Dr. Hemraj Saini

Roll No.: _____

COURSE CODE: 18B1WCI836   MAX. MARKS: 25

COURSE NAME: Block Chain Technologies

COURSE CREDITS: 3   MAX. TIME: 1.5 Hrs

Note: *All questions are compulsory. Carrying of mobile phone during examinations will be treated as case of unfair means.*

Que.1: *[3 marks; CO3]* Alice has a large number of coins each of small value v, which she would like to combine into one coin. She constructs a transaction to do this, but finds that the transaction fee she'd have to spend equals the sum of her coin values, based on this information estimate v.

Que.2: Explain the following terms-

   i.   *[2 marks; CO3]* Brain wallet

   ii.   *[2 marks; CO3]* Hierarchical Wallet

Que.3: *[3 marks; CO4]* What are six different steps for bitcoin mining? Explain through pictorial diagram that how a valid block if found?

Que.4: Answer the following questions-

   i.   *[2 marks; CO4]* What are various energy aspects of bitcoin mining? Explain.

   ii.   *[2 marks; CO4]* Explain two different methods to estimate energy consumption in bitcoin mining. Explicitly estimate lower and upper limits of energy consumption in bitcoin mining.

Que.5: *[3 marks; CO4]* What do you understand by anonymity in bitcoin? Explain how you can do de-anonymize Bitcoin?

Que.6: *[3 marks; CO5]* What is mixing in bitcoin? Explain decentralized mixing.

Que.7: *[5x1=5 marks; CO5]* Explain the following terms/statements-

   i.   Zerocoin and zerocash

   ii.   Block-withholding attack

   iii.   Anti money –laundering in bitcion

   iv.   Bribery attack

   v.   Relationship between the three forms of consensus in bitcoin