Mid-Term Examination

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

Submission Link: https://forms.gle/ATaGJiguq1N4KdJA6

Deadline: 10 a.m., 4th October 2020

Make appropriate assumption whenever necessary.

1. What are the basic differences between Bitcoin and Ethereum? **[3 marks]**
2. How does a smart contract work in blockchain? What is Gas in ethereum and what is its primary role? **[4+3 marks]**
3. 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. Explain how a network node will check the validity of T3 w.r.t. T1 and T2? **[10 marks]**
4. Suppose bitcoin uses only public key as its address, then what changes would you incorporate in the transaction in order to enable its validation by any nodes in the network? **[5 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":"15.00",
                                "scriptPubKey":"OP_DUP OP_HASH160 <hash of p4> OP_EQUALVERIFY OP_CHECKSIG"
                }

          ]

}
```