Rhys Bowden, University of Melbourne

The Bitcoin block arrival process

Abstract

Bitcoin is the new "cash of the Internet". A system based on a peer-to-peer network with no central control, Bitcoin nevertheless maintains a single distributed global ledger called the blockchain. As part of this process, miners and their computers run independent Bernoulli tests at a huge rate (around 3×10^{16} per second), each with the same very low probability of success. Each time a test succeeds a new block is added to the end of the blockchain. This means block arrivals should be very well approximated by a Poisson process. The total computer power dedicated to mining is constantly changing leading to a inhomogeneous Poisson process where the underlying rate is known only through the number of arriving blocks. Further, the probability of success is changed every 2016 blocks in an attempt to keep the block arrival rate constant. This, coupled with other features like propagation delay of blocks and only having one realisation makes modelling and fitting the block arrival process a challenge. We show that simple models of the system are insufficient to reproduce important phenomena, but we can form a sequence of increasingly accurate approximations.