EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 1: 20 points Date: August 14, 2018

1. [5 points] How does the 4-byte `nBits` field in the Bitcoin block header get converted into a 256-bit target value?

2. [5 points] How are Bitcoin coinbase transactions guaranteed to have different TXIDs? *Hint: See BIP34*

3. [5 points] Convert the following scripts into their hexadecimal bytecode representations. For convenience, represent all data such as `<PubKeyHash>` and `<PubKey1>` as all zero bytes. *Hint: See script.h in the Bitcoin github repository*
   (a) `OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
   (b) `OP_2 <PubKey1> <PubKey2> <PubKey3> OP_3 OP_CHECKMULTISIG`
   (c) `OP_HASH160 <RedeemScriptHash> OP_EQUAL`

4. [5 points] Describe response scripts which will unlock the following challenge scripts. All data items in the challenge scripts have an implicit data push operator before them which pushes the item onto the stack.
   (a) `OP_2DUP OP_SHA256 <Hash1> OP_EQUALVERIFY OP_SHA256 <Hash2> OP_EQUALVERIFY`
   (b) `OP_SIZE OP_ROT OP_SIZE OP_NIP OP_EQUAL`
   (c) `OP_IF OP_DROP <PubKeyB> OP_CHECKSIG OP_ELSE OP_DROP <PubKeyA> OP_CHECKSIG OP_ENDIF`