Building Applications

LND for Developers, Developers, Developers

Design Philosophy

- Works end-to-end: you can just pay and receive, done.
- Community developed, releases on the cutting edge
- Soup to nuts APIs: signing, chain, logging, path finding

Integrating LND

- Current best option: GRPC
- In development: embed LND for mobile, etc
- Future: WASD support, install as a library

Chain Backends

- Use Bitcoin Core. btcd is very useful for testing though
- Neutrino: validating, more private SPV, sync in minutes
- Future: pruned mode, authenticated Neutrino

Chain Wallet

- AEZeed Format: BIP 39 + birthday, version, KDF
- LND is 2 wallets in 1: chain and channels.
- Chain aspects of LN are tricky and multi-stage

Channel Setup

- To receive, get in-bound capacity. Limit min-chan size
- To send, choose stable channels. Not the biggest ones!
- The future is autopilot, outsourced channel hassles.

Receiving Funds

- Payment requests vs invoices
- Normal features: expiry, fallback, description, hop hints
- LND features: internal descriptions, custom pre-images

Processing Receives

- Listen to the invoices subscription: internally, externally
- Move received payments through external db stages
- Guard pre-images until payment, then push them out

Sending Payments

- Query routes (local graph) to see if a payment is possible
- You can send to routes, (implement mission control)
- Chain sends are supported, future is splice-out, swaps

Balances

- Chain balance: vanilla, sweeps
- Limbo balance: timelocked, limbo, pending resolution
- Channel balances: reserve, minus commit fees

The Graph

- Everyone sees everyone else with public channels
- Channels have dual sided relationships: outgoing edges
- The future of apps is off the public graph

Wallet Security

- Hot wallet fails closed
- Macaroons scope run-time permissions
- Stay online, commit smaller amounts

Reliability

- Limit funds, shard across wallets, use iptables
- RAID can be used, but the future is a distributed db
- Static backups coming soon

Alts

- LTC support is included
- It’s fairly straightforward to swap in and out
- In the future the routing network will take care of it

Publish

- Don’t make closed source wallets
- LND has a wallet project you can fork, but it’s GPL
- Try to be a good citizen