

## Computer Assignment 5


Winter 2024


**Deadline:** Mar 22, 2024, 11:59 PM  
(Upload it to Gradescope.)

---

# Project Description

## Part 1: Learning about blockchains!

First, watch this video:  What is a Blockchain? (Animated + Examples)

Then, watch this one:  But how does bitcoin actually work?


Also, Watch lecture 17 (Review).

If you want to read more details, then read the original Bitcoin paper here:

<https://bitcoin.org/bitcoin.pdf>

## Part 2: Create your own blockchain network

Now you have learned about blockchains, the goal in this part is to build a simple blockchain network from scratch, your network must be able to create a block, perform a transaction between two users and update the chain with the transaction.

You should use this template:  yourBlockchain . You have to write your code using Apps Script. To open it, go to Extensions-> Apps Script. A new tab should be opened.

Here is what you need to do:

1. Initialize a Genesis Block:
  - a. Define the creation of the blockchain, the first element in the chain. *This is already given for the first block.*
2. Define a new block:
  - a. As we add blocks to the chain, we would need to first create these new blocks that have to be added.
  - b. Define what consists of a block and what this block that is to be added to the chain will consist of.
  - c. Add a new block on the Sheet. Change the block number, transactions, timestamps, etc. **All these parts can be done manually!**

3. Perform a Proof Of Work:

- a. The crucial step here, use the previous hash, the current block, and a “nonce” to perform the transaction. Use sha256 to perform hashing.
- b. This is the action of a “miner” where a sender defines a transaction and now the miner has to mine the transaction based on the current block, the hash of the previous block, and a “nonce”. A nonce is some string value that along with the previous hash and the current block solves a cryptographic puzzle.
- c. The cryptographic puzzle you will solve is to generate a hash that starts with 4 zeros. (64-bit hash). **NOTE: if your code runs out of time without finding the nonce, you can solve a simpler puzzle where the hash starts with 3 zeros (we accept either 3 or 4).**
- d. You have to write your own code to find the proper nonce.
- e. Once the block is mined, add the mined block to your blockchain by providing the correct nonce.

## Part 3: Mine your block onto our chain

The second part of the project requires you to act as a miner and mine your data onto our blockchain, based on a provided previous hash, your name (and anything else you want), and a correct nonce.

Here is our blockchain: [📄 ClassBlockchain](#) . The first two blocks are already given! Please add your block as the next (valid) one.

DO NOT replace your classmates' blocks! Yours should be ADDED after the last valid block and BEFORE block N! **If you replace someone else's block, you won't get any points for this project!**

## Bonus:

For 20 extra points (which will be added to your CA5), write a Python code that automatically does everything you need to create a new block by interacting with the classBlockchain Sheet. Your code should read the last valid block hash, create a new block, populate your transactions, and find the correct nonce to generate the correct hash.

## Notes:

1. If you are not familiar with Google Script syntax, there are plenty of available tools! The code you have to add is simple and straightforward so it shouldn't be too hard to write your code even if you are not familiar with the environment at all!

## What to Submit:

1. A pdf file that includes:
  - a. Your code.

- b. Take a screenshot of the Class blockchain with your name shown. (Make sure that your name is properly added to the blockchain. We will search your name to give you full credit.)
2. If you are doing the Bonus, attach the bonus part to the pdf too! Make sure to clearly indicate that your submission includes the bonus part.
  - a. Your Python code.
  - b. You should also upload a screenshot, showing that your code has correctly added a new block to our blockchain.