University of Chicago
ECON2340/CMSC23280: Cryptocurrencies, Winter 2019
David Cash, Harald Uhlig, and Ben Zhao

Assignment 1: Understanding Cryptocurrencies

Due at 11:59pm Wednesday, January 16th

Introduction

This assignment will familiarize you with fundamental components of a Bitcoin-style blockchain and prepare you for future assignments involving this same blockchain. You will be given access to a web-based application written in Python that operates a cryptocurrency called the GoodCoin. By using this application on your local computer and exploring the code that runs it, you will discover answers to a series of questions listed below. You will prepare a short writeup composed of your answers to these questions and submit it through Canvas.

The cryptocurrency in question, called the GoodCoin, has been written fresh for this class, so please alert the TAs if you find significant bugs. Before getting to the questions, we discuss the rules for this assignment and how you can access the code for this assignment. Additionally, we welcome your constructive feedback on how to make this code more user-friendly and a better teaching tool.

Rules

Collaboration policy. Please respect the following collaboration policy: You may discuss problems with up to 3 other students in the class, *but you must write up your own responses. You should never see your collaborators' writing.* At the beginning of your submission write-up, you must indicate the names of your (1, 2, or 3) collaborators, if any. You may switch groups between assignments but not within the same assignment.

Sources. Cite any sources you use. You may Google liberally to learn basic Python.

Piazza. We encourage you to post questions on Piazza. If you have a question that you believe will reveal secrets you have discovered while working on the assignment, post privately to just the instructors. If you have a question that you believe will be of general interest or clarifies the assignment, please post publicly. If you are uncertain, post privately; we will make public posts that we believe are of general interest.

Grading. Responses will be graded for correctness and clarity.

Assignment Tech Set-Up and Overview

All the questions for this assignment can be answered by using the GoodCoin blockchain application, exploring the GoodCoin code, and drawing upon material from class lectures.

Setting up Python

The GoodCoin is written in Python 3, so you will need to have Python 3 installed on your computer in order to use it. Most computers are shipped with a pre-installed version of at least Python 2, but if you need to get Python 3 set up, the guide found at https://realpython.com/installing-python/ will be helpful.

Accessing the GoodCoin

Download the goodcoin.tar file from Canvas, place it in a convenient directory, and untar it (run "tar xvf goodcoin.tar" if you are using a Linux command line).

Running the GoodCoin

The README.org file included with the GoodCoin code should have enough information to get you started. You may need to "pip install" (https://ehmatthes.github.io/pcc/chapter_12/installing_pip.html) several of the Python packages required for the application if you haven't done so previously.

What and How to Submit

You should submit a file `<YOUR CNETID>-assignment1.pdf/txt` that contains responses in English to the questions asked below. You will upload this file to Canvas.

Instructions

After downloading the code and installing the required packages, spend time playing around with the GoodCoin. Explore the code, mine blocks, conduct transactions, and see what you can do. Once you have spent sufficient time understanding how the GoodCoin works, draw on your newfound knowledge to answer the following questions. Note that the relevant code for this assignment lives in blockchain.py and server.py. The other files in the repository (besides the README.org file) are necessary to the functioning of the application but not neccessary to your understanding of the GoodCoin and consequently can be left alone.

Questions

The questions below are divided into two categories, data structures and consensus. Each category contains several questions regarding that subject matter. For each question, a short (1-4 complete, grammatically correct English sentences) response is expected. Grades will be determined by the correctness and clarity of your response.

Data Structures (45 points)

1. Why is the unspent transaction output (UTXO) pool in the GoodCoin necessary?
2. What consequences would arise if multiple nodes were participating in the GoodCoin network and did not effectively synchronize their UTXO pools?

3. What are the criteria for a valid transaction in the GoodCoin?

Consensus (45 points)

1. What criterion does the GoodCoin employ to resolve conflicts in blockchain versions between the nodes? What are the benefits and downfalls of this criterion?
2. What proof of work is used in the GoodCoin?
3. What, in general, is the purpose of a proof of work in a blockchain system?