The Bitcoin Lightning Network:
Scalable Off-Chain Instant Payments

Joseph Poon
joseph@lightning.network

Thaddeus Dryja
rx@awsomnet.org

January 14, 2016
DRAFT Version 0.5.9.2

Abstract

The bitcoin protocol can encompass the global financial transaction volume in all electronic payment systems today, without a single custodial third party holding funds or requiring participants to have anything more than a computer using a broadband connection. A decentralized system is proposed whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels) whose transfer of value occurs off-blockchain. If Bitcoin transactions can be signed with a new sighash type that addresses malleability, these transfers may occur between untrusted parties along the transfer route by contracts which, in the event of uncooperative or hostile participants, are enforceable via broadcast over the bitcoin blockchain in the event of uncooperative or hostile participants, through a series of decrementing timelocks.

1 The Bitcoin Blockchain Scalability Problem

The Bitcoin[1] blockchain holds great promise for distributed ledgers, but the blockchain as a payment platform, by itself, cannot cover the world's commerce anytime in the near future. The blockchain is a gossip protocol whereby all state modifications to the ledger are broadcast to all participants. It is through this "gossip protocol" that consensus of the state, everyone's balances, is agreed upon. If each node in the bitcoin network must know about every single transaction that occurs globally, that may