

Dr Hemraj Samra

Roll No.: _____

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -III EXAMINATION- May 2019

B.Tech (CSE&IT) VIII Semester

COURSE CODE: 18B1WCI836

MAX. MARKS: 35

COURSE NAME: Block Chain Technologies

COURSE CREDITS: 3

MAX. TIME: 2 Hrs

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

Que.1: a) [2.5 Marks; CO6] What are the basic requirements to design a puzzle for Bitcoin? What is bad-puzzle and good-puzzle? Explain with an appropriate example.

b) [2.5 Marks; CO6] What is ASIC-resistant puzzle in Bitcoin? Write and explain different methods to design ASIC-resistant puzzle.

Que.2: a) [3 Marks; CO6] Explain Proof-of-useful-work. Explain different challenges in adapting Proof-of-useful-work.

b) [2 Marks; CO6] Explain the following term in detail:-

i. Vigilante attack

ii. Proof-of-Stake

Que.3: a) [2.5 Marks; CO7] Explain attacks on Proof-of-"Clairvoyance". If we want to use Bitcoin instead of newspapers for timestamping, where should we place the hash commitment? Somewhere in a transaction? Or directly in a block? Explain.

b) [2.5 Marks; CO7] "Bitcoins are fungible". Explain the statement wrt smart properties.

Que.4: a) [3 Marks; CO7] Bitcoin can solve the real-world multiparty lotteries without trust, how? Explain

b) [2 Marks; CO7] Explain the following terms in detail:

i. NIST beacon

ii. Bitcoin as a beacon

Que.5: a) [2.5 Marks; CO8] Why altcoins are required? Explain three different types of altcoins in detail.

b) [2.5 Marks; CO8] What is merge mining? How it works? Explain in detail.

Que.6: a) [2.5 Marks; CO8] Explain the process of atomic cross chain swap. Clearly writes its usage.

b) [2.5 Marks; CO8] Explain the life cycle of the altcoin. Provide the detail explanation of Pump-and-Dump Cycle.

Que.7: a) [2 Marks; CO8] We can use block chain as the vehicle for decentralization, how? Explain with an example.

b) [3 Marks; CO5] Explain the following terms-

i. Proff-of-Pay

ii. Proof-of-burn

iii. Smart contract