Lalita Sharkey 01063704

CS 764/864: Blockchains and Cryptocurrencies:

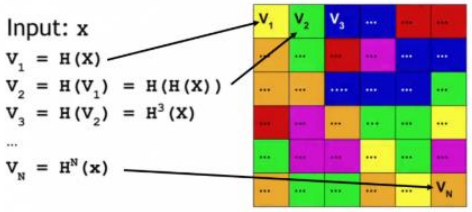
Fundamentals, Technologies, and Economics

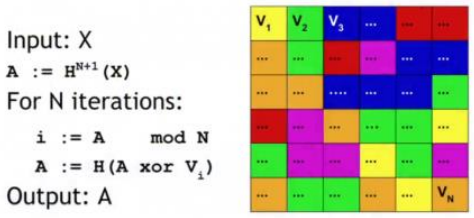
Module 9: Homework 9

Q1. Use Scrypt hash, a memory-hard puzzle, to find the hash of the following ASCII string “scrypt is a memory hard hash function. It is most widely used as an alternative bitcoin puzzle.” Assume N=216

Ref: http://learningspot.altervista.org/asic-resistant-mining-puzzles/

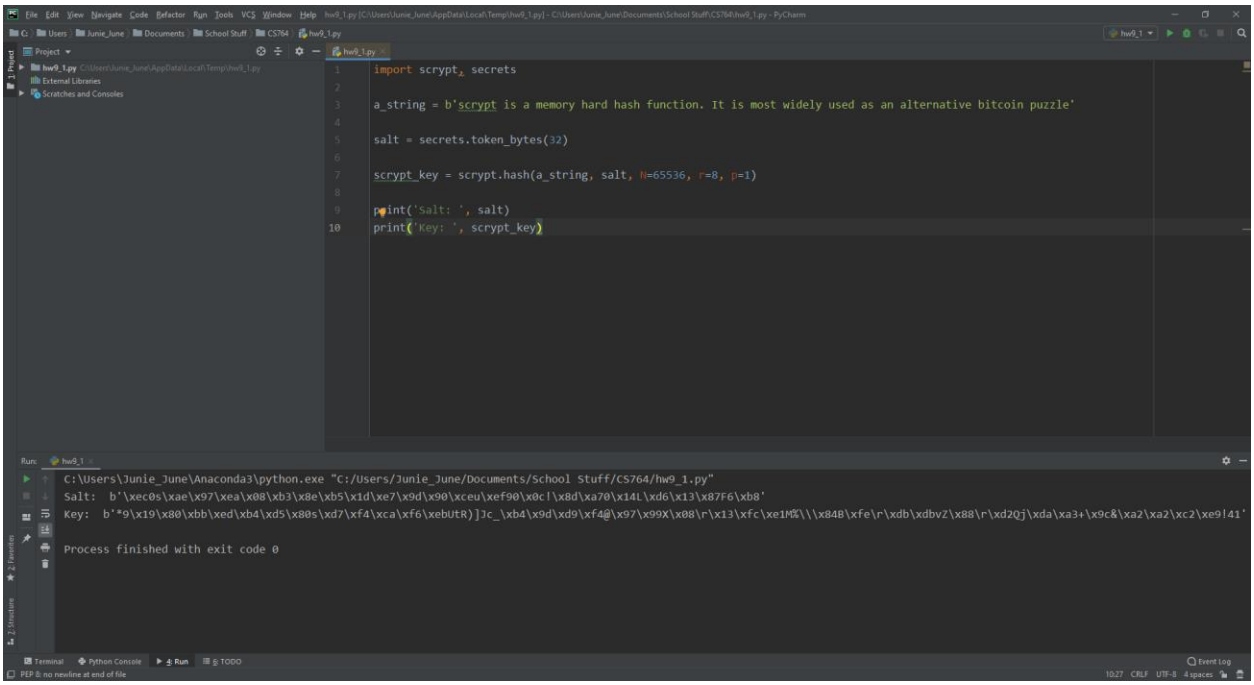
SCRYPT COMPUTATION





Two compute Scrypt hash function of an input string x, H(x), two steps are necessary:

1. Fill a large block of random-access memory with random values. The block can be seen as a matrix that is filled with N iterations. The first value v1 is the hash of x. The second value v2 is the hash of v1. And so on, until reaching vn.
2. Read from this block in a random order. Then we use the accumulator A to pick values back from those cells in a random way. At beginning, the first value is the hash function applied to vn. At every iteration, we compute the value of the index to be picked as the remainder of the division of A by N. Then we compute the following A value applying the hash to (A xor vn). The final value of A after N iterations is the output.



Salt:

\xec0s\xae\x97\xea\x08\xb3\x8e\xb5\x1d\xe7\x9d\x90\xceu\xef90\x0c!\x8d\xa70\x14L\xd6\x13\x87F6\xb8

Key:

*9\x19\x80\xbb\xed\xb4\xd5\x80s\xd7\xf4\xca\xf6\xebUtR)]Jc_\xb4\x9d\xd9\xf4@\x97\x99X\x08\r\x13\xfc\xe1M%\\\x84B\xfe\r\xdb\xdbvZ\x88\r\xd2Qj\xda\xa3+\x9c&\xa2\xa2\xc2\xe9!41

Q2. Lottery with Hash commitments. We have 3 parties in a lottery where one of them will be a winner. Assume X chooses 58906, Y chooses 79654702, and Z chooses 2578012. Each compute SHA-256 hash of their chosen number. They publish their hashes first; then they publish their random numbers; the winner is the one: (H(X) XOR H(Y) XOR Z) mod 3. X is the winner if the final value is 0; Y is the winner if it is 1; and Z is the winner if it is 2. Compute the steps and show each step; and show the final winner.

```
Everyone's hashes
    X: 62bb4451a420dda4dcacb684d6ea659fe2bc65a9e69b2c9174f5704f79f1750d
    Y: 445d769493d9b66c058d1e14e6396b3bd4ded89a3194fbcfbac5b462f39b361b
    Z: a9f2cdd5a0dbf563ad23973feda15d95c5f6a38aeed29c3cc5fd979d0bc6f19a
Everyone's random numbers
    X: 58906
    Y: 79654702
    Z: 2578012

The final value is  1
The Lottery winner is Y
```

Q3 Discuss how a new cryptocurrency “Monarch coin” be built on top of existing Bitcoin network.

I believe we could fork Monarch Coin from the existing but coin. A Bitcoin fork is basically an alteration of the current Bitcoin code (or protocol). A fork can result in the creation of new coins that can be claimed by existing Bitcoin owners. A Bitcoin fork happens when new code is “branched” out of Bitcoin’s source code in order to slightly change the rules of the Bitcoin network. Soft forks that play well with the old rules, and hard forks that create new rules completely. Hard forks result in the creation of new coins that abide to these new rules. Each person that held Bitcoins before the fork, will now get the Monarch Coin equal to the amount of his Bitcoin holdings at the time of the fork. The Monarch Coin either be claimed freely using DIY methods or by using services, which take the hassle away but may charge considerable fees.

Ref: https://99bitcoins.com/bitcoin-fork-segwit-vs-bitcoin-unlimited-explained-simply/