Take Home Midterm Exam

CS731A

Release: 13 Feb 2019. Due: 15 Feb 2019. No Late submission will be allowed.

Instruction: Please type in your answers using latex or any other word processor of your choice, and generate a pdf file for submission. Only pdf files will be accepted on gradescope. Also note that you need to write your answer in the order they are given in the question paper, and while submitting, you have to mark each answer for which question they belong to. So please take enough time in hand to submit – and do not wait till the last moment (11:55 pm on the 15th Feb 2019).

Your answers must be well thought out, without any rambling and circumlocution. We will NOT try to find the correct answer in a long-winding answer and will assume that you did not answer correctly. We will not entertain an in-person explanation after grading is done. So your answers must be self-evident, to-the-point, crystal clear answer to the question asked. Any code listing must be neatly formatted for readability with sufficient comments explaining what each line is doing.

1. **[5 points]** Bitcoin transaction rate is 7 transactions per second which is very low compared to traditional payment system. (a) Provide 2 suggestions for changes in the bitcoin blockchain protocol that will increase the transaction rate to 70/second. (b) For each such suggestion, explain why current bitcoin developers do not implement these changes? (What will be the issues with respect to security and integrity of the blockchain if they did?)

2. **[10 points]** Implement a short C/C++ program using SSL crypto-library you installed during your first homework project to (a) create a public key/private key pair for yourself through the program. (b) convert the public key to a bitcoin address (hashing and base58 encoding). Provide your full code listing (with comments for each line), your public key, and the bitcoin address you generate.

3. **[10 points]** My friend told me "*In bitcoin blockchain, double-spend attack is never possible*". Is he right or wrong? Explain your answer.

4. **[5+ 5 = 10 points]** *Selfish Mining* is a behavior of some miners of bitcoin blockchain where a miner withholds the information that he/she has successfully mined a block in the hope of mining another consecutive block before other miners mine a single block. The Selfish miner then publishes the two consecutive blocks together when another miner announces finding a new block. (a) What gains does such a miner obtain by exhibiting such a behavior? (b) A bitcoin developer suggests that each block header must have a timestamp so that we can detect the selfish mining behavior. Do you think that will help in detecting selfish miners?

5. **[5 + 10+ 5 + 10 = 30 points]** Assume that for each miner, the probability of successfully solving the hash-puzzle is p. Also assume that there are n miners in the system. Also, assume once a block has been mined, the new block reaches every node instantaneously (no network latency). So, all miners can start mining the next block simultaneously.

   (a) What is the probability that after the last successfully mined block, k miners will successfully solve the hash puzzle almost simultaneously?

   (b) Prove that the time to mine the next block after the last successfully mined block follows the exponential distribution. What is the parameter of the exponential distribution?

   (c) In the real bitcoin network where the above assumptions are not all valid, can we select which miner's block should be added to the blockchain based on a time stamp provided by the miners into their block headers?

   (d) Suppose Bob – the merchant wants to have a policy that orders placed to him will ship within x minutes of the transaction of payment placed by the buyer to Bob. What value of x must Bob choose so that he can have 99% confidence that 6 blocks will be found in the next x minutes?

6. **[10 points]** If a miner misbehaves, can other miners "boycott" him/her by refusing to build on top of his/her blocks in the future? Will such a "boycott" keep the miners from behaving badly?

7. **[5 points]** Mining pools in the bitcoin works because the members of a pool can prove that they are working hard by sending in their "near-valid" hashes to the pool manager. What measure can a designer of a blockchain take in designing their proof-of-work puzzle or in the way blocks are formed so that mining pool formation will be highly discouraged?

8. **[10 points]** Install `nodejs, npm, ganache-cli, truffle` as discussed in class. Then create a simple smart contract in a file named "`myFirstContract.sol`" which has just one stored state `uint balance`, and a function "`getBalance()`" that returns the current balance. The balance value will be initialized at the constructor function to 100. So your call to `getBalance()` will always return 100. You must list your `myFirstContract.sol` code listing with comments, and your migration script for this contract, and your configuration script "`truffle-config.js`" – after you successfully

run and deploy the contract on ganache based simulated network. Your code listing must have enough comments, and neatly formatted.

9. **[10 points]** Explain how the Ethereum blockchain and Bitcoin Blockchain differ by writing 5 points that you see as pros of Ethereum over Bitcoin, and 5 points, that you see as cons of Ethereum over Bitcoin. Your answer should be technically justifiably and not frivolous points such as "I do not like Digital Currency" or "Ethereum is too complicated". The answers should be to-the-point, and technically sound points.