CPSC 310: Homework 4

Due April 23, 2019, by 10pm

1. Implement a blockchain. By this, we mean implement the ledger — a trustless, decentralized datastore — that underlies the use of blockchains for cryptocurrencies and other use cases. Recommended reading is the Bitcoin whitepaper at `https://bitcoin.org/bitcoin.pdf`, with sections (1), (3), (4), and (5) most relevant to the assignment. You may use any programming language you prefer, but a code skeleton will be provided as `blockchain.py`; similarly, the nodes may communicate over HTTP or TCP as you prefer. Your node software must be able to "mine" a new block and broadcast it to the network, validate the correctness of a new block and the entire chain, and be able to request and receive a copy of the entire chain to store locally.

2. Using your implementation, create four nodes, which we'll call the *generator* node, the *honest* node, the *dishonest* node, and the *joiner* node. Note that these terms are entirely informal and have been introduced in order to clarify Part (3); in a blockchain, all nodes are officially considered equivalent in role and function. The four nodes may be implemented as four independent scripts or as one script invoked with different arguments.

3. Put instructions in a README.txt file that, when executed, cause the following to happen.

   (a) The generator node mines the genesis block and broadcasts it to the honest and dishonest nodes.

   (b) The honest node mines a block and broadcasts it to the generator and dishonest nodes.

   (c) The dishonest node mines a block that ignores the existence of the block from (b) and sends it to the generator and honest nodes, which reject it.

   (d) The honest node mines another block and sends it to the generator node, who accepts it, and the dishonest node, which rejects it.

   (e) The joiner node requests a copy of the blockchain from all the other nodes and accepts the majority chain.

   Each node should print out the current status of its chain after all of (a) through (e) have completed.

4. At the conclusion of Part (3), there should be competing chains that have diverged from one another existent in the various nodes. Think about this divergence visually and then do some research; after you've done the research, answer the following questions in your README.txt file. (a) What is the term used for the state of the network at the end of this execution? (b) Why is this term sometimes used in a positive light?