The Theory Behind Blockchains (Spring 19)
Problem Set 2

Submission: By 15:00 on April 10th, 2019. To be graded by Nathan Geier.

Instructions: You can collaborate with each other and consult external resources. However, you should write the solution on your own, and for each question, list all collaborators and external resources. Otherwise, write explicitly "None". Do not discuss solutions in the course forums; you are welcome to ask for clarifications if needed.

Total number of points in this problem set: 110.

1 Classical Byzantine Agreement (55 points)

a. **(15 points)** Assume there exists some BA protocol for (n, t) where $t \geq n/3$ (i.e., the number of corrupted parties t can be larger than a third of the total number of parties). Show a BA protocol for $(n, t) = (3, 1)$.

b. **(15 points)** Show that if we can solve the broadcast problem for some n and $t < n/2$, then we can solve BA with the same (n, t).

c. **(15 points)** Consider the signature-based broadcast protocol from class (Dolev-Strong protocol), and imagine we would have eliminated round $t + 1$, and only run it for t rounds. Describe an attack against the protocol.

d. **(10 points)** Consider Rabin's BA protocol from the recitation, and recall that we haven't described the break condition from the loop that each honest party executes. Describe a suitable break condition and show that conditioned on termination of all honest parties, they indeed reach a consensus. What is the expected number of rounds of the protocol?

2 Proof of Work and Bitcoin's Consensus (55 points)

In the following, assume you are given an oracle access to a random function $R\colon \{0,1\}^k \mapsto \{0,1\}^k$.

a. **(15 points)** Consider a puzzle given by $y = R(x)$ for a random $x \in \{0,1\}^k$ where the solution is a preimage of y. Show how to solve t puzzles in time $O(k \log(t)) \times (2^k + t)$ using 2^k queries to the function R.

b. **(15 points)** Consider a puzzle given by a random input x where a solution is (i, y) such that $y = R(R(R \dots R(x))$ iterated i times, and y starts with $k/100$ zeros (letting $(i, y) = (\perp, \perp)$ in case no such solution exists). Is this candidate a good proof of work? Explain your answer (informally).

c. **(15 points)** Consider a puzzle given by a string x of length $k/2$, where the solution is a string y of the same length such that $R(x, y)$ starts with $k/4$ zeros. Show that for any t distinct challenges $x_1 \dots x_t$, the expected number of calls to R required for solving all t puzzles is $t \times 2^{k/4}$.

d. **(10 points)** Bitcoin's Consensus: Assume merchants provide merchandise after seeing six confirmations. Assume an ISP (Internet Service Provider) completely controls the incoming communication to a given merchant. Can the ISP launch a double spending attack against the merchant? How much time would this roughly require provided that a block is discovered every ten minutes on average?