

BITCOIN PRICE

\$606.83



SUBSCRIBE

MEMPOOL: #core-dev #blockchain #technical #wall-street #regulation #government



DISTRIBUTED : HEALTH

October 3, 2016

Nashville, TN

How Falcon, FIBRE and the Fast Relay Network Speed Up Bitcoin Block Propagation (Part 2)

Jul 29, 2016 04:13 PM by Aaron van Wirdum



Bitcoin is designed as a peer-to-peer network, where nodes randomly connect to other nodes. Transactions and blocks are transmitted over this network by these nodes, until each has received all. This works quite well, as the distributed model makes Bitcoin relatively censorship-resistant; there is no central point of control to shut down or pressure into compliance.

But it also has a significant downside: The peer-to-peer network is relatively slow. As such, miners (and pools) sometimes waste hash power mining on top of an old block while a newer block is finding its way through the network. Transmission delay, therefore, benefits pooled mining as well as geographic clustering of miners, incentivizing a more centralized mining topology. This is generally considered one of the bottlenecks for scalability, as larger blocks (which can include more transactions) propagate even more slowly.

Over the past years, therefore, several projects have been in development to increase the speed of block propagation. These projects focus on roughly two main issues: block compression to limit the amount of data that needs to be propagated over the network, and relay speed to cut the time it takes for blocks to propagate.

This two-part series provides an overview of these projects. Part 1 covered block compression. Part 2 will examine ways of speeding up the network.

Fast Relay Network (AKA Matt Corallo's Relay Network)

The Fast Relay Network, also known as Matt Corallo's Relay Network, is a relatively straightforward relay network setup by Corallo, and has existed for some years. The Fast Relay Network consists of nine nodes, distributed strategically around the globe. Designed as a hub-and-spoke model, miners can connect to the relay node closest to them to send and receive blocks over this network. This is significantly faster than Bitcoin's peer-to-peer network.

The main downside of the Fast Relay Network is that it's relatively centralized: Corallo controls it. And while the software is open source, no one else has set up a similar open relay network so far. (Though mining pools do have similar — but closed — setups among themselves, and typically for “internal” use among their own nodes.)

For more details, see [Bitcoin Magazine's earlier article on the Fast Relay Network](#).

Falcon

As blocks are transferred over Bitcoin's peer-to-peer network, they are really transmitted in several IP-packets. Each node on the network receives each packet, and reconstructs blocks from the data in these different packets. Once the block is reconstructed and considered valid, nodes forward the block to other nodes. Again, of course, in different packets.

To speed this process up, Cornell University researchers Soumya Basu, Ittay Eyal and Emin Gün Sirer are developing the [Falcon](#) relay network. Falcon uses a technique called “cut-through routing,” where nodes don't wait to receive all packages to forward them. Instead, they forward each package as soon as they receive it, while initially checking only the block header. They reconstruct the block in the meantime, as the rest of the packages arrive.

This solution does have one disadvantage: Nodes can validate a full block only after they have received all required packages. As such, there's a small risk of a dishonest miner transmitting invalid packages all across the network, wasting competitor resources.

To solve this, the Falcon network operates with gatekeepers: the Cornell University team. As such, the Falcon network itself isn't entirely decentralized; the idea is that it decentralizes Bitcoin's overall network topology through diversity.

FIBRE

As noted, blocks on the Bitcoin network are really transmitted in several IP-packets. Unfortunately, package-loss is a significant bottleneck for propagation

speed; even on relay networks. While it doesn't necessarily happen very often, packet-loss can cause spikes in transmission-time, as nodes need to re-communicate data.

FIBRE (Fast Internet Bitcoin Relay Engine), also developed by Corallo, is a re-designed relay-protocol. As perhaps its most interesting solution, it is built on the User Datagram Protocol (UDP). This is an alternative to the far more common TCP internet protocol, and currently mostly used for Voice over IP (Skype) and gaming. As an important differentiator from all the above protocols, UDP allows FIBRE to use a nifty trick known as Forward Error Correction (FEC). This lets nodes reconstruct all of the transmitted data even if some of it got lost on the way.

And: FIBRE is specifically designed for Compact Blocks; the innovation discussed in Part 1 of this series. The combination of FIBRE with Compact Blocks, as statistics collected by Corallo show, make FIBRE nearly as fast as the speed of light.

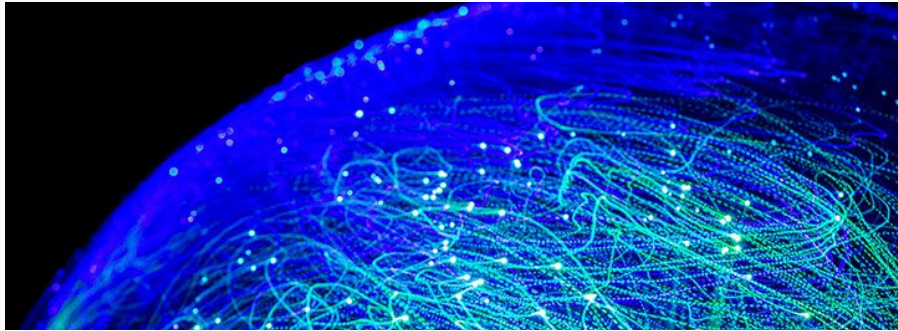
Lastly, FIBRE is designed to be a more decentralized alternative to other relay networks. Specifically, as a key feature of FIBRE, it's designed as a sort of “add on” for Bitcoin Core, so anyone who runs a node should be able set up his or her own network.



by Aaron van Wirdum

Aaron van Wirdum ([Twitter](#) / [email](#) / [pgp](#) / [bitcoin](#)) has a background in political history, with a specialization in the effects of new technology on societies. He discovered Bitcoin in early 2013, and has been writing his way through the rabbit hole since. Interested in decentralized consensus, FOSS, privacy in the digital age, censorship resistant payments, and more of that stereotypical Bitcoin stuff.

Related Articles:



APR 07, 2016

Replacing Bitcoin Transactions: Community Responses to Opt-In Replace-By-Fee

#TECHNICAL



APR 13, 2016

Bitcoins Are Not Tied Up on the Lightning Network, Say Creators Poon and Dryja

#TECHNICAL



APR 15, 2016

Bitcoin Core 0.12.1 Released, Major Step Forward for Scalability

#TECHNICAL



APR 19, 2016

Greg Maxwell: Lightning Network Better Than Sidechains for Scaling Bitcoin

#TECHNICAL

