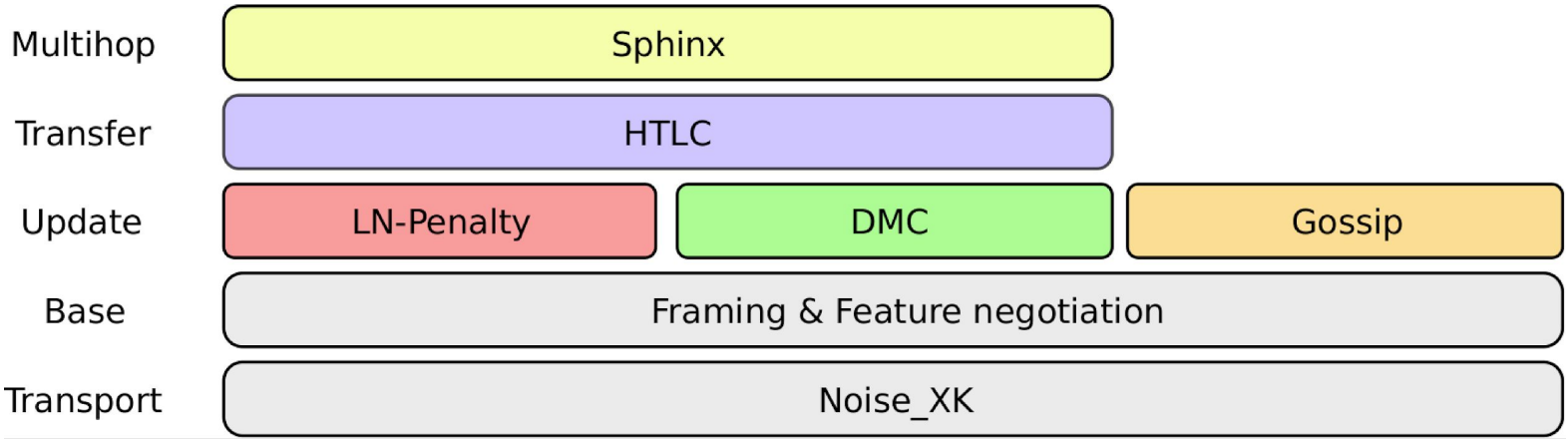
Blockstream

Lightning Network Overview

Dr. Christian Decker

Core Tech Engineer

The Lightning Stack



1 Layers

Transport Layer (BOLT 08)

Goals

- Authenticate Node Identity
  - Fingerprint Resistant
- Setup Transport Encryption
  - Confidentiality
  - Authentication
  - Integrity

Implementation

- Persistent Identities (Node ID)
- Noise Protocol Framework (Noise_XK)
  - SHA256
  - ChaCha20
  - Poly1305

Message Framing (BOLT 08)

Control Messages (BOLT 01)

init

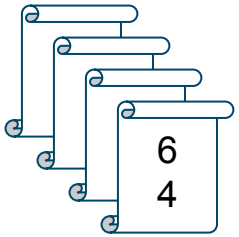
- type: 16 (`init`)
- data:
  - [`2:gflen`]
  - [`gflen:globalfeatures`]
  - [`2:lflen`]
  - [`lflen:localfeatures`]

error

- type: 17 (`error`)
- data:
  - [`32:channel_id`]
  - [`2:len`]
  - [`len:data`]

Update Layer (BOLT 02)

User	Balance
Alice	~~5~~ 6
Bob	~~5~~ 4
Carol	5



Transfer Layer (BOLT 02)

Off-Chain Case:

- **Collaborative success**
  Recipient presents sender with the hash preimage, and both update state to remove the HTLC output.
- **Uncollaborative success**
  Recipient shows sender hash, but sender refuses to remove the HTLC output. Drop to chain to enforce success using the HTLC-success transaction before timeout expires
- **Timeout**
  Drop to chain and eventually use HTLC-Timeout transaction, before upstream timeout expires, to avoid being out of pocket.

On-Chain Case:

- **Collaborative success**
  Too late, we're already on-chain, HTLC output was created.
- **Uncollaborative success**
  Enforce success using the HTLC-success transaction before timeout expires.
- **Timeout**
  Use HTLC-Timeout transaction, before upstream timeout expires, to avoid being out of pocket.

Transfer Layer (BOLT 02)

```
# To remote node with revocation key
OP_DUP OP_HASH160 <RIPEMD160(SHA256(revocationpubkey))> OP_EQUAL
OP_IF
    OP_CHECKSIG
OP_ELSE
    <remote_htlcpubkey> OP_SWAP OP_SIZE 32 OP_EQUAL
    OP_NOTIF
        # To local node via HTLC-timeout transaction (timelocked).
        OP_DROP 2 OP_SWAP <local_htlcpubkey> 2 OP_CHECKMULTISIG
    OP_ELSE
        # To remote node with preimage.
        OP_HASH160 <RIPEMD160(payment_hash)> OP_EQUALVERIFY
        OP_CHECKSIG
    OP_ENDIF
  OP_ENDIF
```

Multihop Layer (BOLT 04)

Gossip Layer (BOLT 07)

2 Bits and Pieces

Bits and Pieces

DNS Bootstrap (BOLT 10)

Invoices (BOLT 11)

Please send 0.0025 BTC for a cup of nonsense (ナンセンス 1杯) to the same peer, within one minute

lnbc2500u1pvjluezpp5qqqsyqcyq5rqwzqfqqqsyqcyq5rqwzqfqqqsyqcyq5rqwzqfqypqdpquwpc4curk03c9wlrswe78q4eyqc7d8d0xqzpuyk0sg5g70me25alkluzd2x62aysf2pyy8edtjeevuv4p2d5p76r4zkmneet7uvyakky2zr4cusd45tftc9c5fh0nnqpnl2jfll544esqchsrny

Thank You

@Snyke

@Blockstream

Blockstream.com