Information Technology University

Department of Computer Science

http://www.itu.edu.pk

Assist. Prof. Dr. Muhammad Umar

Blockchain

Assignment #2

Question 1: 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 other's block before broadcasting theirs.

4a. What determines whose block will end up on the consensus branch?

4b. What factors affect the rate of orphan blocks? Can you derive a formula for the rate based on these parameters?

4c. Try to empirically measure this rate on the Bitcoin network.

4d. If Mynie hears about Minnie's block just before she's about to discover hers, does that mean she wasted her effort?

4e. Do all miners have their blocks orphaned at the same rate, or are some miners affected disproportionately?

Question 2: Green addresses: One problem with green addresses is that there is no punishment against double-spending within the Bitcoin system itself. To solve this, you decide to design an altcoin called "GreenCoin" that has built-in support for green addresses. Any attempt at double spending from addresses (or transaction outputs) that have been designated as "green" must incur a financial penalty in a way that can be enforced by miners. Propose a possible design for GreenCoin.

Submission Details:

- Submit your answer to the above questions in a single pdf file with the name FirstName_RollNumber_02.pdf
- Your answer must be clear and to the point. Do provide explanation where you think is required
- Follow the naming convention.
- For each convention, there is a 3% penalty if you don't follow it.
- Email the instructor or TA if there are any questions.

- Plagiarism will lead to a straight zero with additional consequences as well.
- 10% (of obtained marks) deduction per day for a late submission.