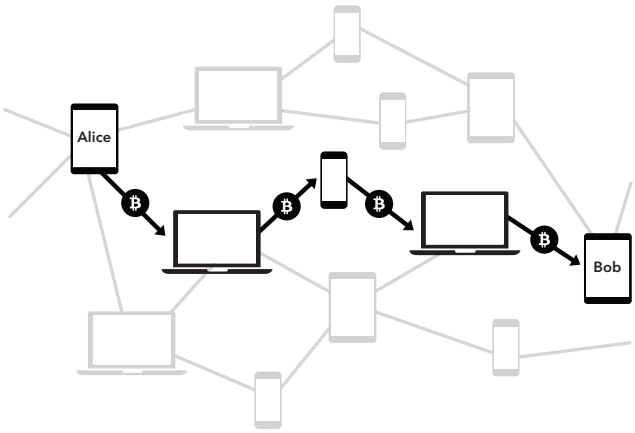
The Bitcoin Lightning Network

http://lightning.network

The Lightning Network is a decentralized system for instant, high-volume micropayments that removes the risk of delegating custody of funds to trusted third parties.



Bitcoin, the world's most widely used and valuable digital currency, allows anyone to send value without a trusted intermediary or depository. Bitcoin contains an advanced scripting system allowing users to program instructions for funds. There are, however, some drawbacks to bitcoin's decentralized design. Transactions confirmed on the bitcoin blockchain take up to one hour before they are irrevesible. Micropayments, or payments less than a few cents, are inconsistently confirmed, and fees render such transactions unviable on the network today.

The Lightning Network solves these problems. It is one of the first implementations of a multi-party Smart Contract (programmable money) using bitcoin's built-in scripting. The Lightning Network is leading technological development in multiparty financial computations with bitcoin.

Instant Payments. Bitcoin aggregates transactions into blocks spaced ten minutes apart. Payments are widely regarded as secure on bitcoin after confirmation of six blocks, or about one hour. On the Lightning Network, payments don't need block confirmations, and are instant and atomic. Lightning can be used at retail point-of-sale terminals, with user device-to-device transactions, or anywhere instant payments are needed.

Micropayments. New markets can be opened with the possibility of micropayments. Lightning enables one to send funds down to 0.00000001 bitcoin without custodial risk. The bitcoin blockchain currently enforces a minimum output size many hundreds of times higher, and a fixed per-transaction fee which makes micropayments impractical. Lightning allows minimal payments denominated in bitcoin, using actual bitcoin transactions.

Scalability. The bitcoin network will need to support orders of magnitude higher transaction volume to meet demand from automated payments. The coming increase in internet-connected devices needs a platform for machine-to-machine payments and automated micropayment services. Lightning Network transactions are conducted off the blockchain without delegation of trust and ownership, allowing users to conduct nearly unlimited transactions between other devices.

How it Works. Funds are placed into a two-party, multisignature "channel" bitcoin address. This channel is represented as an entry on the bitcoin public ledger. In order to spend funds from the channel, both parties must agree on the new balance. The current balance is stored as the most recent transaction signed by both parties, spending from the channel address. To make a payment, both parties sign a new exit transaction spending from the channel address. All old exit transactions are invalidated by doing so.

The Lightning Network does not require cooperation from the counterparty to exit the channel. Both parties have the option to unilaterally close the channel, ending their relationship. Since all parties have multiple multisignature channels with many different users on this network, one can send a payment to any other party across this network.

By embedding the payment conditional upon knowledge of a secure cryptographic hash, payments can be made across a network of channels without the need for any party to have unilateral custodial ownership of funds. The Lightning Network enables what was previously not possible with trusted financial systems vulnerable to monopolies—without the need for custodial trust and ownership, participation on the network can be dynamic and open for all.