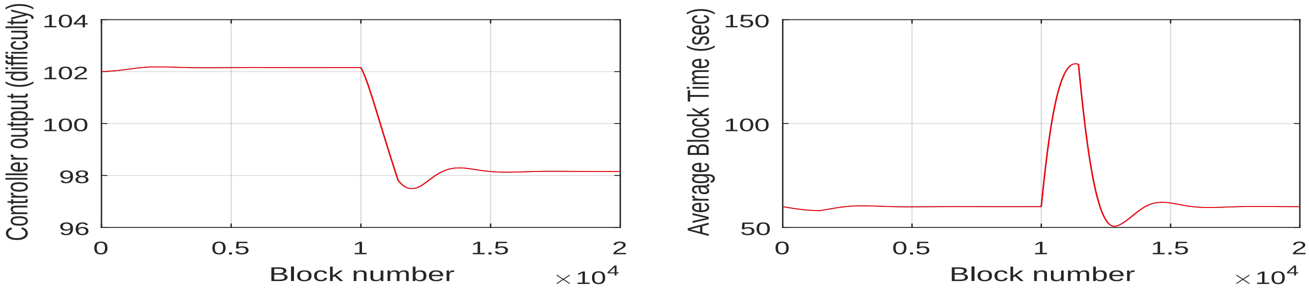
Security of the Bismuth Blockchain

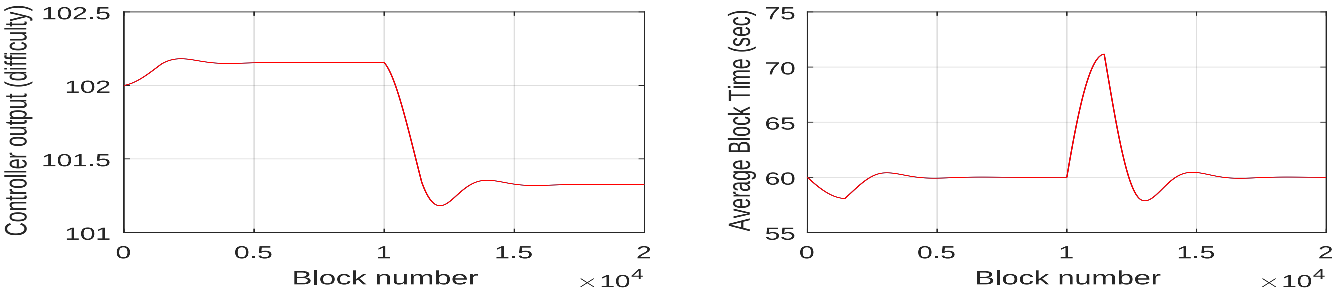
Analysis and Simulation by gh2

May 5, 2018

The Bismuth blockchain uses a feedback control strategy to calculate the difficulty adjustment in the mining process, see this paper in the MIC journal for more details. In combination with this feedback controller Bismuth uses the longest chain rule to determine consensus. How does such an approach compare with the alternative approach of deciding consensus based on total hashwork (ie. selecting the chain which has the most hashwork in it)? To answer this question, the Simulink model shown in Figure 7 in the MIC paper is used. Consider the following scenario: 1) The difficulty level is stable at diff=102 and the 24 hour average blocktime is stable at 60 seconds. 2) At block number 10,000 a large pool with 25% of the total hashpower decides to break off on it's own chain to try to mine a longer chain than the rest of the network. There will now be two competing chains: 1) The chain breaking off with 25% of the original hashpower and 2) The main network which will in this case get reduced to 75% of the original hashpower at block number 10,000.



The figure above shows how the feedback controller and the difficulty adjustment react for the 25% hashpower chain. The difficulty drops from 102 down to 98, while the average blocktime increases to almost 130 seconds, before it comes back down again and settles at 60 seconds. The total accumulated time to generate 20,000 blocks in this example is 14.87 days.



The figure above shows how the feedback controller and the difficulty adjustment react for the other chain with 75% of the hashpower. The difficulty drops from 102 down to 101, while the average blocktime increases to about 71 seconds, before it comes back down again and settles at 60 seconds. The total accumulated time to generate 20,000 blocks in this example is 14.02 days. The reason why the 75% chain generates blocks faster than the 25% chain, is because the overshoot in blocktime (71 seconds vs 130 seconds) is smaller for the chain with the largest hashpower behind it. Since the 75% hashpower chain produces 20,000 blocks in this example faster than the chain with 25% of the hashpower, the 75% chain will also be the longest and the consensus rule currently implemented in Bismuth will select the chain with the most hashwork in it as the winner. As can be seen from this simulation, the chain with the largest amount of remaining hashpower will produce the longest chain in case of a network fork. In other words, Bismuth's implementation of a feedback control algorithm for the difficulty adjustment combined with the longest chain rule achieves the same result as selecting consensus based on the largest total amount of hashwork, a method which is used in other blockchain implementations. Bismuth's unique implementation of difficulty adjustment and longest chain rule can therefore be considered as secure as other consensus implementations based on total hashwork.