Mid-Term Examination

Course Name: Introduction to Blockchain and Cryptocurrency (Code: CS577)

Submission Link: https://forms.gle/SzDbsYnmvd8Jdprb7

Deadline: 9:30 a.m., 25th Sept 2021

Make appropriate assumption whenever necessary.

1. why Merkle Tree is used to store bitcoin transactions in a block? How to prevent double spending attack in bitcoin? **[2+3=5 marks]**
2. Consider the following bitcoin transactions T1, T2 and T3, where h_i, s_i and p_i denote hash value, private key and public key respectively. Suppose T1 and T2 both are already in blockchain, whereas T3 is a new transaction issued by a node. Determine the validity of T3 w.r.t. T1 and T2. Show the detailed execution steps of this validity check and justify your answer. **[6 marks]**
3. Given a new bitcoin transaction T. Since large number of transactions are already recorded in the blockchain, how to search the input transactions of T in order to check the validity of T? Propose a mechanism which may reduce the time and space complexities of this search operations. **[4 marks]**

Transaction T1

```
{
    "hash":"h1",
    "ver":1,
    "vin_sz":1,
    "vout_sz":2,
    "lock_time":0,
    "size":404,
    "in":[

                  {
                  "prev_out":{
                  "hash":"h0",
                  "n": 0
                       }, "scriptSig":"s1  p1"
                  }
         ]

    "out":[
                   {
                                  "value":"10.12",
                                  "scriptPubKey":"OP_DUP OP_HASH160 <hash of p2> OP_EQUALVERIFY OP_CHECKSIG"
                  },

                  {
                                  "value":"5.15",
                                  "scriptPubKey":"OP_DUP OP_HASH160 <hash of p3> OP_EQUALVERIFY OP_CHECKSIG"
                  }
            ]
}
```

Transaction T2

```
{
    "hash":"h2",
    "ver":1,
    "vin_sz":1,
    "vout_sz":1,
    "lock_time":0,
    "size":205,
    "in":[

                  {
                  "prev_out":{
                  "hash":"h1",
                  "n": 1
                            }, "scriptSig":"s3  p3"
                  }
         ]


    "out":[
                   {
                                  "value":"5.00",
                                  "scriptPubKey":"OP_DUP OP_HASH160 <hash of p2> OP_EQUALVERIFY OP_CHECKSIG"
                  }

          ]

}
```

Transaction T3

```
{
   "hash":"h3",
   "ver":1,
   "vin_sz":2,
   "vout_sz":1,
   "lock_time":0,
   "size":604,
   "in":[

              {
              "prev_out":{
              "hash":"h1",
              "n": 0
                    }, "scriptSig":"s2  p2"
              },

              {
              "prev_out":{
              "hash":"h2",
              "n": 0
                     }, "scriptSig":"s2  p2"
              }

        ]


   "out":[
              {
                           "value":"15.10",
                           "scriptPubKey":"OP_DUP OP_HASH160 <hash of p4> OP_EQUALVERIFY OP_CHECKSIG"
              }

         ]

}
```