COL106 : 2021-22 (Semester I)
Project: Overview

Venkata Koppula

August 23, 2021

1 Introduction

Welcome to COL106! As mentioned in class, this course has a lab + project component. The project for this semester is related to *cryptocurrencies*. Perhaps many of you already have some level of familiarity with cryptocurrencies (such as Bitcoin). However, we will **not** be assuming any background with regard to this. We will introduce all the needed components, break down the project into six assignments, each of which can be solved using only the concepts discussed in this course. Hopefully, by the end of the semester, all of you will have your own cryptocurrency implementation. In this outline document, we will describe cryptocurrencies at a very high level.

2 Cryptocurrencies

Before we talk about cryptocurrencies, let us review what a currency is (in loose terms). A traditional currency system (such as the Rupee in India) has a few essential features:

- There is a central entity that can produce the currency. [1]
- There is a physical object (a note or a coin), that has certain currency value associated with it, and it is very hard to 'copy'. This is known as *anti-counterfeiting*, and this is an essential feature of any currency.[2]
- Finally, people can exchange this physical object for goods and services (sometimes you do this in person, sometimes you use a bank for this purpose).

Hopefully all of you are familiar with the above. In 2009, a fascinating new form of currency named Bitcoin was proposed, and has gained immense popularity over the last few years. Since then, many other similar currencies have emerged, and these are collectively referred to as *cryptocurrencies*.[3] Besides being a currency, these ideas have led to several interesting technologies (that have nothing to do with a currency system), and many countries are actively working towards using these emerging technologies. For instance, India's Ministry of Electronics and Information Technology recently published a draft of the national strategy to use such technologies.

So how are cryptocurrencies different from regular currencies? The most important distinction is that they is 'digital' – a unit of the cryptocurrency is just a string of characters that can be stored on your computing device. This should immediately raise a few questions:

- How do we prevent counterfeiting? Any string of characters can be copied, so if someone has one unit of the cryptocurrency, then can he/she produce infinitely many units of the currency?

[1] F.O.F.Y: How are the Rupee notes/coins produced in India?

[2] F.O.F.Y: What are the anti-counterfeiting measures in our national currency?

[3] Please do not confuse cryptocurrencies with banking services like Net Banking, or UPI payment. As we will see later in this course, NetBanking, UPI payments etc are much closer to the regular banking, while cryptocurrencies are very different. For instance, we cannot have NetBanking or UPI payments without a bank, but this is not the case with cryptocurrencies.

- A related challenge in the case of cryptocurrencies is that of *double-spending*. Suppose I have one unit of a cryptocurrency, I should not be able to spend this unit of currency at different places. Note that in the case of physical currency, this is not an issue – if you have a rupee note, you cannot spend it with two people.

3 DSCoin: Our Very Own Cryptocurrency

In this course, we will develop our own cryptocurrency, which we have called DSCoin.[4] Uptil now, we have briefly discussed what a cryptocurrency is. There are two other question that you should ask at this point: *why cryptocurrency*, and *how cryptocurrency*. The 'how' question (how is this cryptocurrency produced/stored, how are transactions made in this currency, etc) will be addressed gradually over the course of this semester. To address the 'why' question, let us consider the following toy scenario.

3.1 Toy Scenario

Suppose, whenever someone joins IIT Delhi as a student, the institute gives him/her 1000 DSCoins. There is also a corresponding software that the students can install, and this software can be used to spend the DSCoins, as well as receive the payments. And these coins can be used for various things (such as sharing your class-notes, holding help-sessions before exams).

Let us first look at the most basic version: every DSCoin is a unique number (so each student receives 1000 such unique numbers on joining IITD). We will refer to this coin number as the *serial number* of the coin. There is an administrative unit at IIT Delhi, who will keep track of the serial numbers associated with each student.

Whenever person A wants to send a coin to person B, person A sends a message to the IITD admin team, stating two things : one of the serial numbers snum that he/she possesses, together with the recipient's details. The IITD admin team first checks that person A indeed has the snum coin. Next, they delete this serial number from person A's account, and include it in person B's account. Once this is done, they send a message to person B, informing him/her that the transaction is complete, and person B is now the new owner of the snum coin. Once person B receives this message, he/she can deliver the goods/services to person A.

First, check that this is a valid currency. Assuming that the IITD admin team is maintaining their database correctly, there can be no double-spending, and counterfeiting is also not possible. The main drawback of this simple scheme is that every transaction needs to be approved/processed by the IITD admin team. And imagine if you had to do this at a global level!

We would like to have a solution where there is no need for the IITD admin team to process each transaction. And to do this, we require a few simple tools from cryptography (hence these currencies are called cryptocurrencies).

3.2 Plan for the Semester

During the course of this semester, we will build this cryptocurrency, as well as the software for processing transactions. Note that our scheme will be very similar to the one used by Bitcoin, so hopefully you will get a good flavor of this exciting new technology. Essentially, there are two categories of tools required for this project. We will require a couple of simple ideas from cryptography (which will be introduced in the first few lab sessions). Next, we will use some of the data structures that we will learn in this course. Hopefully, this will illustrate how the data structures discussed in this course are the *main driving force* behind some of the most interesting real-world technologies.

[4] Propose a better name for our cryptocurrency.