Our goal is to derive a upper bound on the average network latency for Bitcoin. The figure 15.7 seconds has been used, but this is exceeding unlikely, as we will see.

Temporary chain splits happen naturally for network latency reasons. Blocks are created roughly every 600 seconds, so a few seconds latency would suggest that occasionally one miner would produce a block before learning of a block that may have been broadcast a few seconds earlier. But we can be very precise.

We model this by letting $\Delta_{i,j}$ be the delay between miners i and j. Let p_i be the hashrate of miner $i, i \in \{1, ..., N\}$. Notice that

$$\sum_{i=1}^{N} p_i = 1$$

where N is a possibly large but finite number. Assuming an omniscient universal timeclock which can determine absolutely which miner finds the next block; miner i finds it first with probability p_i. The probability that miner j does not find a block before learning of the block broadcast by miner i is given by

$$e^{-p_j \Delta_{i,j}}$$

where $\Delta_{i,j}$ is given in units of 10 minutes. This is the probability of a Poisson distribution produces 0 success in the time $\Delta_{i,j}$, which models block discovery. Thus the probability that the block reaches all miners with none of them having found a competing block is

$$\prod_j e^{-p_j \Delta_{i,j}} = \exp\left(-\sum_j p_j \Delta_{i,j}\right).$$

Summing over all first finders i, the probability that the next block reaches all miners without any conflicts is

$$\sum_i p_i \exp\left(-\sum_j p_j \Delta_{i,j}\right).$$

To get an upper bound on this probability, we use Jensen's inequality; let

$$g_i = \sum_j p_j \Delta_{i,j}$$

then

$$\sum_i p_i \exp\left(-\sum_j p_j \Delta_{i,j}\right) = \sum_i p_i e^{-g_i} \leq \exp\left(-\sum_i p_i g_i\right) = \exp\left(-\sum_{i,j} p_i p_j \Delta_{i,j}\right).$$

So the probability of a broadcast block saturating the network without a fork is bounded above by the negative exponential of the average propagation time.

Because this occurence is usually observable, we can compute determine the likelihood of what we are observing given some possible average delay.

Let

$$\lambda \geq 1 - \exp\left(-\sum_{i,j} p_i p_j \Delta_{i,j}\right)$$

be the probability of a fork for each block.

If we measure a year as 52 560 blocks, the expected number of forks found in a year will be

$$\mu = 52\,560\lambda.$$

For the full distribution we use the Poisson distribution, the expected number of forks found in a year is

$$\Pr\left(\text{fork in a year} = k\right) = e^{-\mu}\frac{\mu^k}{k!}.$$

For example, suppose that the average delay is 1 second. Then we have

$$\lambda \geq 1 - \exp\left(-\frac{1}{600}\right) = 1.665\,3 \times 10^{-3}$$

$$\mu = 52\,560\lambda \approx 87.527.$$

So if the delay is one second, we would expect at least 87 forks per year.

Now if the average delay were to be 15 seconds, we would compute

$$\lambda \geq 1 - \exp\left(-\frac{15}{600}\right) \approx 0.024\,69.$$

Over a year, the expected number of observed forks would be (at least)

$$52\,560 * \left(1 - \exp\left(-\frac{15}{600}\right)\right) \approx 1297.7$$

Of course, there is randomness involved, so we can compute likelihood. The likelihood of observing k forks, if the block delay is 15 seconds, is given by

$$L(k, 15) = e^{-1297.7}\frac{1297.7^k}{k!}.$$

So the likelihood of witnessing less than 200 forks is

$$\sum_{k=0}^{200} e^{-1297.7}\frac{1297.7^k}{k!} \approx 1.685\,2 \times 10^{-316}.$$

This is approximately the likelihood of correctly choosing 3 atoms out of all of the atoms of the observable universe, in order.

Given a number of observed forks k we can use the maximumim likelihood parameter $\mu = k$. So for example, if we observe 30 forks in a year, a reasonable estimate of the chance of a fork is

$$\lambda = \frac{30}{52\,560}.$$

Solving

$$\frac{30}{52\,560} = 1 - e^{-\Delta}$$

we get

$$e^{-\Delta} = 1 - \frac{30}{52\,560} = \frac{1751}{1752}$$

$$\begin{aligned} \Delta &= 5.709\,4 \times 10^{-4} \text{ (units of ten minutes)} \\ &= 600 * \ln(1752/1751) \approx 0.34 \end{aligned}$$

(To be fair, we aren't accounting for the probability that the fork happens but is unobserved)