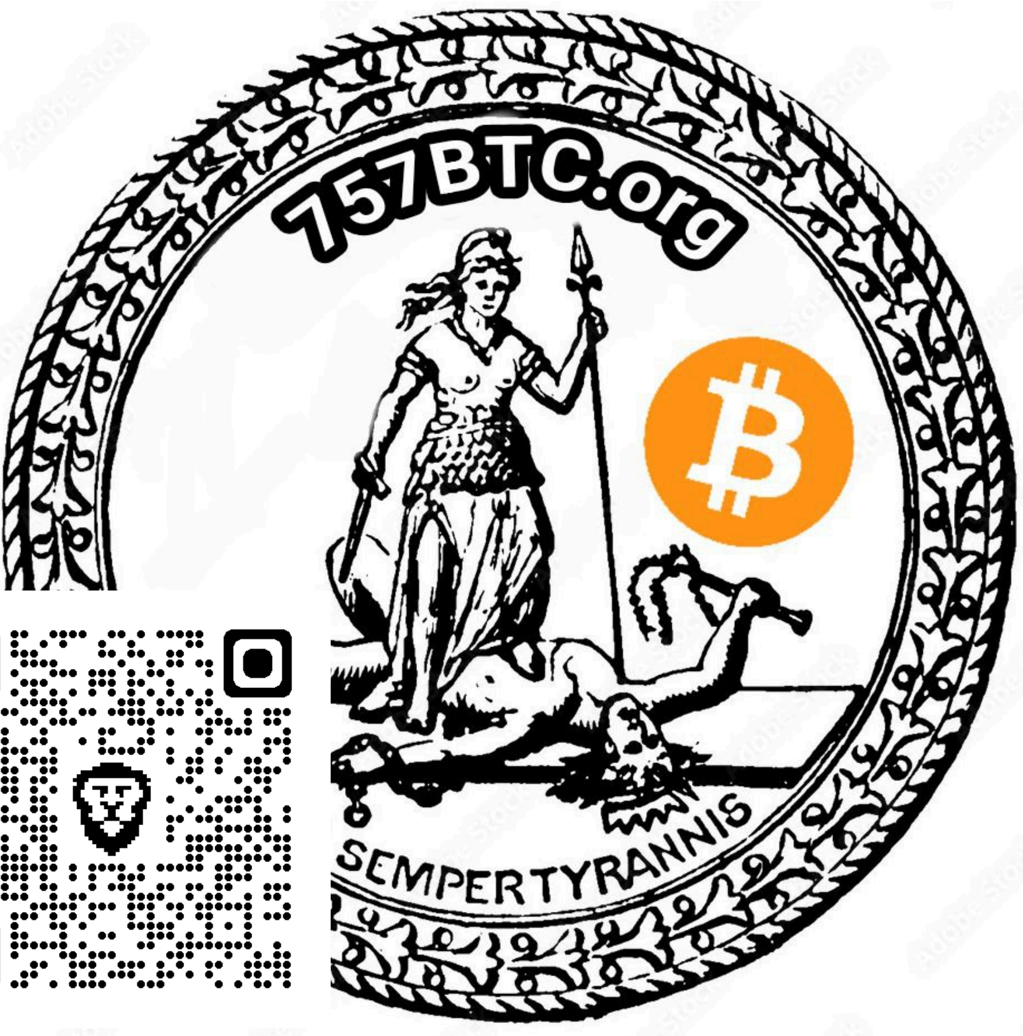
Bitcoin Lightning Workshop

757BTC

https://www.757btc.org/

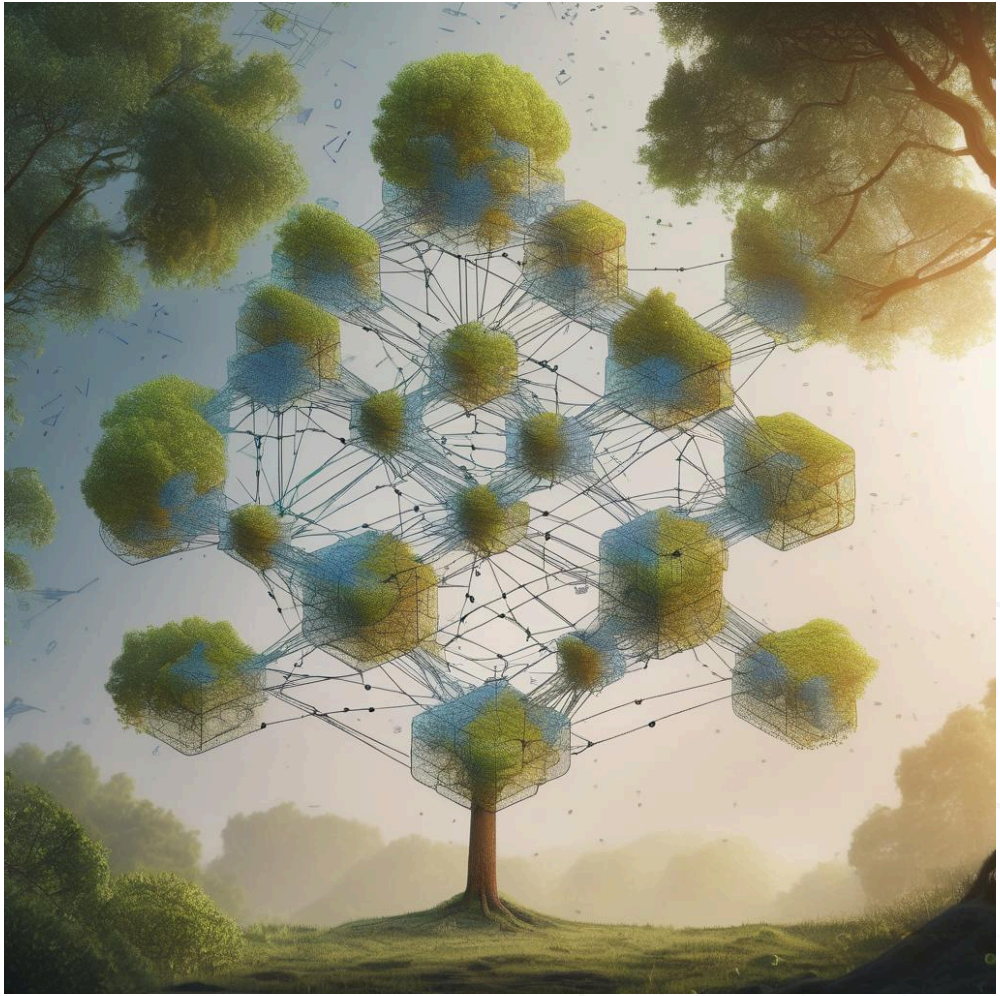


Topics

- Onchain Prereq
- Layer 2
- Types of Nodes
- Lightning Channels
- Liquidity
- Lightning Transaction
- Unilateral Exit
- Tools/Resources

Bitcoin Onchain

- UTXO (address with sats)
- Signing a transaction
- Multi-Sig
- Broadcasting a transaction
- Time and Money
- Most secure, finality, source of truth

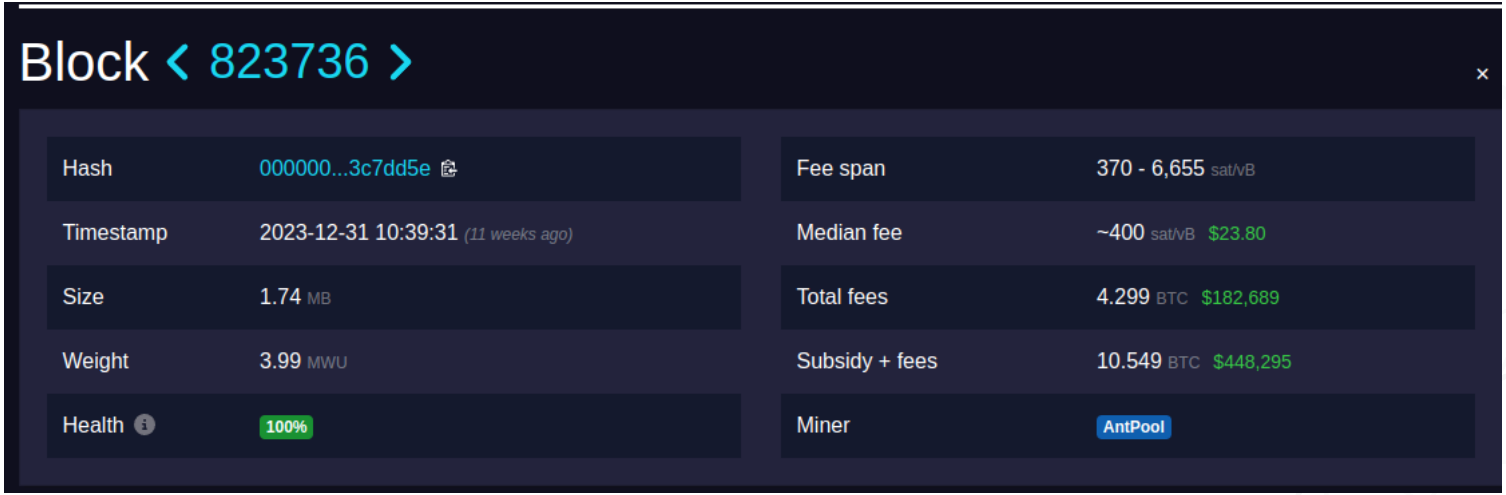


Bitcoin Layer 1 (Base Layer, On-chain)

- The most secure, decentralized, and self interacting layer
- Base Layer because this should be the anchor of all other layers
- On-chain because this layer is the bitcoin blockchain
  - You can send and receive bitcoin to the blockchain using wallet applications
  - Transactions are broadcasted and blocks are verified with Full Node servers
  - Transactions are stored and managed in Full Nodes’ Mempool
  - Bitcoin blocks are created with Miner servers

Onchain Fee Market

mempool
.space
Explore the full Bitcoin ecosystem®



Block < 823736 >

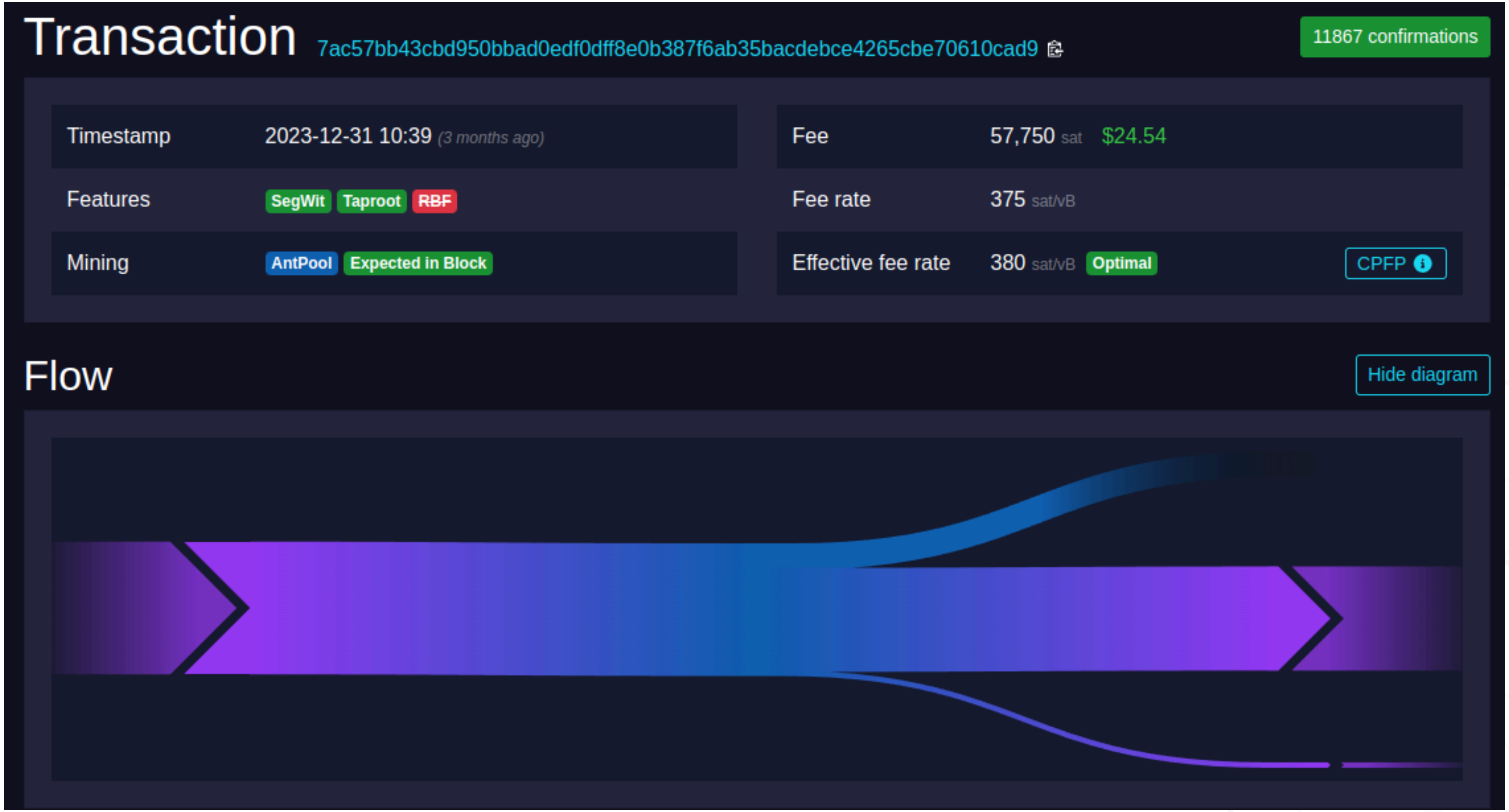
Hash	000000...3c7dd5e	Fee span	370 - 6,655 sat/vB
Timestamp	2023-12-31 10:39:31 *(11 weeks ago)*	Median fee	~400 sat/vB $23.80
Size	1.74 MB	Total fees	4.299 BTC $182,689
Weight	3.99 MWU	Subsidy + fees	10.549 BTC $448,295
Health	100%	Miner	AntPool

- When demand is high, onchain fees can be high (fees based on block space)
- Unspent Transactions (UTXO) or Bitcoin address with sats needs to hold large amounts of sats (roughly at least 20,000 sats)

Transaction Example

mempool
.space

Explore the full Bitcoin ecosystem®



Transaction 7ac57bb43cbd950bbad0edf0dff8e0b387f6ab35bacdebce4265cbe70610cad9

11867 confirmations

Timestamp	2023-12-31 10:39 *(3 months ago)*	Fee	57,750 sat $24.54
Features	SegWit Taproot ~~RBF~~	Fee rate	375 sat/vB
Mining	AntPool Expected in Block	Effective fee rate	380 sat/vB Optimal CPFP

Flow

What is a layer 2?

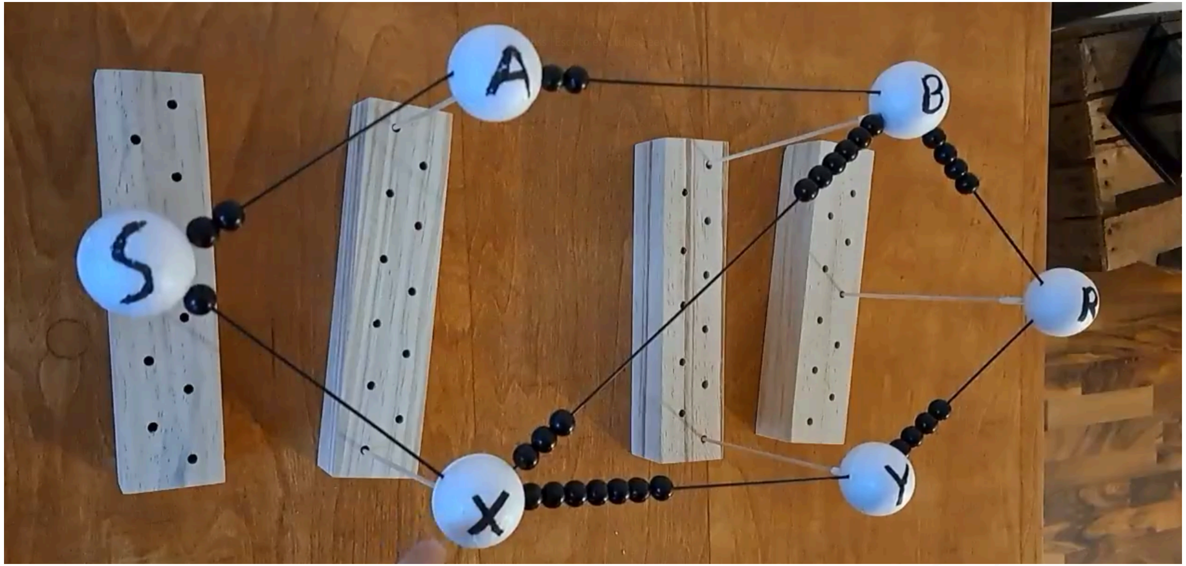
- Another way to represent bitcoin that is not on chain
- Could be:
    - I.O.U. with your friends (do you trust your friends)
    - Bar tab (do you trust the bar, does the bar trust you)
    - How can we keep track of the the state and how can we do it in a trustless way?
- Desired:
    - Anchored to on-chain (source of truth)
    - Unilateral exit
    - Privacy
    - Cheaper fees
    - Faster transactions

Bitcoin Layer 2

- Base layer is too slow and too expensive (for small transactions)
- On-chain is great for wealth storage but not so great for day to day spending
- Shared UTXO concept
  - How can we more efficiently utilize a single UTXO of bitcoin for transactions with a group of people?
  - How can we maintain control to each user (unilateral exit to base layer)
- **You don’t get speed and cheap fees for free, there will be trade off’s**
  - Everyone must choose what risk/reward is best for them based on their needs of Bitcoin
  - Understanding the risks is difficult

Lightning Bitcoin

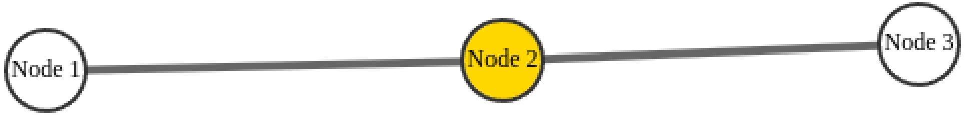
Lightning Layer 2



- Peer-to-Peer Channel
- Multisig shared UTXO
  - onchain is truth!
- Near Instant Tx (in ms)
- Transaction fees low based on amount of sats transacted instead of block size (small amount of sats small fee, large amount sats large fee)
- Both peers (lightning node server) need to be online for a transaction
- Unilateral Exit

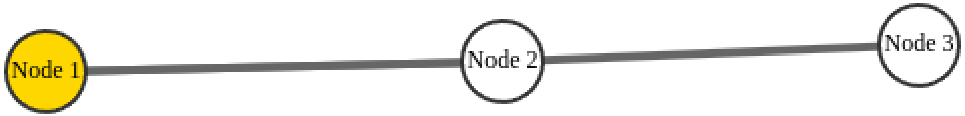
Types of Lightning Nodes (Routing)

- Routing Node (Clear-net or Tor)
  - Is the backbone of the network and handles the routing of sats across the network
  - Clear-net address or domain (https://example.com)
  - Tor address generated:
    fgb7kdu523n5c5v6bwwipovubdwaiqvkofgsgjwjedfbhdx5umtf22yd.onion:9735



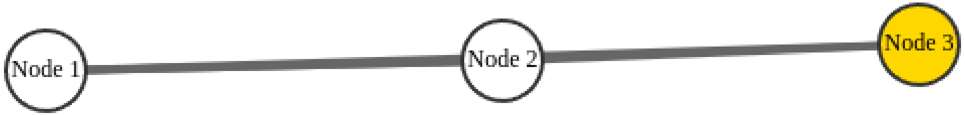
Types of Lightning Nodes (Private Node)

- Private Node (edge node)
  - Specific use node for individuals or for organizations (relies on private channels that are hidden and can’t be routed with)
  - channel is not broadcasted over the lightning network



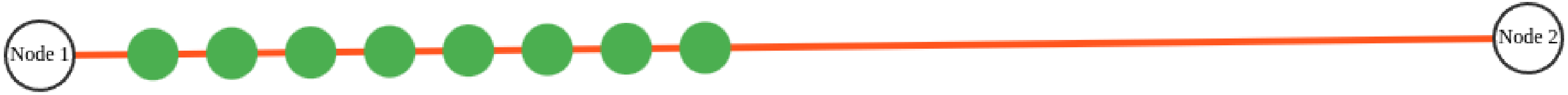
Types of Lightning Nodes (Loop Node)

- Lightning Loop Node (edge node)
  - Special service node run by large liquidity nodes to facilitate moving sats on and off of the lightning network



Lightning Channel Open

- Channels are established as a 2x2 multisig between two peers
  - Onchain Transaction
- When the channel is opened all sats are with the peer that opened the channel
  - Outbound capability



Lightning Liquidity

- potential to move sats from one end of the channel to the other
    - inbound
    - outbound
- Starts as all outbound to the peer that opens the channel
- Inbound is the most challenging to get
    - LSP’s and Routing nodes offer inbound liquidity for sale (they open a channel to you)
    - Spend sats from your channel increases inbound liquidity
    - Loop out sats to get inbound liquidity
- Routing nodes have to manage channels

Lightning Transaction (Not Push)

- Routing and path discovery
    - handled by the sender
    - only the sender knows the full path
    - (every intermediary node and final node don’t know)
- Onion routed transaction
- Hashed Time Lock Contract (Requires Invoice)
    - Hash function is one way compressed function (black box analogy)
    - Time constraint
    - Incentive propagation to prevent cheating and encourage cooperation
- Lightning channel state and updated close tx signed by both peers

Channel Closure

- Broadcasting the channel close tx (defaults to on chain wallet of node, can be specified as different for example cold storage)
- Cooperative - both peers agree to the closure, low fee and fast close time
- Forced - one peer just closes the channel, higher fee and time lock
    - Unilateral
    - time lock to allow settlement and agreement of any pending htlc’s
- Justice Transaction (special case in forced closure)
    - If node is caught cheating (closing channel state is not the latest)
    - all the sats allocated to that channel go to the victim

Lighting closure comparison

Feature	**Collaborative Close**	**Forced Close**
Who initiates	Both parties	One party (unilateral)
On-chain fee	Low	High
Speed of fund access	Fast (1 block)	Slower (due to timelocks)
Used when	Cooperative shutdown	Peer is offline/unresponsive
HTLC handling	Off-chain clean settlement	On-chain, messy resolution
Risk of penalty	None	Yes, if you broadcast stale state

Lightning Node Recovery

- **Seed phrase** of on chain wallet of lightning node
  - All channel closures will default to that wallet
  - back this up like any seed phrase
- If node goes offline seed phrase will always work, but channels remain open
- Static Channel Backup (encrypted with seed phrase)
  - file that has the list of channels
  - the peers associated with each channel
  - the ability to message the channel peers and initiate a force closure through them
  - back this up every time a channel is opened or closed (keep somewhere safe digital)

Resources (Nodes)

- Lightning Nodes (LND, CLightning, LDK, BreezSDk)
    - LND (most common)
        - https://github.com/lightningnetwork/lnd
    - Core Lightning (Clnd)
        - https://corelightning.org/
    - Lightning Development Kit (LDK)
        - https://lightningdevkit.org/
    - Breez Software Development Kit (Breez SDK)
        - https://breez.technology/sdk/

Resources (Mobile Nodes)

- Mobile Nodes (Zeus, Breez, Phoenix)
  - Zeus
    - https://zeusln.com/
  - Breez
    - https://breez.technology/
  - Phoenix (Just recently allowed back in the US)
    - https://phoenix.acinq.co/

Resources (LSP Based Apps)

- LSP Based apps (Strike, Cashapp, Wallet of Satoshi, Lnbits, Alby hub)
  - Strike
    - https://strike.me/
  - Cashapp
    - https://cash.app/
  - Wallet of Satoshi (WoS)
    - https://www.walletofsatoshi.com/
  - LnBits (Self hosted LSP)
    - https://lnbits.com/
  - Alby Hub (Self hosted LSP)
    - https://albyhub.com/

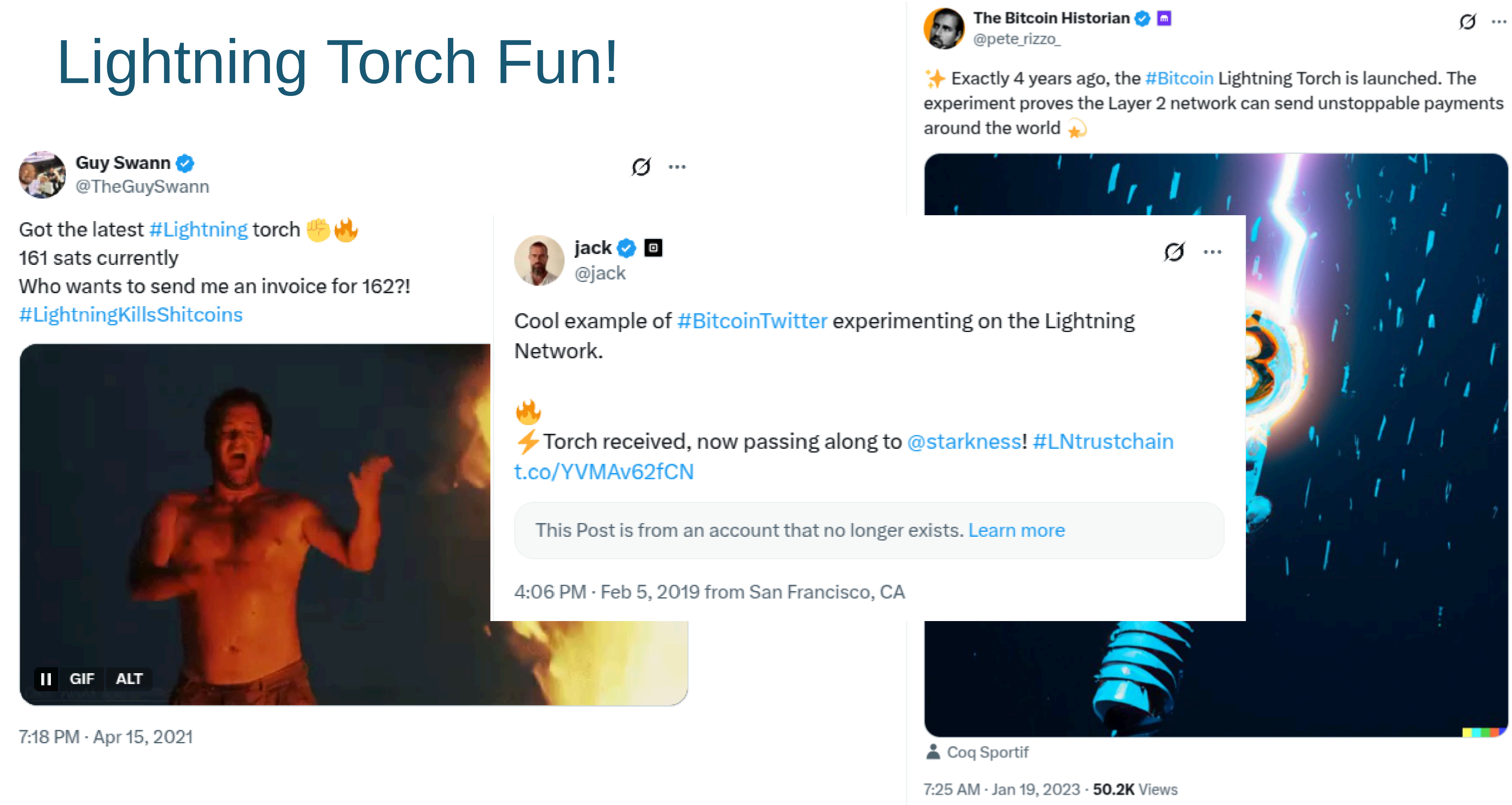
Resources (Loop Services)

- Loop services (Loop, Boltz)
  - Loop
    - https://lightning.engineering/loop/
  - Boltz
    - https://boltz.exchange/

Resources (Node Management)

- Chantools (open source terminal tools to recover lightning funds)
  - https://github.com/lightninglabs/chantools
- Node Management (Balance of Satoshis, Lightning Terminal, Ride the Lightning, Thunderhub)
  - https://github.com/alexbosworth/balanceofsatoshis
  - https://terminal.lightning.engineering/
  - https://github.com/Ride-The-Lightning/RTL
  - https://www.thunderhub.io/

Lightning Torch Fun!



Guy Swann
@TheGuySwann

Got the latest #Lightning torch ✊🔥
161 sats currently
Who wants to send me an invoice for 162?!
#LightningKillsShitcoins

7:18 PM · Apr 15, 2021

jack
@jack

Cool example of #BitcoinTwitter experimenting on the Lightning Network.

🔥
⚡Torch received, now passing along to @starkness! #LNtrustchain
t.co/YVMAv62fCN

This Post is from an account that no longer exists. Learn more

4:06 PM · Feb 5, 2019 from San Francisco, CA

The Bitcoin Historian
@pete_rizzo_

✨ Exactly 4 years ago, the #Bitcoin Lightning Torch is launched. The experiment proves the Layer 2 network can send unstoppable payments around the world 💫

Coq Sportif

7:25 AM · Jan 19, 2023 · 50.2K Views