Lightning Network Meeting on Interoperability and Specifications

On October 10th and 11th, following Scaling Bitcoin Milan, participants implementing the Bitcoin Lightning Network produced a general outline for agreement on the Lightning Network protocol scope and specification. Over the past year, the Lightning community has been working on exploring the problem space and writing implementations, creating many Lightning channels and transactions on the Bitcoin Test Network. This meeting is a culmination of these efforts, across many companies within the Bitcoin ecosystem, and finalizing the implementations towards protocol compatibility and releases in the coming weeks and months.

Meeting Participants

Lightning implementers in the meeting include (in alphabetical order):
Alex Ostrovski
Christian Decker
Christopher “JJ” Jeffrey
Corné Plooy
Elizabeth Stark
Fabrice Drouin
Joseph Poon
Mykola Sakhno
Olaoluwa “roasbeef” Osuntokun
Pierre-Marie Padiou
Rusty Russell
Thaddeus Dryja

These participants represent organizations including: ACINQ, Amiko Pay, Bcoin/Purse.io, Bitfury, Blockstream, and Lightning Labs.

While unable to attend, ideas discussed were included from:
Mats Jerratsch
Anthony Towns
Pavel Prikhodko
Slava Zhygulin
and many other contributors who brought great insights.

About the Lightning Network

The Lightning Network enables a high-volume of transactions on the Bitcoin blockchain, and enables entirely new use cases for Bitcoin such as extremely low-value micropayments and near-instant confirmation. Lightning uses a network of bi-directional payment channels, whereby payment across the network is atomically enforced through hash-locked smart

contracts. Individual balance states are enforced using real bitcoin transactions whose broadcast on the blockchain is deferred until a later date, and enforced through time-enforced commitments bonded on-chain. The Lightning Network's simplicity and efficiency is dependent upon a malleability fix to Bitcoin for security (i.e. Segregated Witness).

New use cases range from pay-per-click articles, bandwidth sharing, to near-instant transfers to bitcoin services and marketplaces. Lightning allows for Bitcoin to bring about the opportunities enabled by low-fee, low-friction, high-volume transaction processing.

Meeting Summary

We agreed on a general outline for protocol compatibility, with the draft specification to be finalized and open to review by the community soon:

- ❏ The core commitment protocol: How channel states are updated and the format of the bitcoin transactions. Two-stage HTLCs were selected as per Mats Jerratsch's mailing list suggestion.
- ❏ Initial wire protocol: focus was around creating a system for future upgradability and announcing capabilities.
- ❏ A basic routing protocol on launch
- ❏ General format for encrypted messaging between nodes, as well as format for onion message for multi-hop.
- ❏ Simple payment address/QR-code, with a more detailed protocol to be drafted.
- ❏ Format for outsourcing channel closure detection and penalties
- ❏ Convergence on naming to reduce confusion, e.g. Payment Hash/Preimage, Commitment Hash/Preimage.
- ❏ No agreement could be reached on a theme song.

The Future / Next Steps

We will be finalizing the specification for review in the coming weeks. In particular, we are interested in getting input from all stakeholders within the Bitcoin ecosystem and how Lightning can best serve their needs and bring greater opportunity for Bitcoin.

Subsequently, in the following weeks, many implementations will begin testing compatibility between implementations to prepare for mainnet alpha/beta releases, so that the wider ecosystem can begin using Lightning and build new Bitcoin products and services.