Bitcoin, Blockchain and Cryptoassets
Exercise Set 2

In this second exercise set, we will mainly cover the content of the lectures on transaction consensus.

Keep in mind that solving this exercise set is voluntary and UNGRADED. The solutions are either shared already or will be in due time.

Exercise 1

In this exercise you have to analyze several made up ideas for changes to the consensus protocol of the Bitcoin Blockchain. We ask you to determine the (protocol-based) fork type which this change implies and what happens when more miners apply the old or the new rule set.

Exercise 1.1

The current maximal block size on the Bitcoin Blockchain is 1 MB (ignoring the segwit extension). Assume, that some miners want to increase the block size to 2 MB in order to double the number of transactions that can be processed per block. What kind of fork type would this change result in (ceteris paribus)? Will there likely occur a chain split if more computational resources are allocated to the new (a) or the old (b) consensus protocol? Why?

Exercise 1.2

So far there is no minimal transaction fee in the Bitcoin Blockchain. Assume that, to ensure the remuneration of the miners, a Bitcoin Improvement Proposal (BIP) is released which implements a minimal transaction fee of 0.0015 BTC (≈ CHF 75 at the time of writing this tutorial). What kind of fork type would this change result in (ceteris paribus)? Will there likely occur a chain split if more computational resources are allocated to the new (a) or the old (b) consensus protocol? Why?

Exercise 1.3

Assume the next BIP plans to implement a new minimal block size of 0.5 MB[1] and at the same time, a maximal block size of 2 MB. What kind of fork type would this change result in (ceteris paribus)? Will there likely occur a chain split if more computational resources are allocated to the new (a) or the old (b) consensus protocol? Why?

[1] There can be incentives for miners not to include transactions in a block. One reason can be that smaller sized blocks are distributed faster in the network compared to a ”normal” block of size 1 MB. Thus, a miner could try to outrun competing blocks at the cost of loosing the transaction fees.

Exercises 1.4

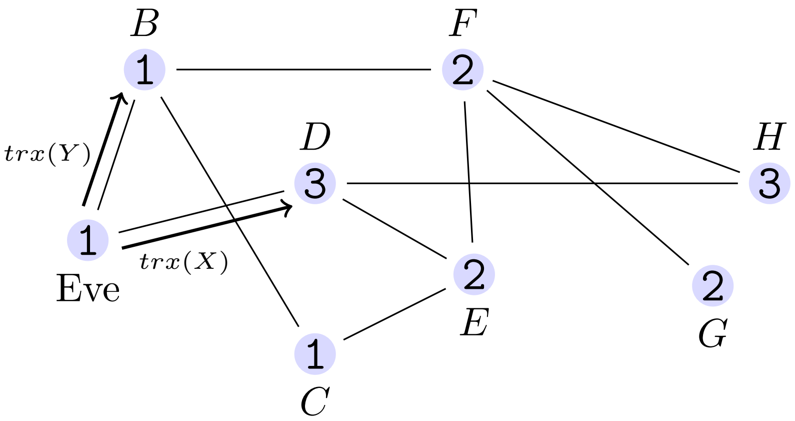
Categorize the following examples into their fork types to further deepen your understanding:

(a) A change in the threshold value so that there are, on average, two blocks found per ten minutes.

(b) A reduction of the remuneration of the miners via the coinbase transaction to maximal 5 BTC[2]

Exercise 2

Consider the network topology below. Eve initiates a transaction X to node D to pay for a coffee. At the same time, she initiates a second transaction Y to node B which references the same UTXO as transaction X but is in favor of another of her own addresses. Her plan is, that transaction Y will be included in the Blockchain, and that she will be long gone when the coffee place realizes, that her coffee-transaction was confirmed. This is one form of a double spend attack. The numbers in the nodes correspond to the respective computational resources used for mining. Assume, that the connections between the nodes are homogeneous[3]. Furthermore nodes will only consider the transaction that reaches them first in their block candidate and will forward only this transaction to connected nodes. Determine the probability that transaction Y will be included in the next block and therefore the success of the double spend attack. Hint: Eve will use her mining power for transaction Y.

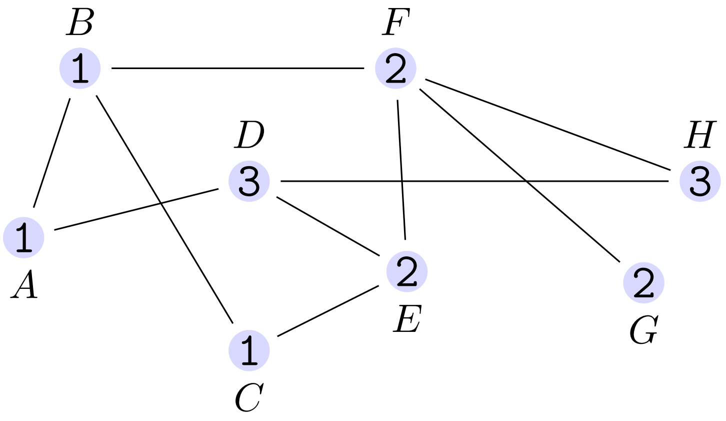


[2] Note that a miner could, in theory, award himself less than the maximal block reward.

[3] This means that it always takes the same time to send a message/transaction to reach the next node.

Exercise 3

Consider the same network topology as before:



Exercise 3.1

a) Compute the expected payoff $\mathbb{E}[R]$ for miner H from the next block that is found (in general). The current block reward is 6.25 BTC. Ignore transaction fees possibly included in the block.

b) Compute the corresponding standard deviation of the payoff to miner H.

Exercise 3.2

In the next step we assume that the miners E, F and G revoke their connections to all nodes and instead join a mining pool hosted by miner H. For simplicity we assume that there are no fees for joining the mining pool.

a) Compute again the expected payoff of miner H from the next block that is found. Assume, that the payoff within the mining pool is divided proportional to the computational resources they contribute to the pool (i.e. if the pool finds a block, miner F receives $\frac{2}{9} \cdot 6.25$)

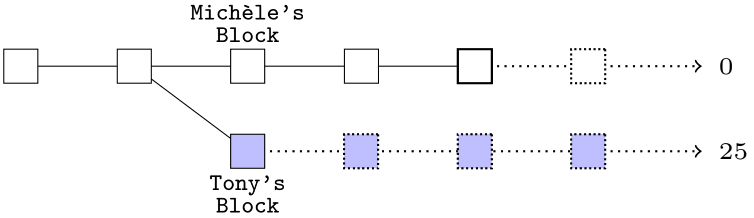
b) Compute the corresponding standard deviation of the expected payoff to miner H.

c) As a last step, can you think of reasons why the consolidation of these four miners into a pool could be problematic for our small example network?

Exercise 4

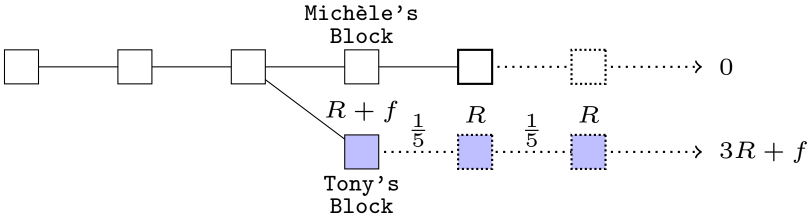
Exercise 4.1

Consider the scenario depicted in the figure below[4]. Michèle and Tony have found a block at the same time, but since then, two blocks were added based on Michèle's block. Tony is very unhappy about this, as he has lost the block reward included in his block because of this. Therefore, he could try to save his initial block reward by finding three consecutive blocks and overtaking the chain with Michèle's block. Compute the relative hash rate $\frac{h}{H}$ of Tony with which he would be indifferent between trying to safe his initial block reward and continuing at the current state of Michèle's chain. Hint: set the expected payoff of Tony's two options equal and solve for the relative hash rate.



Exercise 4.2

In this exercise we slightly alter the story above. Now, we assume that there is only one additional block in Michèle's chain. In addition to that we assume that there were unusually high transaction fees included in the two initially found blocks by Tony and Michèle. We denote these high transaction fees with $f > 0$. All remaining blocks will only include the usual transaction fees, which we assume to be zero for simplicity and thus only consider the block reward R for these blocks. Formulate again the indifference equation for Tony and solve for the transaction fee f. Which relation between f and R results if we assume that Tony controls 20% of the network hash rate ($\frac{h}{H} = \frac{1}{5}$)?



[4] The content of exercise 4 was not covered in the lecture. However it can be found in the (exam relevant) book of the lecture on pages 163 (engl.) or 228 (de).