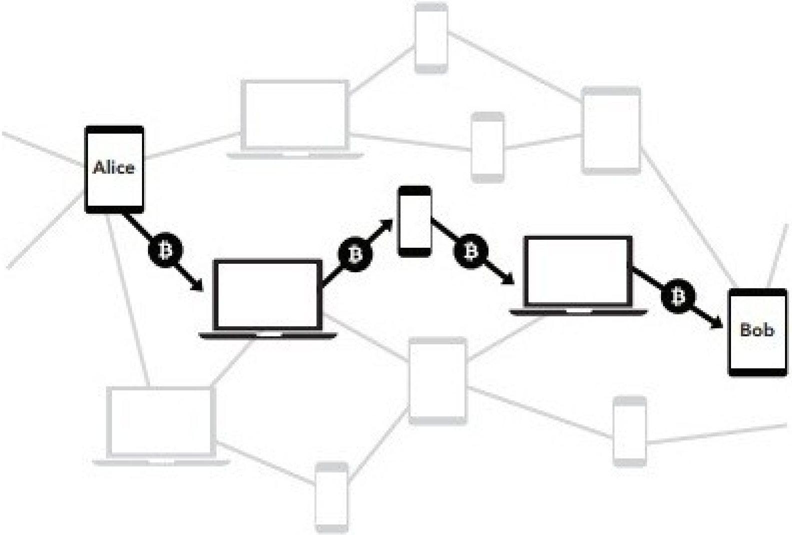
PUZZLE ITC

Lightning Network: A scaling solution for Bitcoin



Bitcoin currently has a problem: It's being chased by it's own success. At the moment the cryptographic network that was designed to be an electronic payment system cannot really be used to buy daily goods. The fees for a transaction are several dollars and a confirmation can take an hour or more. Not really the currency you want to use to buy a coffee...

But there is hope: For the last few years the development of the so called Lightning Network has been in progress and since December of the last year the first alpha versions are available for testing. Puzzle ITC wants to be at the forefront and operate one of the first Lightning Network Hubs.

The problem: Full blocks

The rapid rise in value over the last year has lead to more and more Bitcoin transactions being issued. But the size of a block in Bitcoin is limited to one megabyte, which means about 2000 transactions, depending on their type. So with the 10 minutes on average it takes to mine a new block, that doesn't amount to many transactions per second. Therefore the list of unconfirmed transactions not yet included in a block is long and you have to pay high fees for your transaction to be included in the next block.

The naive solution: Bigger blocks

At first glance, it might appear logical to just increase the size of the blocks. More megabytes means more transactions; problem solved.

But if you compare the 24’000 transactions per second the Visa payment system can handle at it’s peak capacity with what Bitcoin can handle now, you might see the problem with that. It should be apparent that if you want to reach similar transaction throughput in Bitcoin as Visa can handle, the blocks would need to be gigabytes in size. But this contradicts a fundamental principal of Bitcoin: Everybody should be able to run their own node and be able to validate the entire blockchain locally. If you have to download, verify and store gigabytes of data every 10 minutes, you need a very fast internet connection and expensive hardware to handle the load.

As a result, there would be fewer and fewer full Bitcoin nodes which would in turn hurt the decentralization of the network.

The cleverer solution: Scaling off-chain

When the space in the blockchain has become so rare, does it really make sense to store every single small financial interaction in a public ledger for everyone to see? Does my transaction to buy a coffee really need to be stored on thousands of computers for ever? Or wouldn’t it make much more sense to have some sort of smart contract that allocates an initial balance between me and my coffee shop in the blockchain that then can be updated by both parties without publishing every transaction?

That’s exactly what the so called Lightning Network promises: It creates a Payment Channel between two participants with an initially agreed upon balance. Only the creation (and, eventually, the closing) of the channel needs to be published to the blockchain. Everything that happens in-between (in our example: deduction for buying a coffee, customer loyalty payback) is only sent in private between the two participants. The current balance in the channel can be updated within milliseconds and as often as it serves both parties, without the need of settling to the Bitcoin network.

Through a sophisticated cryptographic procedure **[1]** both parties are secured against cheating of the counterpart. Is one of the participants of a payment channel uncooperative, offline for a long time or has malicious intents, the other side can use the blockchain as a decentralized judge and close the channel. No party needs to trust any person or institution to be benevolent, the blockchain always acts as an arbiter in case of a dispute.

The Lightning Network: A layer 2 solution – or TCP/IP for bitcoin

The whole idea of payment channels gets really interesting when you link them together and issue payments through multiple nodes/hubs. Because the cryptographic algorithms that are used to secure a single channel can also be used to pull funds along multiple channels without any node in between being able to divert, block or meaningfully identify them.

You can think of the Lightning Network as a network of channels between nodes, similar to the network of routers that form the internet. Many nodes are connected directly or indirectly with every other node in the network. Payments can be routed between any of these nodes in milliseconds, using minimal fees (as little as a few Satoshi **[2]** or even no fees at all).

This demo video shows **[3]**, how easy it is to send a few dollars or even cents to a website using the Lightning Network.

If you want to know how the technology works in detail, this three part video series **[4]** is an excellent place to start.

Puzzle ITC as a Lightning Network Hub

We at Puzzle ITC are convinced that this technology will help Bitcoin achieve a break-through in user adoption and help the currency to become what it had been designed as: a payment system for everyday transactions.

That's the reason why we want to operate one of the first Lightning Network Hubs in Switzerland and help push the technology. We ran successful tests on the Bitcoin test network in December and are now setting up our productive node on the Bitcoin "mainnet".

Try for yourself

If you want to try out the technology and play around with it, you can start by downloading any of the available client applications **[5]** or the "Eclair Wallet Testnet" mobile app for Android **[6]**and connect to our test node **[7]**. We will publish tutorials and more information on https://lightning-test.puzzle.ch

Also follow us on Twitter (@puzzleitc) to keep up-to-date about the progress of the Lightning Network.

Links:

[1] https://lightning.network/lightning-network-paper.pdf

[2] https://en.bitcoin.it/wiki/Satoshi_(unit)

[3] https://www.youtube.com/watch?v=o_pTB8gCuvQ

[4] https://www.youtube.com/watch?v=XFUYvLW-0oE

[5] http://dev.lightning.community/lapps/

[6] https://play.google.com/store/apps/details?id=fr.acinq.eclair.wallet&hl=en

[7] https://lightning-test.puzzle.ch/