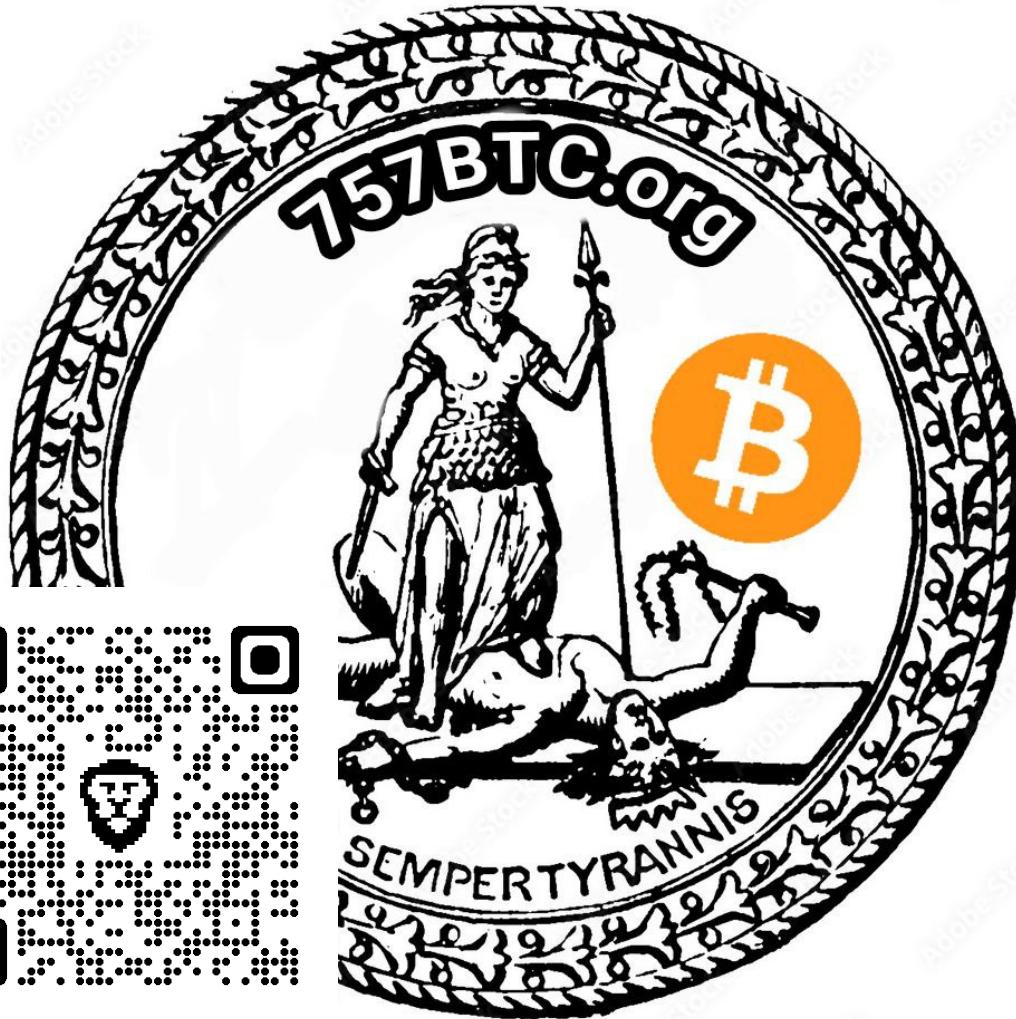


Bitcoin Layers

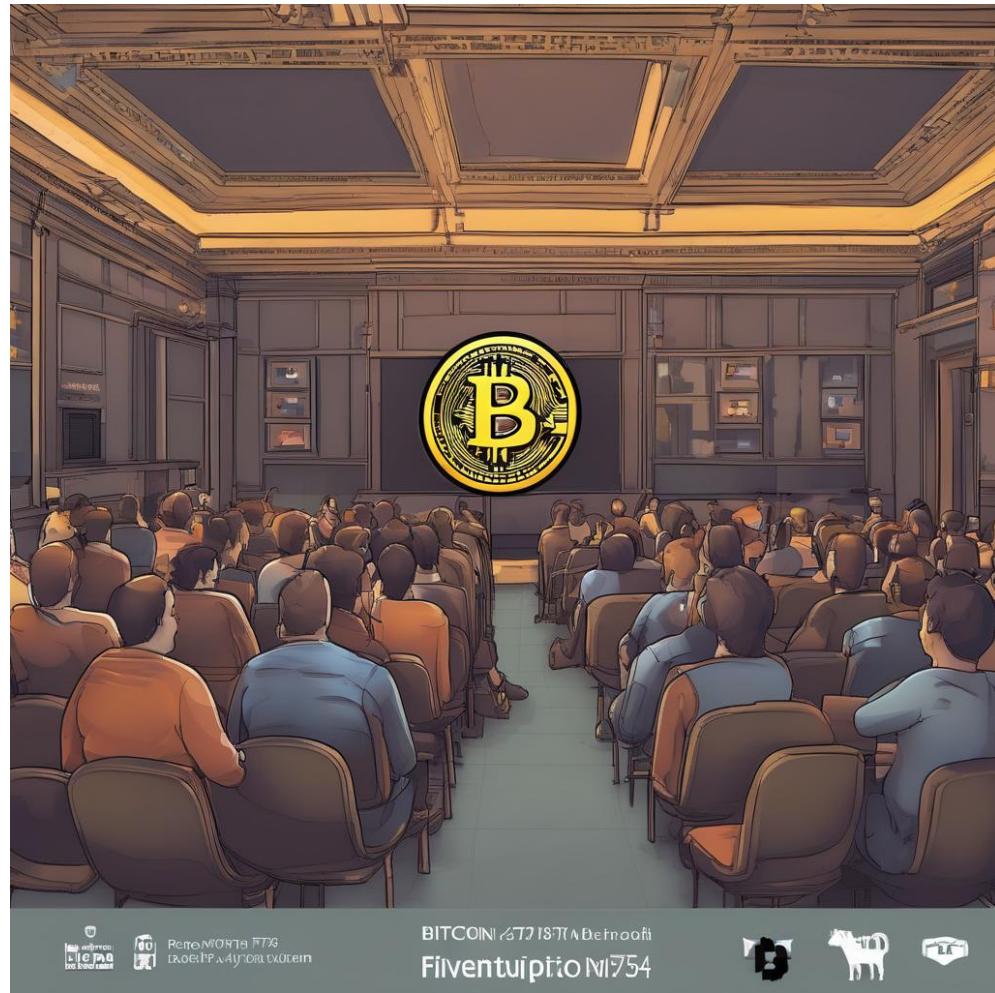
757BTC

<https://www.757btc.org/>



Topics

- Typical tech stack, why layers
- Bitcoin Layer 1 (Onchain)
- Bitcoin Layer 2 (Liquid and Lighting)
- Bitcoin Layer 3 (Cashu and Fedimint)
- How to choose



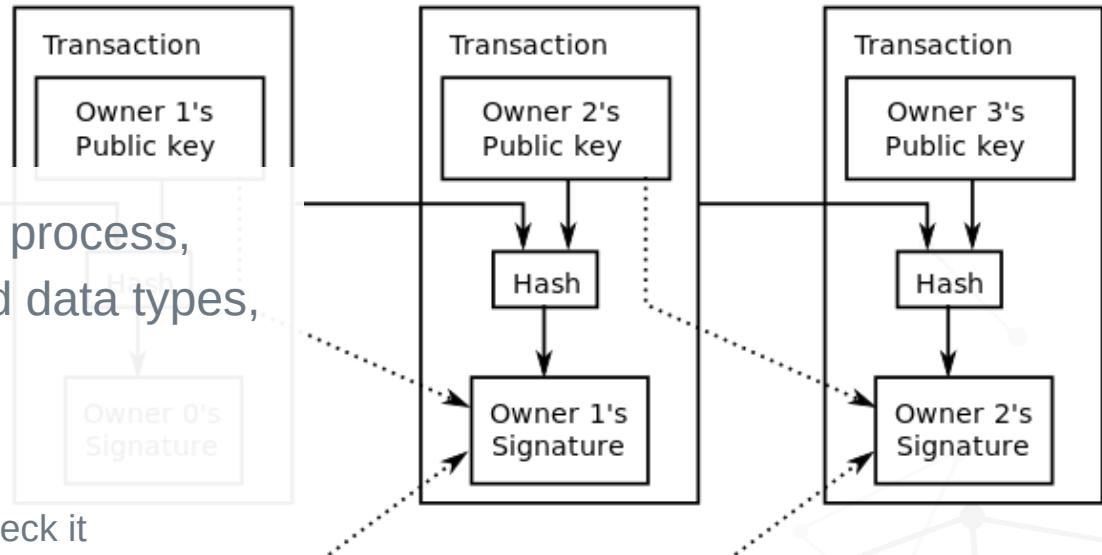
Bitcoin Layers

- Layers enable segregation of application
 - Allows for multiple teams of developers working on each layer
 - Allows for debugging and system resilience
 - Allows for more tools to be built
- Examples
 - Networking layers
 - Computing system layers



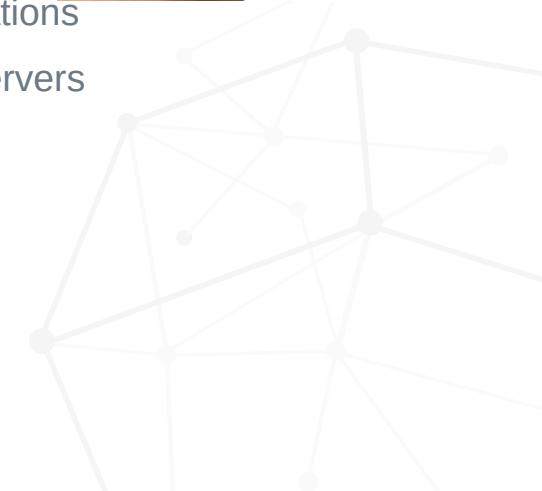
Bitcoin the protocol

- Set of rules that describe the process, how to interact, message and data types, variables, and incentives
- Open sourced
 - anyone can view the code and check it
 - anyone can build on it
- Built in a way that any application can easily interact with it as long as the specification is met

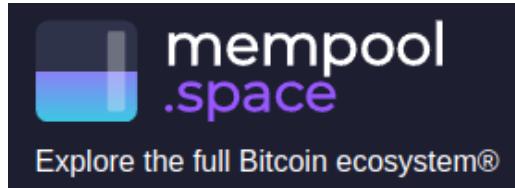


Bitcoin Layer 1 (Base Layer, On-chain)

- 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



Block < 823736 >

Hash	000000...3c7dd5e	Copy	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



Transaction

7ac57bb43cbd950bbad0edf0dff8e0b387f6ab35bacdebce4265cbe70610cad9 [🔗](#) 11867 confirmations

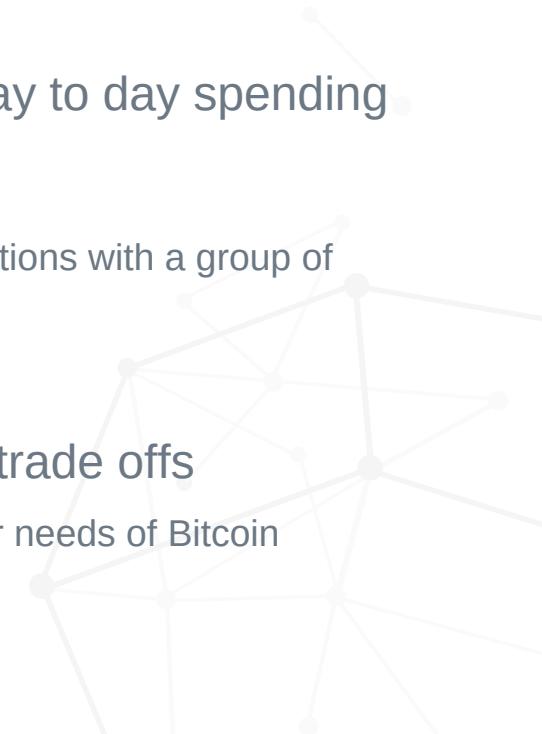
Timestamp	2023-12-31 10:39 (3 months ago)	Fee	57,750 sat \$24.54
Features	SegWit Taproot RBF	Fee rate	375 sat/vB
Mining	AntPool Expected in Block	Effective fee rate	380 sat/vB Optimal
			CPFP ⓘ

Flow

Hide diagram

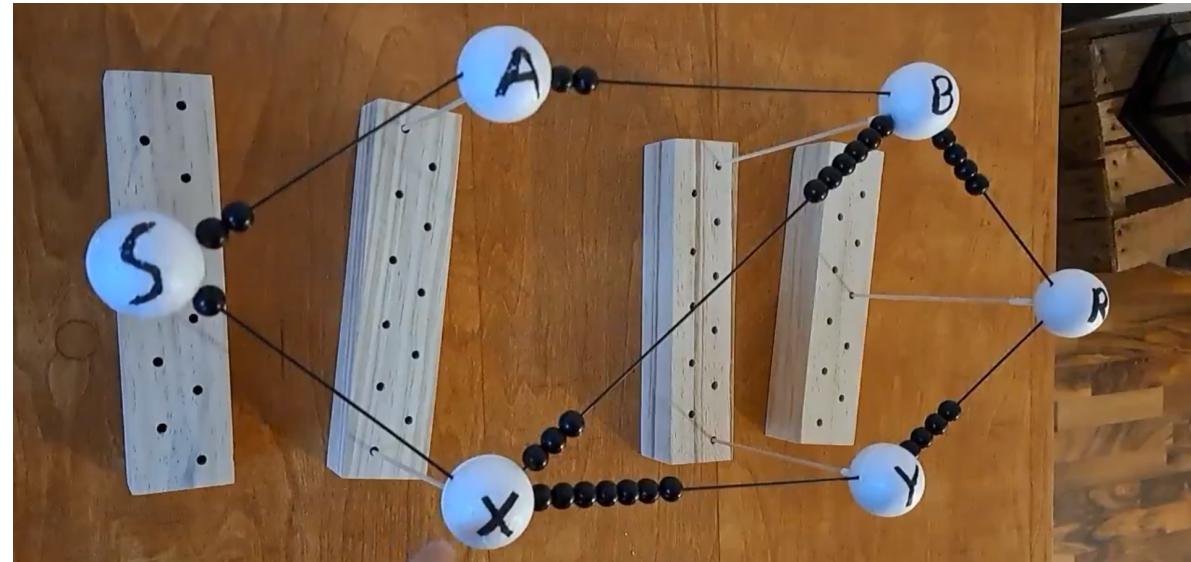
Bitcoin Layer 2

- Base layer is too slow and too expensive
- 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 offs
 - Everyone must choose what risk/reward is best for them based on their needs of Bitcoin
 - Understanding the risks is difficult



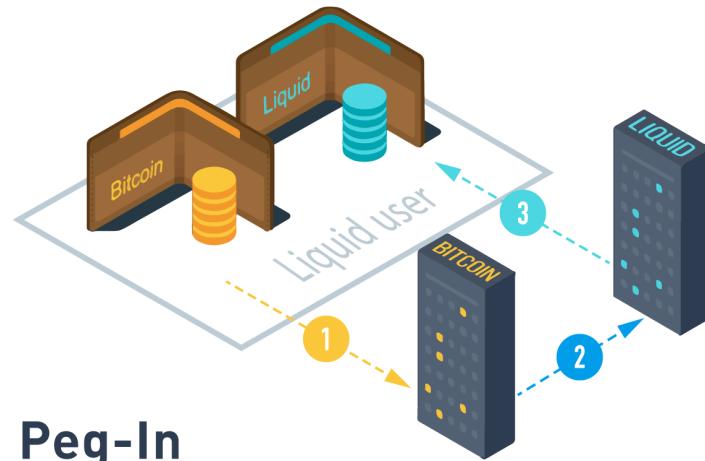
Lightning Layer 2

- Peer to Peer Channel
- Liquidity (in/outbound)
- Multisig shared UTXO
- Both peers (lightning node server) sign transaction
- every time a transaction occurs both peers update the closing channel transaction (signed and everything) but don't broadcast it until one of the peers wants to close
- closing transaction sends portion of utxo back to each peer based on latest state



Liquid Layer 2

- Federated system
- Liquid requires blocks be signed by at least 2/3's of all block signers
- Round Robin signing, the rest of signers verify the transaction
- 1 minute block times, Larger block size
- Confidential transactions (not even the signers can see)
- Unilateral exit to on-chain (17 minutes roughly)

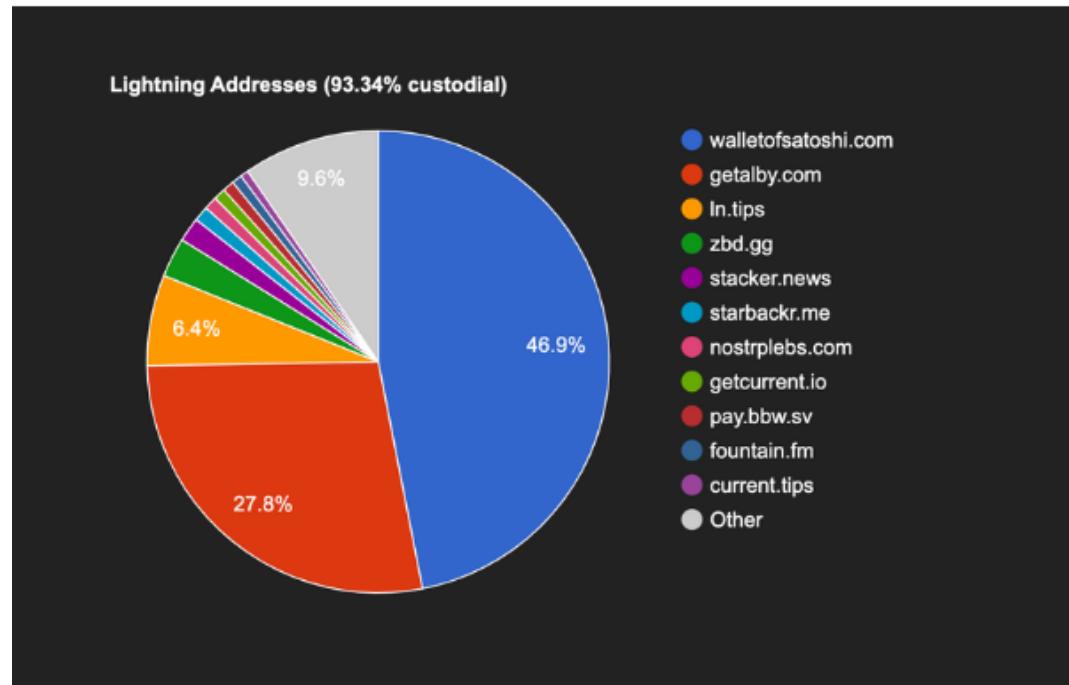


Peg-In

- 1 Liquid user sends BTC over the Bitcoin Network to peg-in address.
- 2 Liquid user waits for 102 confirmations. Functionaries in Liquid Network now accept this freezing of BTC and allow access to L-BTC.
- 3 Liquid user claims L-BTC and it appears in their Liquid wallet.

Layer 2 Utilization

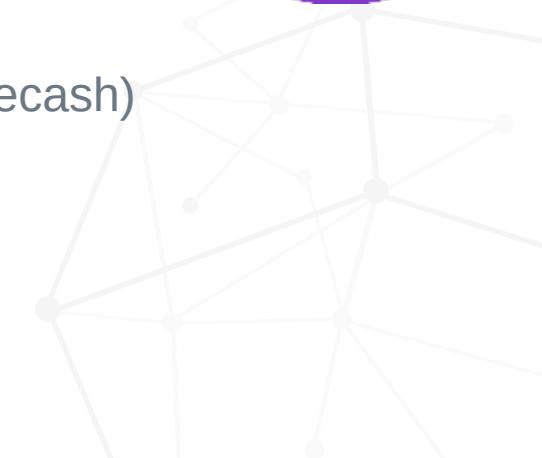
- Lightning most utilized
- Podcast 2.0
- Nostr
- P2P payments
- Online Payments
- Rewards and small transactions
- 93.4% custodial....
- Privacy Sucks...



Layer 3 (Chaumian Ecash)



- Can users get the custodial experience but with privacy?
- David Chaum created Ecash cryptography in the 80's
- Using the Blinded Signature
- Mints can mint ecash from pegged sats
- Creates digital lightning giftcards that can be subdivided (ecash)
- ecash can be redeemed whenever you want
- ecash can be traded between users anonymously offline



Cost/Benefit of Bitcoin Custody

- Custodial vs non-Custodial
- KYC and AML
- Privacy Ramifications
- Forward Privacy
- Tips and Tools

