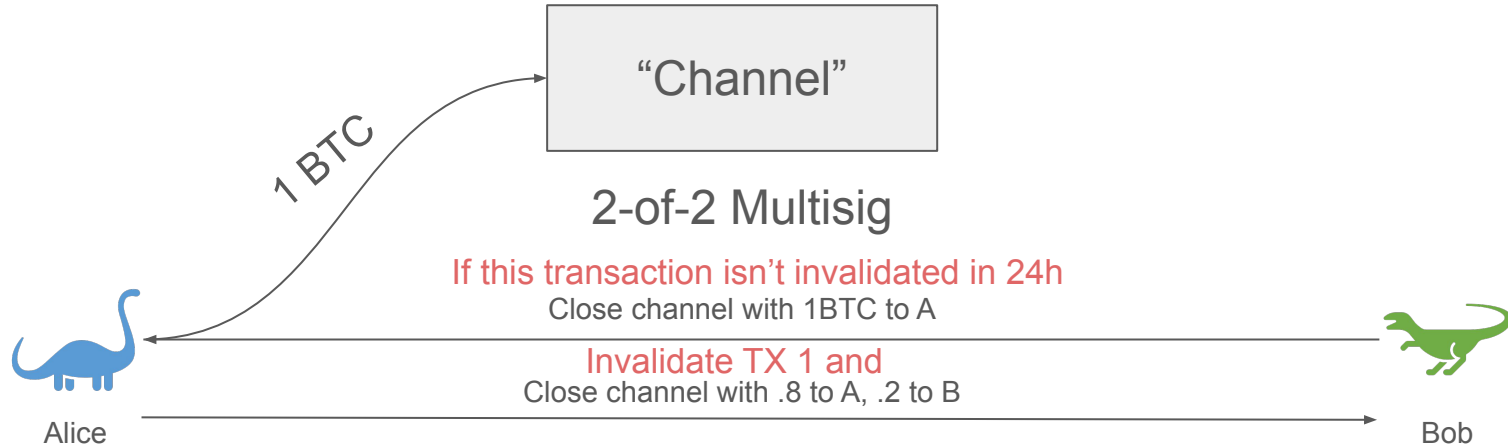
When the channel is closed,  
only the last of these  
transactions is posted to the  
Bitcoin blockchain

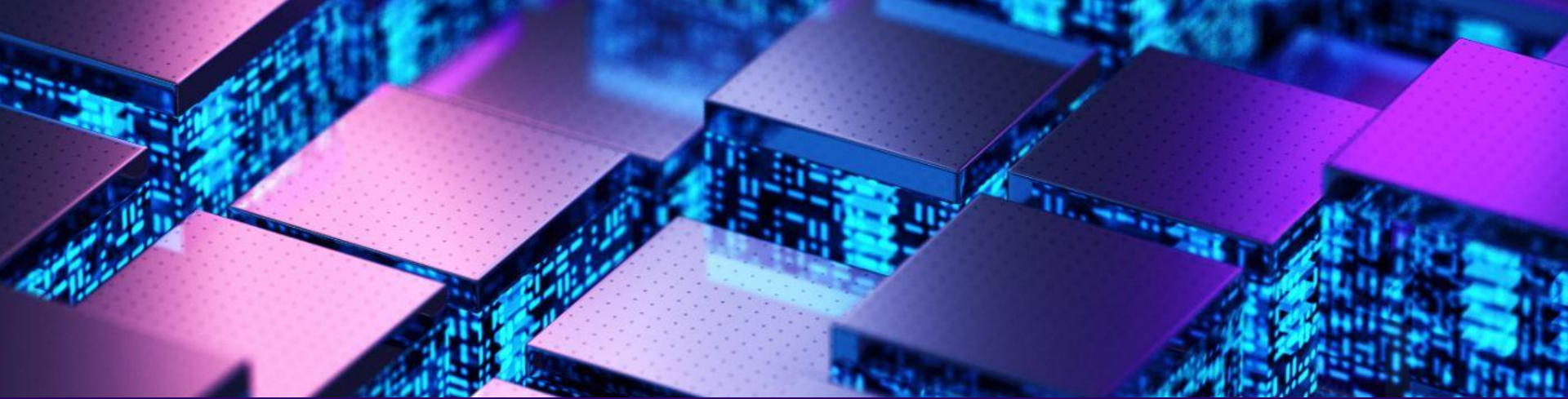


# Lightning Channels



# Lightning Channels





What's going on with Lightning?

# Lightning nodes

- Any user can run a Lightning Node
  - [Most](#) nodes run [lnd](#)
  - Install (open-source) node client, and Bitcoin node
- It's annoying to run a node
  - Individuals rarely run their own nodes
  - “Custodial” nodes handle payments
    - E.g. [WalletOfSatoshi](#)
  - Lightning is mostly custodial



## Real-Time Lightning Network Statistics

### Number of Nodes

**16,415** ↓ -0.21%

### Number of Channels


**74,034** ↓ -1.5%

### Network Capacity

**5,405.68 BTC** ↑ +0%  
\$158,816,405.38

### Node Countdown

**983,588**  
1.6%



The screenshot shows a video call interface for 'THE CHOPPING BLOCK'. It features four participants in a 2x2 grid: Tarun (top-left, with orange glasses and a blue shirt), Haseeb (top-right, with a microphone), Robert (bottom-left), and Tom (bottom-right, with headphones). Each participant's name and a short bio are displayed below their video feed. The background of the call is dark with a network diagram. To the right of the call, the show's logo and title are displayed, followed by the episode title and number.

**THE CHOPPING BLOCK**

**Are Layer 2s Sucking Up the Value of ETH?**  
- Ep. 484

**Tarun**  
giga-brain and grand poobah at Caustic

**Haseeb**  
Head hypeman at Dragonfly

**Robert**  
crypto connoisseur and captain of Compound

**Tom**  
DeFi Maven and master of memes

“Aren’t most of the channels like BitRefill?”

## Top Products

All gift cards

Apparel

Automobiles

Ecommerce

Electronics

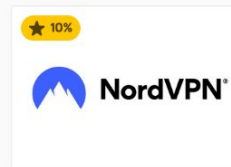
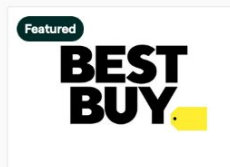
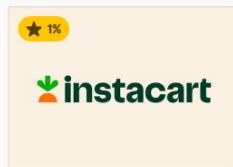
Entertainment

Experiences

Food

Games

## Gift cards, the best way to spend your crypto





ACINQ	3569 channel(s)
WalletOfSatoshi.com	2641 channel(s)
1ML.com node ALPHA	1723 channel(s)
CoinGate	1627 channel(s)
In.nicehash.com [Nicehash]	1369 channel(s)
Boltz	1230 channel(s)
Kraken 🍷⚡	1190 channel(s)
bfX-Ind0	1109 channel(s)
deezy	1000 channel(s)
OpenNode.com	992 channel(s)
gameb_1	967 channel(s)
BCash_Is_Trash	914 channel(s)
bfX-Ind1	824 channel(s)
mainnet.lightningconductor.net	799 channel(s)
tippin.me	719 channel(s)
southxchange.com	691 channel(s)
gameb_2	664 channel(s)
ando.masterofpearls.net	636 channel(s)
CryptoChill	594 channel(s)
LNBIG.com [Ind-01]	584 channel(s)
Bitrefill Routing	572 channel(s)

ACINQ - creates Eclair lightning client

WalletOfSatoshi - Custodial wallet

1ML - Lightning explorer

CoinGate - Payment processor

NiceHash - Mining power marketplace

Boltz - Lightning ↔ BTC exchange

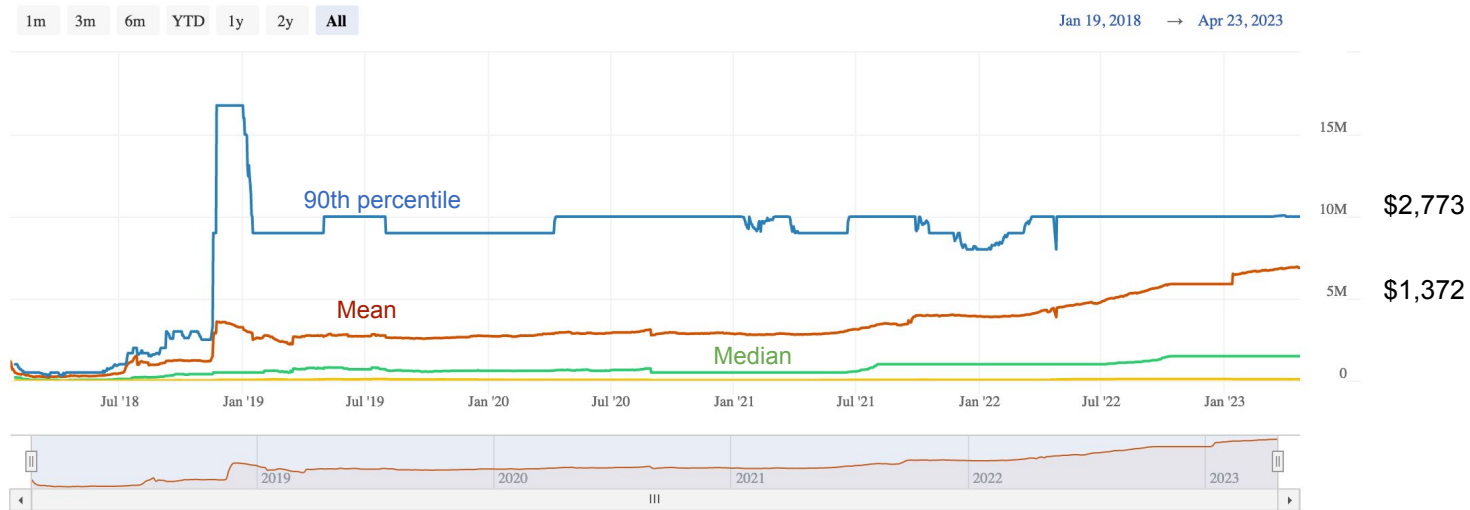
Kraken - Exchange

BitRefill has 572 channels (#21)

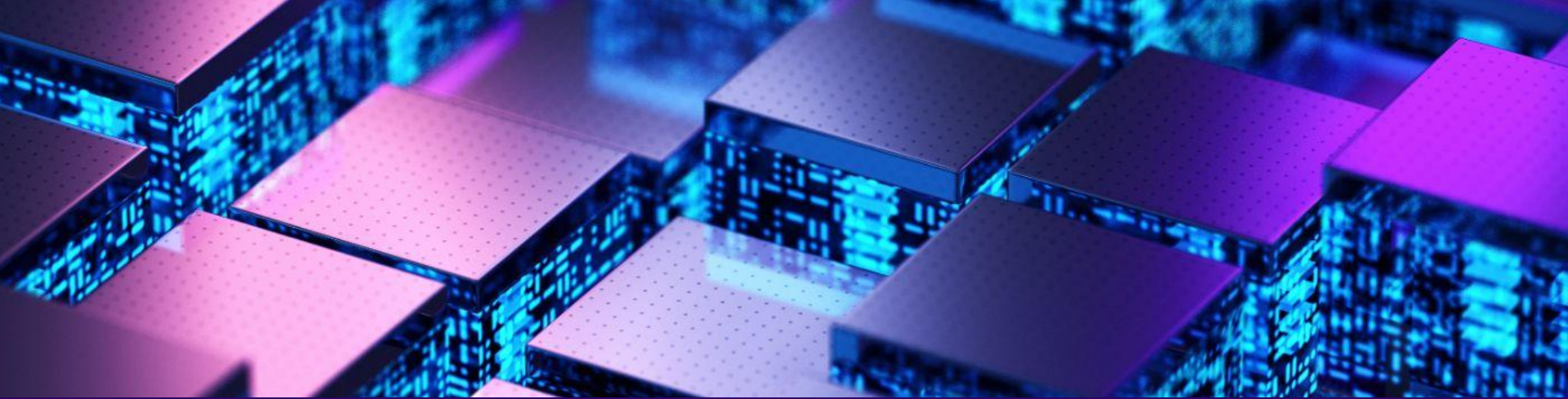
# The Lightning Network is Opaque

- Bitcoin transactions are totally public
- Lightning transactions are not recorded on the blockchain
  - Only channel open / closes are recorded
  - This only records *net* flow
  - [Channel open / closes are obfuscated, they look like ordinary 2-of-2 multisig transactions](#)
- Lightning nodes gossip known channels
- Lightning topology can be approximated by running a lightning node
- This method is [inexact](#)

# Channel Sizes



<https://bitcoinvisuals.com/ln-capacity-per-channel>



# Problems with Lightning

# Problems

- Custodial
  - FinCen will likely view custodial Lightning nodes as Money Services Businesses and regulate them as such
- Non-custodial
  - It's hard to run a node
  - If you wanted to support 1B lightning channels the channel opens alone would consume 3 years of block space



# Technical Details

- [Bitcoin Lightning Network Explained: How it Actually Works](#)
- [Bitcoin Lightning Transactions & Protocol Deep Dive](#)