Variable Blockrate Cryptocurrencies

As of time of writing, all popular (including experimental) cryptocurrencies have an established block rate. Bitcoin is at 10 minutes, litecoin is at 2.5 minutes, and some coins go as low as 30 seconds. These numbers all seem arbitrary, and so far even the very fast coins seem to be able to handle the workload.

Realistically, a blockchain can be as fast as the network can propagate information to the rest of the network. A node merely has to receive the previous block by the time that it has mined the next block with high enough probability to prevent most of the work from being wasted.

This requires that the network have some sense of how fast is “sufficiently slow.” A stochastic method can be used to determine if a blockrate is too high. Each time a POW block is produced, the party responsible for producing the block announces the block to the whole network. If the entire network receives the block before another block is produced, the blockrate can be increased. However, if multiple blocks are produced from the same parent block (IE the network does not propagate the first block fast enough to prevent work from being wasted) then the block speed of the network is reduced.

Over time, the speed of the network should converge to something that is roughly as fast as the network can tolerate. The amount that the blockrate adjusts for each event will be according to an error function. Error functions can be simple (blockrate increases by .1% per success, decreases by .1% per failure), error functions can favor little block failure (blockrate increases by .1% per success and decreases by 2% per failure), or an error function could potentially be as complex as using a deterministic machine learning algorithm to determine the best blockrate given the current string of failures and successes. (realistically the most suitable error function will fall somewhere between these two extremes).

The benefit to having a variable blockrate is that the network will automatically adjust in speed as the currency grows and network technology changes. As the network grows larger and spans a greater geography or more complex set of nodes, the blockchain can slow down to minimize the volume of failed blocks. As technology expands and latencies reduce and bandwidths increase, the blockspeed can increase.

Right now it seems as though most blockrates are arbitrarily picked. Because most mining is done through pools, blockspeeds can be very quick if the pools are highly connected. If the volume of pools grow or popular pools do not have great connections to eachother, the currency can be threatened by a blockrate that is too fast for the network to keep up. Most mining will be lost to failed forks. It seems as though cryptocurrencies as a whole are capable of handling blockrates much faster than the popular 10 minutes and 2.5 minutes, but speeding a currency up too much might put it at risk for future changes to the network.

With variable speed blockrates, an error function can be chosen that causes the currency to always hover around an optimal blockrate, and gives the currency a better ability to adapt to changing network environments.