Blockchain Technology Fall, 2023
Tutorial 4, Week 7 (Oct 24)
Due Date: Nov 8

Questions:

Suppose Alice, Bob, Carol run a company. To be safe, they agree that only when at least two of them approve, the bitcoins of the company can be spent. Suppose Alice has key pair (PK_1, SK_1), Bob has key pair (PK_2, SK_2), and Carol has key pair (PK_3, SK_3). Please describe how they receive and spend bitcoins of the company **(100 points)**.

Hint: (1) Suppose a customer David (who has key pair (PK_4, SK_4), and an unspent TXO $(val = 200, addr = H(PK_4))$ identified by $(TX_0, idx = 0)$) sends 100 BTC to the company by a transaction TX_1, and the company later spends 60BTC of these 100 BTC to a customer Eve (with PK_5) by a transaction TX_2 . Describe the details of the two transactions, i.e. TX_1, and TX_2, including the scriptSig and scriptPubKey.

(2) You may need to study or design the mechanism of the OP_CHECKMULTIPLESIG operator, for example, its input parameters and outputs.