Prisms in Many Forms

What is the prism's priorities?

- Should the split amount be strictly enforced?
- Should the all the prism's payments fail if a single member is offline? (atomicity)
- Should the prism be trustless?

Priority: Enforced Split Amounts

Features and Requirements

- Needs a prism coordinator
- Prism coordinator enforces the splits
- Prism coordinator can retry payments

Tradeoffs

- Trusted coordinator

Priority: Atomicity and Trustlessness

Features and Requirements

- Coordinator can not take funds
- Probably needs coordination among prism member nodes
- Probably needs a different type of channel construction (e.g. might need PTLCs or signature aggregation)

Tradeoffs

- Complexity
- A single member could make the payment fail (need async payments to fix)

Priority: Trustless

Features and Requirements

- Use BIP-353
  - rockband@twelve.cash
  - bitcoin:?prism=[{lno: "lon123...abc", split: 0.25}, {lno: "lon456...def", split: 0.25}, {lno: "lon789...ghi", split: 0.25}, {lno: "lon012...jkl", split: 0.25}]
- Sender's device uses the prism as a general guideline
- No member can stop the prism by being offline

Priority: Trustless

Tradeoffs

- Might not be a prism in the technical sense, but looks kind of like a prism if you squint at it
- Sender can change the split amounts (might be good)
- Requires wallets to support it