Sheet 1, WS 2018/19
Cryptocurrencies and Blockchain
Published 9.11.2018
Deadline 30.11.2018

Katinka Wolter
Larissa Zech
Inst. für Informatik
Freie Universität Berlin

Assignment 1. Bitcoin Various Topics

Please explain your answers to the following questions and quantify your answers as far as possible.

1. If a malicious ISP completely controls a users connections, can it launch a doublespend attack against the user? How much computational effort would this take?
2. Consider the following scenario: Even when all nodes are honest, blocks will occasionally get orphaned: if two miners Minnie and Mynie discover blocks nearly simultaneously, neither will have time to hear about the others block before broadcasting hers.
   (a) What determines whose block will end up on the consensus branch?
   (b) What factors affect the rate of orphan blocks? Can you derive a formula for the rate based on these parameters?
   (c) Try to empirically measure this rate on the Bitcoin network.
   (d) If Mynie hears about Minnies block just before shes about to discover hers, does that mean she wasted her effort?
3. Assuming that the total hash power of the network stays constant, what is the probability that a block will be found in the next 10 minutes?
4. Suppose Bob the merchant wants to have a policy that orders will ship within x minutes after receipt of payment. What value of x should Bob choose so that with 99% confidence 6 blocks will be found within x minutes?

Assignment 2. Validation of transactions

Please consider the attachment assignment1.zip. Please implement the requested functions and demonstrate that your validation of transactions is correct. Please hand in your results together with your code.