6.857 Homework	**Problem Set 2**	# 2-3 Cryptocurrency
Changping Chen		
Peinan Chenn		
Skanda Koppula		March 8, 2015

(a) 000000c4d41c812229f06b454c5be8ed7578a839ce14a564e29439700b0000d1

(b) 000000000013e89b64470493ae52b798b8c0c3392be7664bf913851134eae35f if the current chain is the longest chain. 0000000013bd8a5052bf398013a5847d17df2ed0ab5856e937e060748bfd3ea6 if a different chain overtakes the longest chain when the assignment is due. I currently suspect that the teams pushing the chain where we have the second hash are hiding their results and will publish all of them when the assignment is due. We coded a GPU based Java program using the aparapi library and continuously tried to add to the current longest chain. The program works by randomly creating hashes and checking if they have the correct number of zeros. Every some seconds, we query to see if the current node has a next node. If so, we stop trying to build a block and work on the next block instead. Generally, we waited at most 4 confirmations to determine that our block was on the longest chain. We have about 300 Megahashes/second and have been running this since 2/26.

(c) To reverse a transaction six levels deep into the chain, you'll need a hashing rate higher than the Bitcoin network hash rate to catch up and create blocks faster than the network. The current hashrate is 339617 Terahash/s (`https://bitcoinwisdom.com/bitcoin/difficulty`). A high end ASICs designed for mining (e.g. AntMiner S4) is advertised at 2 million Mhash/sec, costs $1400, draws 1400 Watts (`https://en.bitcoin.it/wiki/Mining_hardware_comparison`). To achieve a faster than network speed, we'd need about $\frac{339617 \cdot 10^{12}}{2 \cdot 10^6 \cdot 10^6} = 169,809$ of these miners. Wed also need a few more machines to not just match, but also outpace the network to catch up our chain, so well chuck in 1106 more: 172,500 mining ASICs, for a total of $241500000 in initial hardware costs. Bitcoin requires about 51 zeroes at the end of the hash, so itll take about 2^{51} hash guesses to find a valid block hash. That means that to recover 6 blocks with our 1000 extra machines would take $\frac{2^{51}}{2 \cdot 10^6} \cdot \frac{1}{60 \cdot 60 \cdot 60} \cdot 6 \cdot 1000 = 78$ days. Assuming a $0.12 kWH electricity rate, power consumpetion would add another $0.12 \cdot 1400 \cdot (24 \cdot 78) = \$314496$.

(d) Peinan and Skanda spent it on food.