白崇佑

109065534

For the sake of bitcoin mining, we need to do the proof of work(PoW) process to earn the reward, the process of PoW is in the following:

1. There is a string consisting of the header of the current block, the information of the transaction, time stamp and a random number
2. The following is to apply double-SHA-256, which is like: SHA-256(SHA-256(string))
3. There is a requirement that the beginning of the result of the function must be zero, and people need to utilize the computing power of their equipment to find out the input to match the requirement.

The coding work is to implement the process above to collect the new transactions into a block.