Base & Transport Layer

Chaincode LN residency - NY 2019

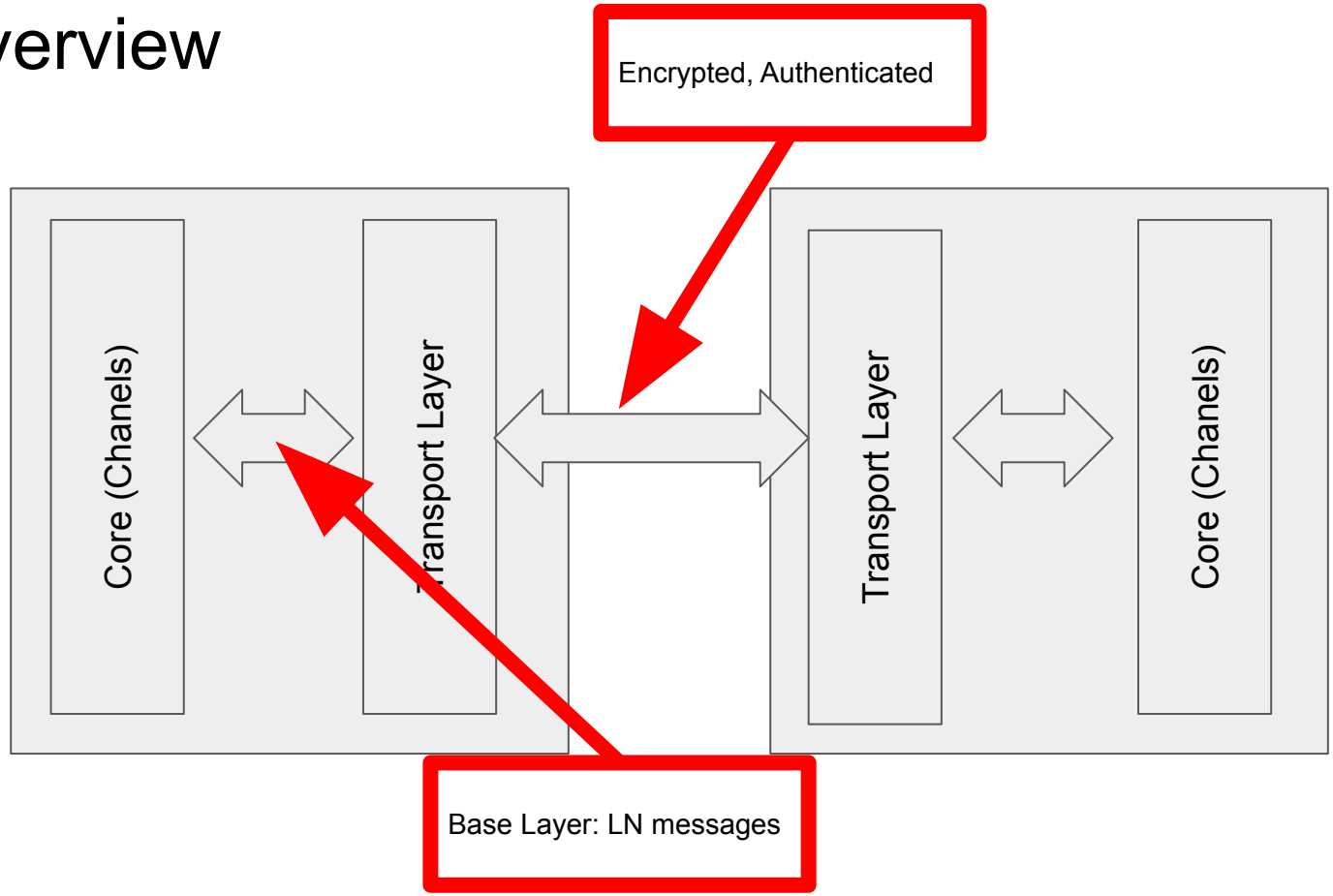
Fabrice Drouin <fabrice.drouin@acinq.fr> - https://acinq.co/

Basis Of Lightning Technology

- **BOLT #1: Base Protocol**
- BOLT #2: Peer Protocol for Channel Management
- BOLT #3: Bitcoin Transaction and Script Formats
- BOLT #4: Onion Routing Protocol
- BOLT #5: Recommendations for On-chain Transaction Handling
- BOLT #7: P2P Node and Channel Discovery
- **BOLT #8: Encrypted and Authenticated Transport**
- BOLT #9: Assigned Feature Flags
- BOLT #10: DNS Bootstrap and Assisted Node Location
- BOLT #11: Invoice Protocol for Lightning Payments

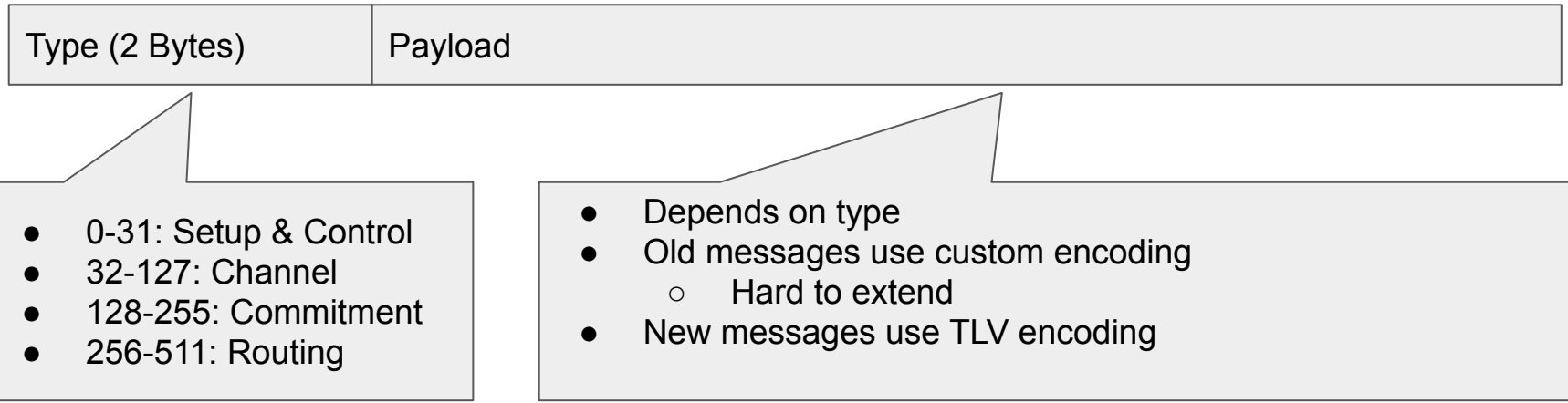
See https://github.com/lightningnetwork/lightning-rfc

Overview


Encrypted, Authenticated
Core (Chanels)
Transport Layer
Transport Layer
Core (Chanels)
Base Layer: LN messages

Base Protocol

- Custom Binary Format
- Max size = 65K



TLV Encoding

- Generic “Type Length Value” binary format
- TLV Record
  - Type: Bitcoin Varint
  - Length : Bitcoin Varint
  - Value: Anything (depends on type)
- TLV Stream
  - Sequence of TLV records
- Additional rules
  - Records sorted by type
  - Type must be unique

=> Nodes can skip records that they don’t understand

Transport Layer

- Based on the Noise Protocol
- Each node has a private/public key pair
  - Node Id = Public Key
- Handshake
  - Nodes exchange and authenticate their public keys
- Encryption
  - Nodes derive 2 encryption keys (inbound and outbound), which are rotated every 500 messages
- Transport Layer passes a binary packet to the application layer

Payment Request

- Basic Payment Information:
  - Payment Hash
  - Amount
  - Expiry
- Metadata
  - Description
- Routing Hints
  - Very useful if last “hop” is private