EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 1 : 10 points — September 5, 2019

1. (2 points) What can go wrong if the Bitcoin block header format shown on the left below is changed to the header format shown on the right? The height of a block is the number of ancestor blocks it has.

Version Number
Hash of Previous Block Header
Hash of Transactions
Timestamp
Threshold
Nonce

Version Number
Block Height
Hash of Transactions
Timestamp
Threshold
Nonce

2. (2 points) Suppose (r, s) is a valid ECDSA signature on a message m created using the Bitcoin curve secp256k1. Let n be the cardinality of the secp256k1 elliptic curve group. Show that $(r, n - s)$ is also a valid ECDSA signature on the same message m.

   Hint: Use the fact that $(n - s)^{-1} = n - s^{-1}$ for all $s \in \mathbb{F}_n^*$.

3. (2 points) The Bitcoin ECDSA signing algorithm has the following steps for a message m and private key k. Here n is the cardinality of the secp256k1 elliptic curve group.

   (i) Compute $e = \text{SHA256}(\text{SHA256}(m))$
   (ii) Choose a random integer j from $\mathbb{F}_n^*$
   (iii) Compute $jP = (x, y)$
   (iv) Calculate $r = x \bmod n$. If $r = 0$, go to step 2.
   (v) Calculate $s = j^{-1}(e + kr) \bmod n$. If $s = 0$, go to step 2.
   (vi) Output (r, s) as signature for m

   Suppose the same random integer j is used to create ECDSA signatures on distinct messages m_1 and m_2. Show that there is a polynomial time adversary who can recover the private key k from the messages m_1, m_2 and their corresponding signatures.

4. (2 points) Suppose a Hyperledger Fabric network requires an application to get **three** endorsements before a transaction proposed by it is added to the blockchain. Explain the steps involved starting from the transaction proposal by the application to the addition of the transaction in the blockchain. Assume there are four peers P_1, P_2, P_3, P_4 connected by the same channel who can endorse a transaction.

5. (2 points) Describe the response script which will unlock the following challenge script. The data items `Hash1` and `Hash2` have an implicit data push operator before them which pushes them onto the stack.

```
OP_2DUP OP_SHA256 <Hash1> OP_EQUALVERIFY OP_SHA256 <Hash2> OP_EQUALVERIFY
```

   Hint: The opcodes in the challenge script work as described below.

Operator	**Description**	**Input Stack**	**Output Stack**
OP_2DUP	Duplicates the top two stack items.	x1 x2	x1 x2 x1 x2
OP_SHA256	Replaces the top stack item with its SHA256 hash	x1 x2	SHA256(x1) x2
OP_EQUALVERIFY	Fails the script execution if the top two stack items are not equal. If they are equal, it pops them and script execution continues.	x1 x2 x3	Script fail or x3