CS6858: Distributed Trust November 02, 2022

Module 2 Test

Instructor: *John Augustine*

Roll no.: EE19B106 Total points: 48

1. (4 marks) What are mining pools? Give two pros and two cons of mining pools. Discuss at least two mining pool variations based on reward distribution.

2. (4 marks) What is mixing? Discuss the underlying principles of mixing and explain why people use mixing.

3. Consider the following possible changes to the Bitcoin software. Would these changes require a fork or not? Justify briefly.
   (a) (1 mark) Transactions in the mempool are deleted after a certain elapsed time.
   (b) (1 mark) The block size is increased from 1 MB to 1.5 MB.
   (c) (1 mark) Bitcoin scripts now supports an op-code which introduces loops and jumps.
   (d) (1 mark) The node enables a new method / RPC call, in which the user can search for stored texts on the Blockchain.

4. Justify whether the following scenarios can be achieved by an attacker holding 51% of the network's hash power.
   (a) (1 mark) The attacker can block transactions from a single address.
   (b) (1 mark) The attacker can halt payments between some users.
   (c) (1 mark) The attacker can change the mining reward.
   (d) (1 mark) The attacker can create coins out of thin air (i.e., by means other than mining).

5. (3 marks) Dave is a freelance graphic designer hired to design a logo for Rachel's new bakery. Dave does not know Rachel personally and is afraid he might not get paid after he shares his work. Can Bitcoin resolve the payment dispute by ensuring Rachel and Dave get their service and BTC, respectively? Explain your answer.

6. Assume you are an attacker planning on a double-spending attempt.
   (a) (2 marks) Describe how to conduct such an attack in the blockchain.
   (b) (2 marks) How does the consensus mechanism in Bitcoin protect the integrity of the transactions in the case of double spending?
   (c) (1 mark) Is Bitcoin tamper-evident? Explain.

7. (6 marks) Draw a detailed schematic of the ethereum virtual machine (as discussed in class). Define the relevant terms (underline them in your answer) and explain how the ethereum virtual machine works.

8. This question pertains to consistency of hashgraphs.
   (a) (1 mark) Define consistency. (In other words, complete the sentence: "Hashgraph A and hashgraph B are consistent if . . .")
   (b) (2 marks) Is the consistency relation (between hashgraphs) an equivalence relation? I.e., is the relationship reflexive, symmetric, and transitive? (Give your verdict on all three.)
   (c) (3 marks) Prove that two hashgraphs held by any two honest members will be consistent.

9. This question pertains to notions of seeing and strongly seeing in hashgraphs.
   (a) (1 mark) Complete the following sentence. An event x can *see* event y if . . .
   (b) (1 mark) Complete the following sentence. An event x can *strongly see* event y if . . .
   (c) (1 mark) State the *Strongly Seeing Lemma*.
   (d) (3 marks) Prove the Strongly Seeing Lemma.

10. Consider each of the possible Byzantine behaviors listed below (in the context of Hedera's hashgraph and consensus algorithm). Explain how Hedera overcomes them.
   (a) (1 mark) Byzantine member A creates an event for a good member B and tries to gossip this new event (without B's consent).
   (b) (1 mark) Byzantine members refuse to communicate events from some good member B.
   (c) (2 marks) Byzantine nodes stop all communication abruptly.
   (d) (2 marks) A Byzantine member A creates two events that have the same self-parent. (Does this behavior have a name? If so, what is it?)