The Lightning Network is a protocol that enables high-volume, low-latency digital micropayments without the need for trusted intermediaries. Using novel Bitcoin multisignature transactions and scripts, Lightning participants do not give unilateral custody of funds to a third party, greatly reducing transaction costs and counterparty risk. While previous micropayment solutions involve holding funds with trusted custodians, the Lightning Network achieves instant micropayments via smart contracts. Through a network of multisignature transactions, any participant on the Lightning Network is able to pay anyone else within the graph of participants.

Lightning's fundamental technology is a local two-party consensus, known as a payment channel. Two parties send an initial amount of Bitcoin into a multisignature transaction with a local consensus on the current balance allocated between the two participants. Updates to the allocation of the current balance can be made only with the cooperation of both parties, using a new transaction which spends from the funds allocated to the multisignature transaction to each party.

One on-blockchain transaction is made to deposit the funds into a multisignature output. Before this transaction is made, a refund transaction is created, which returns the original deposit to both parties. After the transaction is broadcast on-chain, the payment channel is open and ready for transfers. When one wishes to update the balance with a new balance, both parties must consent to the new balance and generate a new spend from the transaction. In effect, they have created numerous "double spends" from an on-blockchain transaction, but have elected not to broadcast the spend until either party wants to redeem their funds on-chain.

These multisignature transactions are real Bitcoin transactions. Either party may broadcast the most recent transaction, the current local consensus state, to the global blockchain at any time to redeem their current balance of funds. As either party may redeem funds from this channel at any time unilaterally, without requiring any cooperation from anyone else, the most recent transaction is effectively their current balance in the channel. They may continue updating the channel with updated states without interacting with the global blockchain until they wish to close out the channel. In other words, updating the local consensus state is actionable on the global consensus state.

Updating the local transaction state is enforceable via mutual revocation of old states. When balances are updated in a channel, the prior state is invalidated via a penalty system. Only the most recent balance state should be broadcast, which spends from the on-chain multisignature output. If either party incorrectly broadcasts an old transaction state, the counterparty may take all the funds in the channel as a penalty. As a result, both parties have a direct economic incentive to only broadcast the most recent transaction state. This is achieved by having an on-chain dispute mediation window before the funds can be dispersed. The global consensus state, the Bitcoin blockchain, becomes a dispute resolution system for off-chain local consensus states. Similar to how the vast majority of legal contracts are adhered to without going to court, the balances in the channel are agreed upon in the off-chain local consensus state, and have the option of on-chain programmatic enforcement.

The innovation of the Lightning Network is the use of time-locked transactions and cryptographic nonces to allow many two-party payment channels to form a connected network where payments can be sent over many channels without trusting the intermediate nodes. The topology is similar to IP networks like the internet: packets are routed over many physical links, and the communicating end nodes don't worry about the route as long as data gets to the destination. This works via a decrementing time-lock that permits every intermediate node along the routing path to accept funds only if they forward it along to the next participant, using disclosure of preimages of cryptographic hashes. In the Lightning Network, nodes are not able to seize funds traveling through their channels even if they fail to forward payments or refuse to perform any actions. A node operates without custody of third party funds, which is enforced by a time-limited cryptographic script. This is all achieved off-chain assuming cooperative parties, and enforced on-chain when one's counterparty is not cooperative.

Through this network of interconnected payment channels, Lightning provides a scalable, decentralized micropayments solution on top of the Bitcoin blockchain.