How a Bitcoin Backbone Gives Small Miners a Leg Up: Matt Corrallo's Relay Network

Nov 19, 2015 7:26 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 node receives all the latest transactions and blocks. 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 there are other, more centralized alternatives for transmitting transaction data, too. The best known of these is “the” relay network, introduced in 2014 and maintained by Bitcoin Core developer Matt Corallo: “It's centralizing, but, hopefully, democratizing.”

On propagation

Corallo's relay network serves two distinct purposes. First, it adds diversity to Bitcoin. Rather than just needing to rely on the peer-to-peer network, Bitcoin users can opt to receive transaction data and blocks through an alternative channel. This makes it harder to successfully attack the Bitcoin network; the relay network functions as a fallback. But the second, and more important reason, is a potential decrease of network latency.

Speaking to *Bitcoin Magazine*, Corallo explained:

> ” The peer-to-peer code in Bitcoin Core is pretty gnarly. It's stable and it works, but it's not very efficient, and it's not very fast. The resulting network latency is a problem, especially for miners. It can sometimes take 10, 15 seconds before they receive newly mined blocks. If you're a miner, 10 seconds is like 1.5 percent loss in revenue. That is potentially a big deal. You don't want that.”

Some of the bigger miners (typically mining pools) have therefore come up with an alternative solution. Rather than using the peer-to-peer network to transmit new blocks, they have created an alternative – private – network. If one of these miners finds a new block, that miner immediately sends it over to the other miners on their private network, meaning all these miners can start mining on the new block immediately.

The problem, of course, is that this disadvantages all miners not using this

The problem, of course, is that this disadvantages all miners *not* using this private network. When a select group of miners starts mining on a new block faster than other miners this select group gets a head start every time one of them finds a block. This is especially worrisome because it is typically the bigger miners who have the time and resources to set up private networks. Smaller miners might, therefore, become less profitable and eventually drop off the network entirely, which centralizes mining even further.

A Leg Up

Corallo's relay network is essentially a hub-and-spoke network, which consists of servers set up in eight well-connected Internet traffic hubs: New York, Seattle, Amsterdam, Beijing, Tokyo, Singapore, Hong Kong and Novosibirsk (located in central Russia). Additionally, the relay network uses a fairly basic compression algorithm. Any Bitcoin node can connect to the nearest hub on Corallo's relay network, and send and receive transactions and blocks to and from other connected nodes.

But unlike Bitcoin's original peer-to-peer network, Corallo's relay network is centrally controlled: by Corallo. This means that users of the network need to rely on Corallo, most importantly for maintenance. (Though this doesn't stop the peer-to-peer network from propagating transactions and blocks in the mean time, of course.)

> The relay network is not the most reliable thing," Corallo acknowledged. "There is no service-level agreement ... once in a while servers go down and I don't fix it right away... sometimes I'm sleeping, or drunk."

But absent better alternatives, the relay network can still save small miners on cost, meaning they can increase their profit, and remain competitive, Corallo hopes.

> It's democratizing in the sense that larger miners do something like this already," he said. "The relay network gives smaller miners a leg up, since they don't need to spend a proportionally large portion of their resources to establish these types of relay networks themselves. So it's centralizing in some ways, but, hopefully decentralizing, in others."

by Aaron van Wirdum

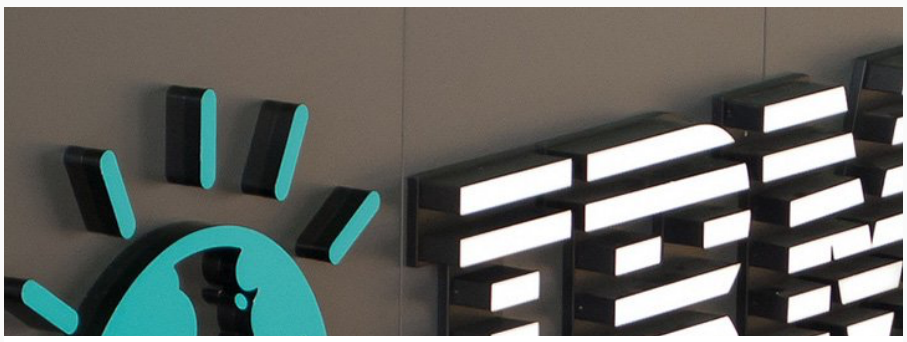
Aaron van Wirdum (twitter - email - pgp) studied Politics and Society in Historical Perspective at Utrecht University, and specialized himself in the influence of freedom of speech and communication technologies on social structures. He published Bitcoin-related articles on several Dutch blogs and co-founded the (now defunct) Dutch Bitcoin news site Coincourant, before he started writing for Bitcoin Magazine and other English Bitcoin media from 2014 on out.

KEYWORDS: #miners #bitcoin #blocks #transactions #nodes

Related Articles:

FEB 04, 2016

Deutsche Bank: Banks Must Partner with Fintech and Digital Currency Businesses or Risk Disappearing Altogether



FEB 04, 2016

IBM Supports Linux Foundation's Hyperledger Blockchain as Industry Standard, Plans Deployment

#NONE

#NONE

NOV 30, 2015

Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents

#NONE

DEC 28, 2015

Segregated Witness: The Right Answer to the Wrong Question

#NONE