

# Lightning, Explained Properly

The mental model most explanations skip, including the one constraint that actually matters: liquidity.

## What Lightning Is

Lightning is a peer-to-peer payment network built on top of Bitcoin. Near-instant settlement, fees measured in fractions of a cent, and payments that never hit the public blockchain. The core insight: not every coffee needs to be recorded on a global ledger forever.

## The Building Block: Payment Channels

A channel is a 2-of-2 multisig contract between two parties.

- **Open:** Alice and Bob lock bitcoin into a shared address (one on-chain transaction)
- **Transact:** they update balances between themselves as many times as they like, instantly, off-chain
- **Close:** the final balance settles on-chain (one more transaction)

**Why it's trustless:** each party always holds a signed transaction that recovers their funds unilaterally. If Bob vanishes, Alice publishes it and gets her money. And if Bob tries to publish an old balance that favors him, the revocation mechanism lets Alice claim everything he had in the channel. Cheating is economically suicidal.

## The Network: Chaining Channels

Alice —channel—> Bob —channel—> Carol

Alice can pay Carol through Bob without a direct channel. What stops Bob from pocketing the payment? **HTLCs** (hash time-lock contracts): Carol creates a secret, the payment is locked to its hash at every hop, and revealing the secret to claim one hop lets everyone upstream claim theirs. The whole chain completes or nobody gets paid.

## Liquidity: The Part Everyone Skips

**You can only send what you have, and you can only receive what your channel partner has on their side.**

Term	Means	Practical effect
Outbound liquidity	Capacity to send	Limited by your channel balance
Inbound liquidity	Capacity to receive	New wallets often can't receive until someone opens capacity toward them

This is why Lightning isn't "install and forget" at the node level, and why modern wallets pay Lightning Service Providers to make liquidity invisible to you.

## BITCOIN BUTLERS

### Three Ways a Channel Ends

Close type	What happens	Cost
Cooperative	Both online, agree, sign together	Clean, fast, cheap
Force close	One side publishes unilaterally; funds time-locked for safety	Slower, pricier
Breach ("justice")	Someone published an old state; the victim claims everything	Catastrophic, for the cheater

### What This Means for Self-Custody

- **Lightning is real Bitcoin.** Same asset, different layer.
- **It is a hot wallet by nature.** Keys must be online to receive and route. Spending money, not savings.
- **Channel backups are not seed phrases.** They're separate and both matter.
- **Custodial Lightning wallets defeat the purpose.** Convenient, but someone else holds the keys.

### The Sensible Path

Stage	Use	Notes
Learning	Small amounts, any reputable wallet	Training wheels are fine with pocket change
Spending	Phoenix or Breez (non-custodial)	Self-custody with the liquidity handled for you
Power user	Zeus + your own node	Full control, full responsibility
Savings	Not Lightning	Cold storage on-chain. Always.

### Common Fears, Answered

- **"What if my channel partner disappears?"** You hold a commitment transaction that recovers your funds without them.
- **"What if they cheat?"** The justice mechanism takes everything they had in the channel.
- **"What if I lose my phone?"** Seed phrase plus channel backup restores you.
- **"Is Lightning less secure?"** Different threat model, not a worse one. Use it like a checking account, not a vault.

**We accept Lightning for everything**, consultations and hardware both. Want help setting up a non-custodial Lightning wallet, or graduating to your own node? One session: [bitcoinbutlers.com/butlers](https://bitcoinbutlers.com/butlers)