Karlsruhe Reports in Informatics 2018,4
Edited by Karlsruhe Institute of Technology,
Faculty of Informatics
ISSN 2190-4782

Bitcoin Cash (BCH) Sybil Nodes on the Bitcoin Peer-to-Peer Network

Till Neudecker

2018

KIT – University of the State of Baden-Wuerttemberg and National Research Center of the Helmholtz Association

Bitcoin Cash (BCH) Sybil Nodes on the Bitcoin Peer-to-Peer Network

Till Neudecker
till.neudecker@kit.edu
Institute of Telematics, Karlsruhe Institute of Technology, Germany

August 4, 2017

Abstract

On August 1st, 2017, the day Bitcoin Cash (BCH) forked, the number of reachable nodes on the bitcoin Peer-to-Peer network increased from 11,0000 to over 16,000. 12 hours later, the number of reachable nodes returned to 11,500. The 5,000 additional connections were caused by sybil peers running on Amazon's cloud services. The peers announced version strings `Bitcoin ABC:0.14.x` and `BUCash:1.1.0` and advertised new BCH blocks.

1 Analysis

We run two monitor nodes that connect to all reachable peers on the bitcoin Peer-to-Peer network[1]. The nodes remain passive and only log the timestamp they received INV messages advertising blocks or transactions from other peers.

Figure 1 shows the number of connections from our monitor nodes. The number of sybil connections is simply the difference between the total number of connections and the number of unique IP addresses we are connected to. On August 1st, 2017, the number of sybil peers increased to up to 5,000 for a period of about 12 hours.

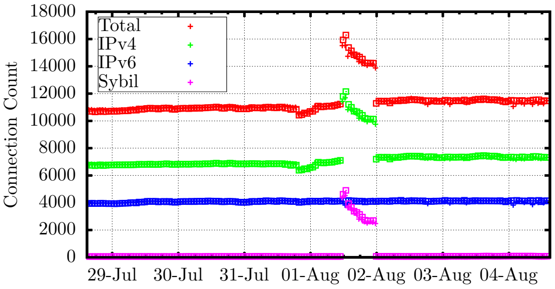

Figure 1: Number of connections.

Figure 2 shows the change in the number of peers announcing a certain version string during the considered period. Most sybil peers announced the version string `Bitcoin ABC:0.14.6(EB8.0)`, however, some peers also announced `BUCash:1.1.0(EB12; AD12)` and `Bitcoin ABC:0.14.5(EB8.0)`. The number of peers announcing `Bitcoin ABC:0.14.6(EB8.0)` was below 100 before, and at around 400 after the sybil period.

Figure 3 shows the change in the number of peers with IP addresses from certain Au-

[1] `https://dsn.tm.kit.edu/bitcoin`

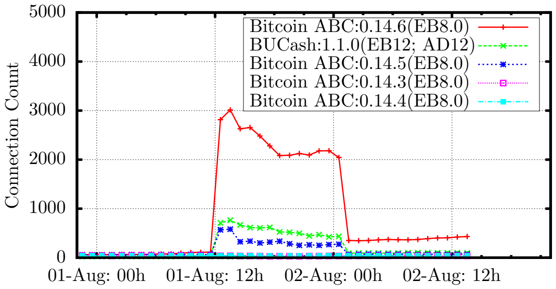

Figure 2: Announced Version Strings, only BCH clients shown.

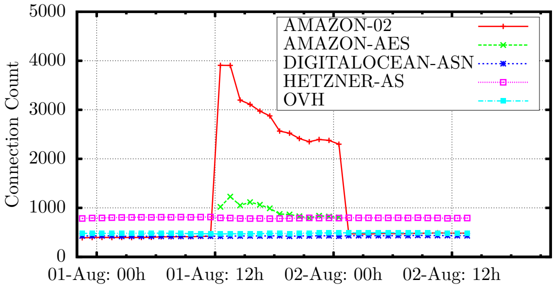

Figure 3: Connections per AS, only AS with most connections shown.

tonomous Systems (AS). We see a steep incline in the number of peers from the AS from Amazon (`AMAZON-02` and `AMAZON-AES`) during the considered period.

Figure 4 shows how many INV messages announcing each BCH block our monitor node received. The blocks on August 1st were announced by roughly 3,500 peers, the blocks on August 2nd were announced by roughly 800 peers. No BCH block was mined during a 13 hour period on August 2nd.

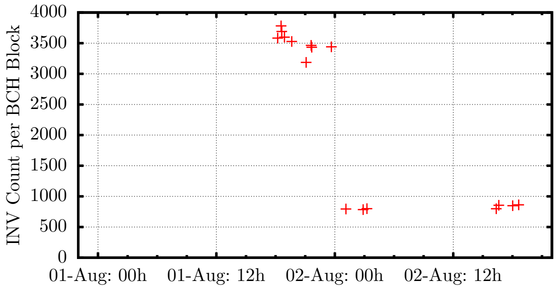

Figure 4: Number of INV messages received for BCH blocks.

2 Discussion

We can only speculate about the motivation for spending the money to run several thousand client instances on cloud services. Possibilities are:

- The newly forked Bitcoin Cash system should be supported by providing more peers that relay blocks and transactions that other peers can connect to.
- The sybil peers could be part of an eclipse attack in which honest peers connect solely to the sybil peers and get cut off from the rest of the network. A possible attacker might be able to exploit the faster difficulty adaption in BCH. Although there were claims that the sybil peers were misbehaving[2] , the sybil peers announced BCH blocks to our monitor node. We could not see any misbehavior, however, we do not receive and analyze blocks and transactions.
- Someone misconfigured his Amazon instances.

[2] `https://www.reddit.com/r/btc/comments/6qvofq/someone_just_launched_over_500_bucash_nodes_on_aws/`