

Understanding Lightning

How good do you know Lightning?

How many (public) nodes exist in LN?

How many channels exist in LN?

How much BTC is stored in LN?

Has Alice a channel with Bob?

Where is the money?

LN in numbers

Number of Nodes	Number of Channels	Network Capacity
14,625 ↑ +0.11%	61,028 ↓ -2.6%	5,015.50 BTC ↓ -5% \$205,596,859.29

How many (public) nodes exist in LN? ~ 15.000

How many channels exist in LN? ~ 61.000

How much BTC is stored in LN? ZERO! NONE! sats are only IOU's!!!

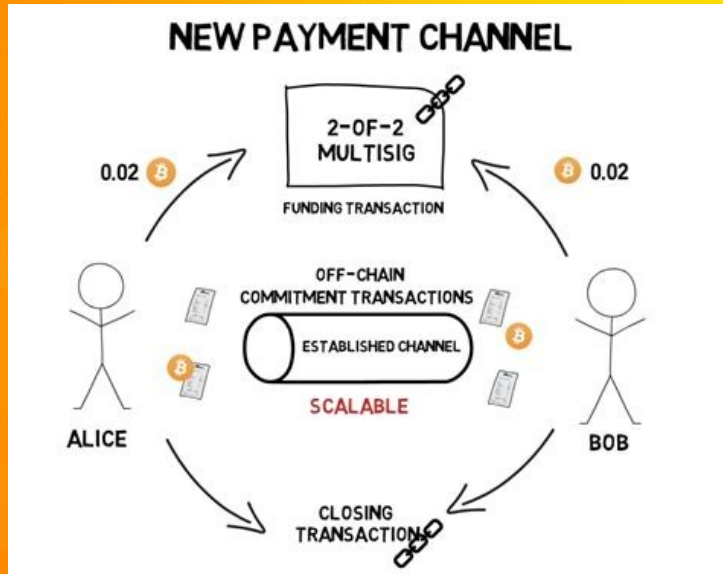
Has Alice a channel with Bob? NO! (if Bob isn't running a node)

Where is the money? Allways in smart contracts on BTC main chain

THE basics!

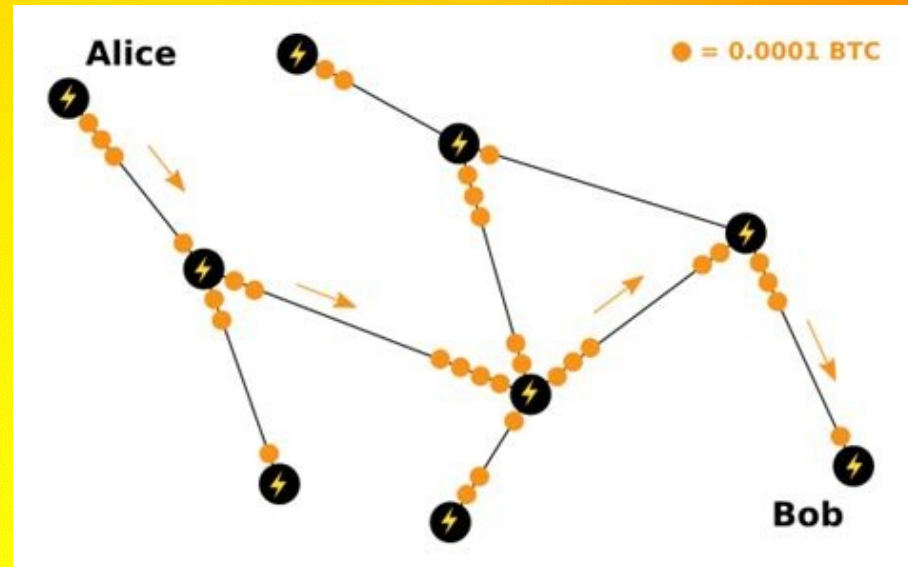
BTC are onchain (in smart contracts)

This is a channel (to a node)



sats are minted (open) and redeemed (close)

This is a route to Bob



ELI5 for LN

- 50 € cash deposit (at the bar)
- IBAN as the return address
- beer tap as LN account
- every mark is an transaction
(waitress should have a copy)
- payment when leaving
(mutual closing)
- change to bank account
(forced closing → guest disappeared)



More basics

- use cases
- wallets
- nodes
- channels
- LSP's
- routing
- invoices
- addresses
- fees

LN use cases

1. payments

(POS + online / pull or push / subscriptions / scheduled+recurring payments / split payments)

buy online <https://plebeian.market/> [ShopinBit](#) [Online-Shops](#)

buy local [BTCMap](#) (App)

2. spend zaps → Nostr, Stacker News, Sparkshot, Bitrefill

3. login with LNURL Auth (Alby, Phoenix, Breez, Blixt, LNTipBot)

→ <https://lightninglogin.live/> <https://stacker.news/> [List](#)

4. use LApps ([WebLN](#) → with Alby, Breez, BlueWallet, Blixt, Joule)

Wallets

- desktop / web / mobile / integrated (Bot)
- LN+BTC vs. LN only
- custodial vs. noncustodial
- autopilot + LSP + autoswap
- light or full node included
- connect own node / n channels
- support LNURL / WebLN / LN address / Lapps / BOLT / TapRoot / slicing / LSP API
- OpenSource / free source / backup L1+L2 / Tor

→ [wallet overview](#)

Wallets

Browser: Alby

PWA: Mutiny

Telegram: LNTipBot

Beginner: Phoenix, Blue

Advanced: Zeus, Blixt

Profi: LNbits

Comparison of the privacy properties of lightning wallets

	Self-custodial	Block filters	Fetch block data from own node	SCID alias	Optional invoice wrapping	Client-side routing	Multiple LSPs	Android trackers ¹	iOS data collected (linked / unlinked)
Wallet of Satoshi	✗	✗	✗	N/A	N/A	✗	✗	0 ✓	1 / 0 ✗
Blink	✗	✗	✗	N/A	N/A	✗	✗	2 ✗	1 / 2 ✗
Alby	✗	✗	✗	N/A	N/A	✗	✗	N/A	N/A
Muun	✓	✗	✗	⚠ ²	✗	✗	✗	2 ✗	0 / 2 ⚠
Phoenix	✓	✗	✓	✗	✗	✗	✗	1 ✗	0 ✓
Bitkit	✓	✗	✓	✗	✗	✓	✗	?	TestFlight only ✗
Breez	✓	✓	✓	✗	✗	✓	✗	?	0 ✓
Mutiny	✓	✗	✓	⚠ ³	✓	✓	✗	?	TestFlight only ✗
Blixt	✓	✓	✓	✓	✗	✓	⚠ ⁴	0 ✓	0 ✓
ZEUS	✓	✓	✓	✓	✓	✓	✓	0 ✓	0 ✓

1. Data from Exodus Privacy <https://exodus-privacy.eu.org/en/>

2. Muun's company nodes are used for all lightning routing

3. Not used with Voltage Flow 2.0 LSP

4. Dunder LSP is FOSS but not used by any major provider yet

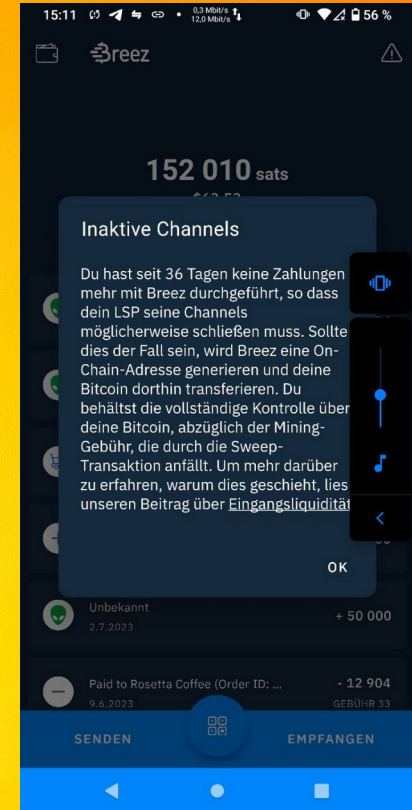
Last updated November 24, 2023

by 

Backup & recovery

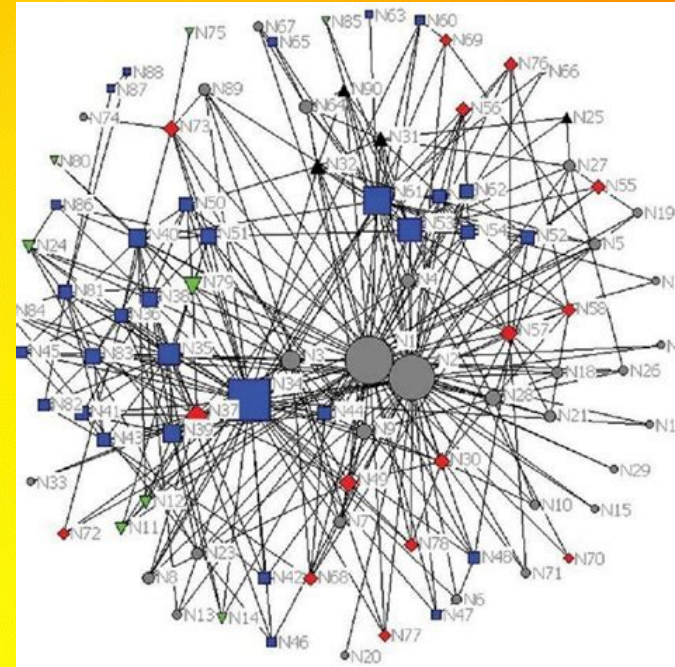
- L1 seeds
- L2 **channel state** → static channel backup (SCB), channel database
→ encrypted, own storage / wallet independent ??
- **recovery**
→ Breez is suboptimal (no L1 wallet → closing address)

Always test recovery before using the wallet!



Nodes

- private or public
- self managed or hosted
- end node and routing nodes
- full node or light node (SPV embedded in wallets)
- node criteria
 - # channels, capacity, good peers, centrality (hops)
 - age, balanced, response time, fees



Node rankings

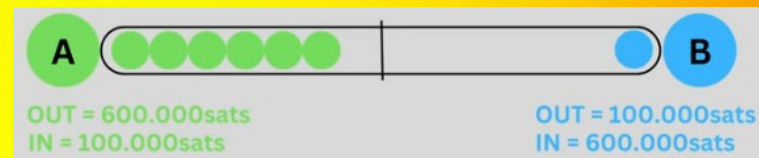
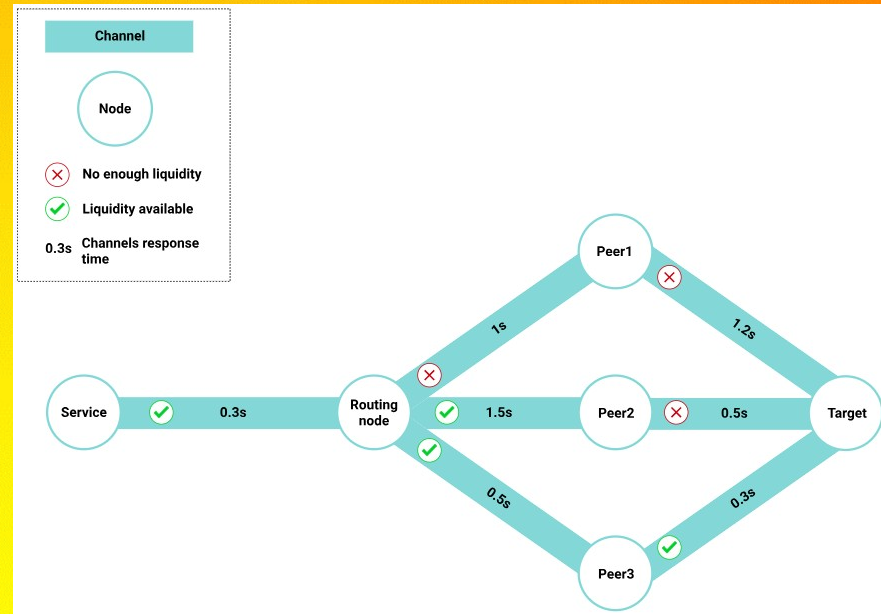
PEER			RESPONSE TIME		LIQUIDITY		CHANNEL		PEER			NODE		
Peer	Channels	Routing Score	Node	Average	Balanced	Ratio	ID	Capacity (sat)	Fee (ppm)	Base fee (sat)	Max HTLC (sat)	Fee (ppm)	Base fee (sat)	Max HTLC (sat)
ACINQ <small>Capacity 8472,35</small>	2147						820665x705x1 902330710054993921	100,000,000	699	1	20,000,000	200	0	20,000,000
nicehash-In1 <small>Capacity 8225,52</small>	1380						814079x1463x1 895089326524137473	300,000,000	1	0.1	297,000,000	10,000	0	297,000,000
nicehash-In1 <small>Capacity 8225,52</small>	1380						810899x443x1 891592879480963073	150,000,000	1	0.1	148,500,000	10,000	0	148,500,000
LQwD-Canada <small>Capacity 837,68</small>	1273						798690x810x1 878168942041497601	50,000,000	100	1	49,500,000	900	0	49,500,000
bfx-lnd1 <small>Capacity 8516,05</small>	972						710062x216x1							
bfx-lnd1 <small>Capacity 8516,05</small>	972													
LNB4G [Hub-1] <small>Capacity 8332,40</small>	899													

Routing Score Percentile (Rank)	Node	Capacity	Response time	Balanced	Hops to network	Features
98th (10)	02dfe525d9c5b4bb52a5 02dfe5...c114f8	818,20 152 channels 111ppm median	1s Channel Average	68% of all Channels	2.33 Liquidity adjusted	
93th (31)	c-otto.de 027ce0...843c71	841,99 124 channels 10ppm median	1.6s Channel Average	71% of all Channels	2.46 Liquidity adjusted	
89th (51)	OLYMPUS by ZEUS 031b30...99e581	810,21 63 channels 2100ppm median	1.5s Channel Average	100% of all Channels	2.62 Liquidity adjusted	
85th (67)	strike 034d7f...ebcf46	818,83 82 channels 3000ppm median	0.3s Channel Average	41% of all Channels	2.53 Liquidity adjusted	
84th (75)	MuRa\$HaL 03c62e...3acd3a	85,70 72 channels 250ppm median	1.1s Channel Average	67% of all Channels	2.48 Liquidity adjusted	
83th (78)	Ludwig 029267...f4330a	82,43 42 channels 249ppm median	0.6s Channel Average	68% of all Channels	2.5 Liquidity adjusted	

<https://Inrouter.app/node-ranking>

Channels

- connection between wallet + node
(via clearnet or Tor)
- **channel types** (custodial, private/public, zero-conf, zombie, TapRoot, wumbo)
- capacity (BTC locked = max. transfer)
- liquidity (inbound + outbound)
- duration (optional)
- commitment fee
- local reserve



Get connected

Open a channel

- a. manually → choose node, capacity, fee rate, (duration)
- fees for opening 3k-10k sats
- fees for closing 3k-40k sats (mutual or forced)
- simple TapRoot channel (better for fees+privacy)

The screenshot shows a mobile application interface for opening a channel. At the top, the status bar displays the time 11:05, signal strength, and battery level at 76%. The app's header is orange with a back arrow and the text "Open channel". Below the header, the "Node URI" field contains "fc226@170.75.163.209:9735" with a camera icon to its right. The "Amount sat" field is set to "250000" with an "ALL" button to its right. The "Amount USD" field shows "102.97". The "Fee-rate" field has a slider set to "101 sat/vB". The "Taproot channel" option is checked with a checkbox. At the bottom, a large orange button is labeled "OPEN CHANNEL".

11:05 8 76 %

← Open channel

Node URI fc226@170.75.163.209:9735

Amount sat 250000 ALL

Amount USD 102.97

Fee-rate 101 sat/vB

Taproot channel ☒

283 759 sats available

OPEN CHANNEL

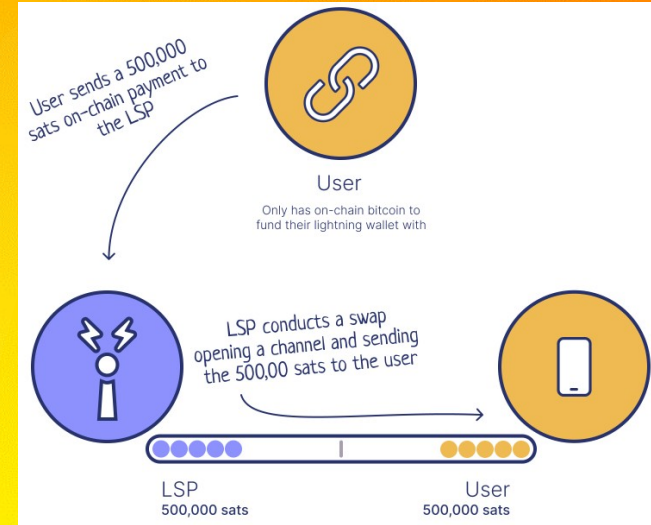
Get connected

Open a channel

b. autopilot (jit, instant, zero-conf)

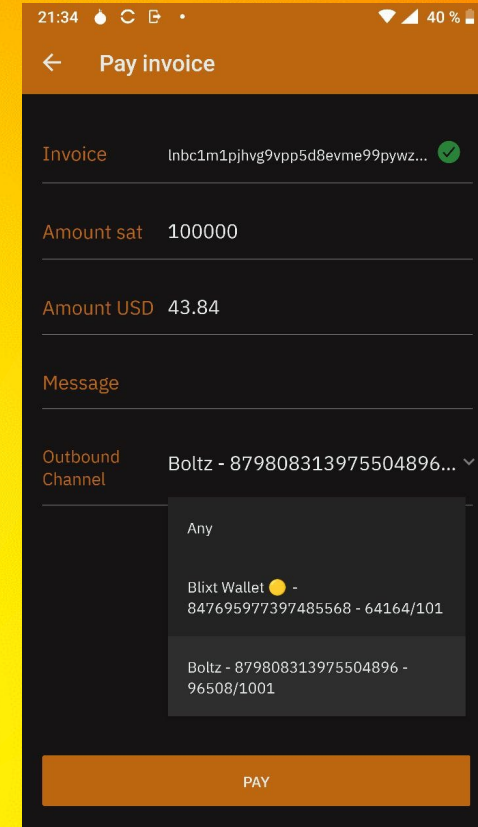
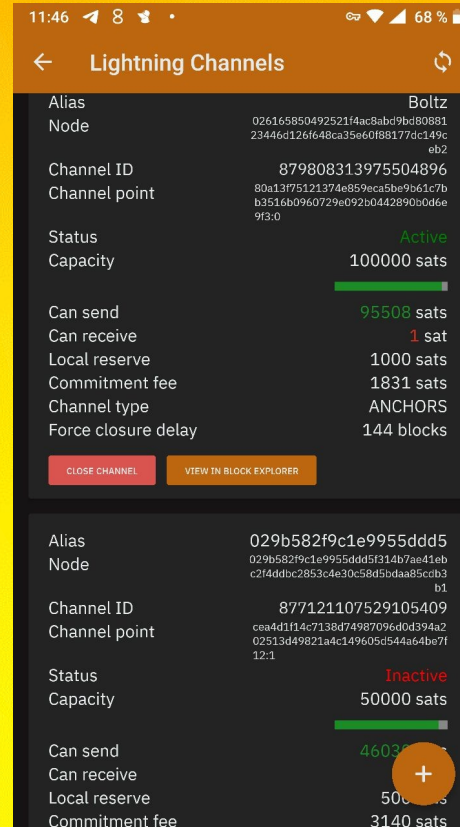
- create invoice / automatic opening / payment ./ fees
- the price covers the transaction of the channel opening, its future force closure and the price for renting funds (dual funded, forced close after xx days of inactivity)

Easy onboarding with LSP's → for the price of lock-ins (Breez, Acinq, Blixt, Olympus, a.o.)



Multi channels

- multi-channel wallets (Blixt, Zeus)
- own your channels
(no timeout closing)
- choose channel for tx
(big+inexpensive for funding,
leased channel for spending)
- manage your liquidity



LSP + LWS

- help users connect to the lightning network while **maintaining self-custody (assisted)**
- opening channels, and offering liquidity management
- support swaps, **LN addresses**, backup services
- realize offline payments (**tippin.me**) and watchtowers
- perform routing optimization

Use LSP's without lock-ins!

LSP API (specs) in progress



LSP rankings

1	WalletOfSatoshi.com 035e...c226	526	99th Percentile	23.7B sats 2.43% of Total	3 yrs Oldest 11%
2	LQwD-Canada 0364...07e1	162	99th Percentile	3.9B sats 0.4% of Total	17 mths Oldest 54%
3	nicehash-In1 0376...10ba	238	99th Percentile	22.6B sats 2.31% of Total	3 yrs Oldest 10%
4	Kraken ⚡ 02f1...0b69	326	99th Percentile	31.4B sats 3.21% of Total	21 mths Oldest 44%
5	LNBig Hub-1 034e...c0d5	241	99th Percentile	33.2B sats 3.4% of Total	5 yrs Oldest 4%
6	LNBig [Hub-2] 033e...b9c7	196	99th Percentile	29.6B sats 3.03% of Total	5 yrs Oldest 4%
7	bfX-lnd1 03cd...01d6	183	99th Percentile	51.6B sats 5.28% of Total	4 yrs Oldest 8%
8	bfX-lnd0 033d...e025	197	98th Percentile	27.5B sats 2.82% of Total	4 yrs Oldest 6%

getalby.com #45 Good			
Capacity	Age	Good Peers	Centrality
9.5B sats	23 mths	97 of 203	92nd

Breez #101 Good			
Capacity	Age	Good Peers	Centrality
2.8B sats	5 yrs	95 of 210	95th

OLYMPUS by ZEUS #112 Good			
Capacity	Age	Good Peers	Centrality
1B sats	10 mths	45 of 59	61st

Blixt Wallet #272 Good			
Capacity	Age	Good Peers	Centrality
1.2B sats	3 yrs	32 of 47	29th

ACINQ #606 Good			
Capacity	Age	Good Peers	Centrality
47.8B sats	5 yrs	104 of 1752	99th

<https://terminal.lightning.engineering/>

Payment routing

- nodes exchange routing informations (gossip)
- a network graph is established, stored and updated
- client or server side routing
- criteria (max. success rate, min. hops + fees)
- depending on amount, entry node(s), channels, multipath routing (AMP)
- invoices can contain information to support routing (privacy issue?)
- Tor, route blinding and rendezvous routing for better privacy

(Re) funding

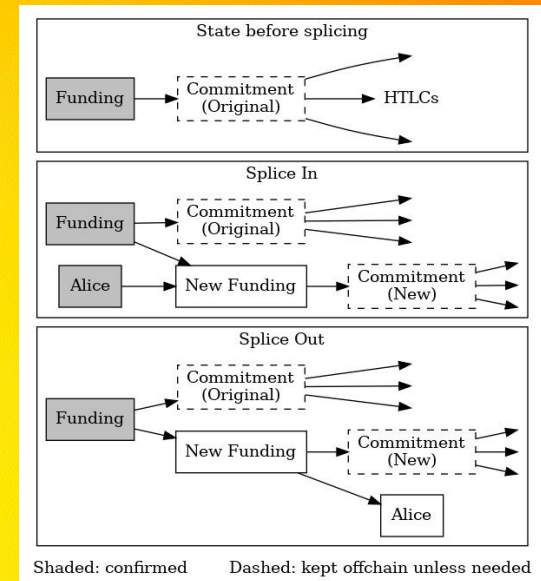
- swap in BTC
- splicing in/out
- swap in Fiat
- use vouchers
- non KYC services

Boltz, Coinswap, Deezy.io, FixedFloat
currently only with Phoenix

<https://pocketbitcoin.com/lightning>

Bitrefill a.o.

<https://kycnot.me/>



Invoices / addresses

- invoice – the basis of payment requests (BOLT 11)
- offers -- for pull payments, subscriptions, [etc.](#) (BOLT 12)
- LNURL – pay, withdraw, [address](#) (via https, needs webserver)
- Node ID – static payment endpoint
- overview of [payment request formats](#)

LN addresses start always with lnbc ...

[BTC addresses](#) start with 1 (legacy), 3 or bc1q (segwit) or bc1p (TapRoot)

Fees

L1 fees

open channel (depends on L1 fees)

- single funded → only L1 fees (for > 300 vByte)
- dual funded → L1 fees + renting fees (depending on channel duration)
- autopilot → differs much (intransparent, no market)

close channel → funded with local reserve (if too low, anchor channels support CPFP)

L2 routing fees (are peanuts, promille of L1)

send 15k sats via invoice Breez + Phoenix (62-64 sats = 0,4%)

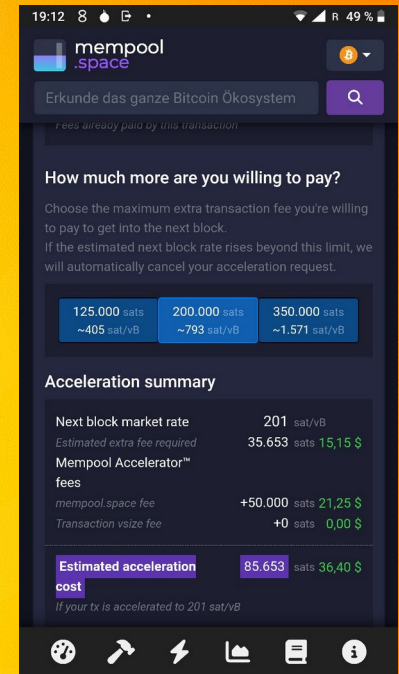
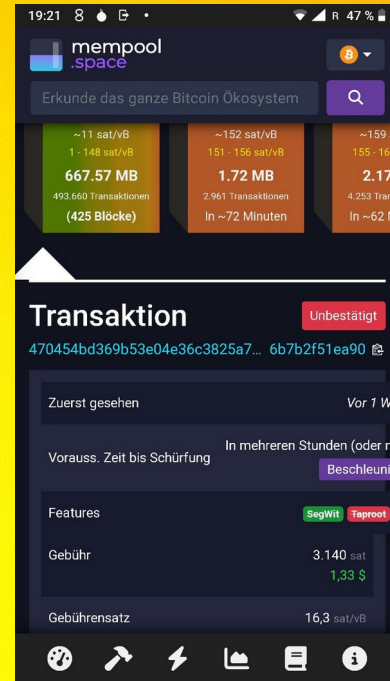
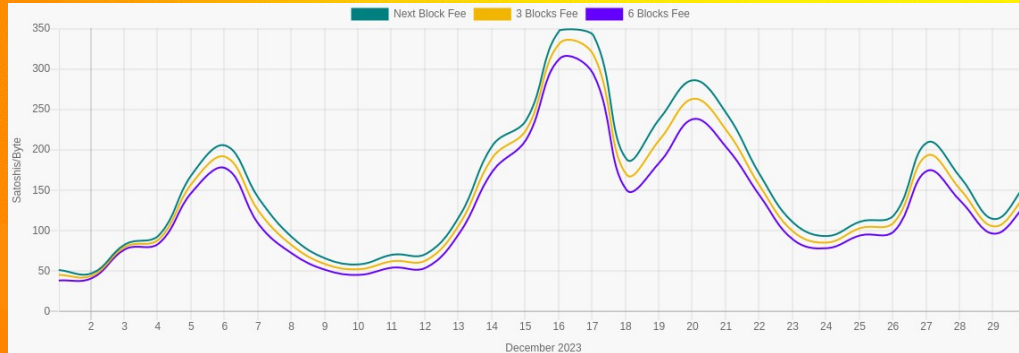
LNTipBot (5 sats = 0,03%), LNbits (0.5 % max 100 sats) → low fees with custodial wallets

transparency Breez, Phoenix, Zeus, Blixt, LightningTipBot

no transparency Alby, BlueWallet

High fee problem

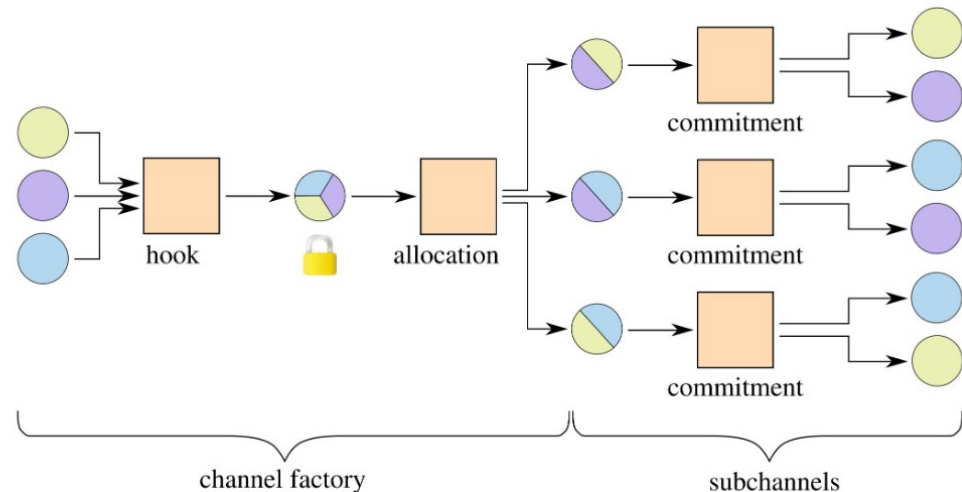
- channel closing failes (more zombies)
- channel opening too expensive



Possible solutions

- channel factories allow a # of users to maintain a single UTXO through a n-of-n multisig account
- multiparty channels (join pools)
- PTLC vs. HTLC
- timeout trees
- Ark (VTXO)
- ???

Channel Factories



Do's and dont's

Do's

- use OpenSource and open access wallets (GitHub)
- test wallet restore before usage
- use enough channel capacity
- use TapRoot channels

Dont's

- no L2 only wallet
- avoid autopilot channels
- avoid LSP lock-in

Recommendations

- | | |
|--------------------|---|
| - wallets | Alby / TG / Phoenix / BlueWallet / Zeus / Blixt |
| - node selection | I'm still learning |
| - LSP selection | check the features you need and the fee schema |
| - channel opening | choose lifetime channels, take a big ONE to fund all your wallets |
| - wallet funding | use non KYC swap in's |
| - fee optimization | optimize channel opening, avoid channel closing |
| - security | always make backups and test recovery |
| - privacy | take care on privacy from day 1, it's hard to blur traces |

Call to action

1. Alice & Bob

→ how can we stop this?

2. Uncle Jim (Shinobi)

- onboarding support

- multiparty channels

- Cashu

3. Banks without bankers (Eric Yakes)

- community nodes + LSP (Dunder)

→ liquidity lease

- Fedimint

→ off-chain lending

- Lightning Box

→ self-custodial address

- Nodeless.io

→ payment processor

FAQ

Any questions?

Standards

- BOLT (11 / 12)
- LNURL
- WebLN
- TapRoot
- LSP API (specs)

Education

- [ELI5 video](#)
- [Bitcoin Design Guide](#)
- [Plan B Network](#) [Kurse](#) [Rohmaterial](#)
- [Lightning Network Curriculum](#)
- [The Lightning Builders Guide](#)
- [Jameson Lopp's incredible collection](#)
- [LN invoice decode](#) [LN invoice decode with data](#)

Sources

LN Wallet overview

<https://bitcoin.design/guide/how-it-works/lightning-services/>

https://en.bitcoin.it/wiki/Lightning_Network

<https://bitcoiner.guide/lightning/>

<https://guide.bolt.fun/guide/>

<https://darthcoin.substack.com/p/getting-started-ln>

<https://www.lightning-landscape.net/projects>

<https://darthcoin.substack.com/p/lightning-network-is-awesome>

L1 fees <https://privacypros.io/tools/bitcoin-fee-estimator/> <https://btc.network/estimate>