18DCS007
RUDRA BARAD

BT
UNIT TEST - I
27/08/2021

Miracle
Page
Date

Q1. Proof of work (POW) is decentralised connected mechanism that requires members of network to expand effort solving an arbitary mathematical puzzle to prevent anybody from doing any kind of malicious act with the system.

→ POW is used widely in cryptocurrency mining, for validating transaction, mining new tokens

→ Due to POW, Bitcoin & other cryptourrency machanism can be proceed peer to peer or a secure manner without the med of trusted 3rd party.

Example:

→ POW requires a computer to randomly engage in hashing functions until it arrives at an output with correct min amount of landing zeroes. Hash block for block #660000, mined on Dec 4, 2000 is with 19 leading zeroes.

→ That block will always contain 745 transaction involving just 1,666 bitcoins. as well as the header of previous black, If someone timed to change a transaction amount even by 0.000001 bitcoin.

18DCS007
RUDRA BARAD

Q3. (A)

BLOCKCHAIN	DISTRIBUTED LEDGER
→ Blockchain is an extensive set of records called blocks which are linked using cryptography	Distributed ledger is a shared and synchronised database of transaction records of assets
→ Blockchain is dynamic form of distributed ledger technology based on chain of blocks.	Not all distributed ledgers employ a chain of blocks as in Blockchain Technology
→ The organization and development of Blockchain technology is decentralized.	Corporate organization of a distributed ledger technology may not be decentralized.

(B) CENTRALIZED SYSTEM - Systems that use client / server architecture where one or more client nodes are directly connected to central server.

DECENTRALIZED SYSTEM - Every node makes its own decision. The final behaviour of system is aggregate of decisions of individual nodes

~~DISTRIBUTED SYSTEM~~ - ~~Every node makes~~ It doesn't have one central owner. Instead, they use multiple ~~central owner~~

18DCS007
RUDRA BARAD

MERKLE TREE are generated by repeatedly computing hash functions. till only are hash remains which is known as ~~no~~ ~~seed~~ ~~hash~~. root hash.

Here the banker of L_2 nodes so computed and stored in above level L_1 and the hash of L_1 are computed & stored in root hash.

18DCS007
RUDRA BARAD

Q4. (A) PUBLIC KEY CRYPTOGRAPHY - It is an encryption technique that uses a paired public & private key algorithm for secure data communication. A sender uses receipients public key to encrypt to decrypt receipients private key may be used.

DIGITAL SIGNATURE - A digital signature is mathematical technique used to validate authenticity & integrity of a message, software or digital document.

(B)

SYMMETRIC KEY ENCRYP.	ASYMMETRIC KEY ENCRYP.
→ It only requires a single key on both encryption and decryption	→ It requires two key one to encrypt & other one to decrypt
→ It is used when large amount of data is requir to transfer	→ It is used to transfer small amount of data.
→ The size of cipher text is small or same than original plain text	→ The size of cipher txt is same or longer than original plain text.
→ Eg 3DES, AES, DES	→ Eg. DSA, RSA, Diffie Helman.

18DCS007
RUDRA BARAD

Q5. CIA triade refers to the 3 goals of cyber security confidentiality, integrity, availability of organization system, network & data.

(i) CONFIDENTIALITY - the main aim is to hide information from unauthorized access.

Sender & intended receipient should be able to access the content of the message but disclosed to unintended people.

(ii) INTEGRITY - the aim is to protect data / messag from unauthorized change.

(iii) AVAILABLITY - The aim is info /content should be available to authorized used when it is needed.

An active attack attempt to alter system resources or affect their operation. It is difficult to prevent active attack.

(i) MASQUERADING - It is type of activ attack in which attacker impersonat somebody

(ii) REPLAYING - In this attacker obtains the copies of messag sent by authorised user & latr tries to replay it to creat unauthorized effect.

18DCS007
RUDRA BARAD

Q6. HASH FUNCTION - A hash function maps a variable length manage into a fixed length value known as message digest.

Different mesrages have different hash valur i.e. hash functions are collison free.

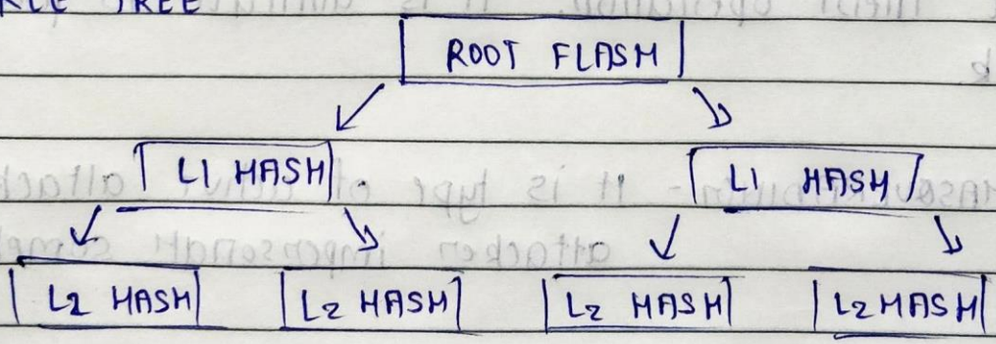
SHA 256 - 256 bit digest is generated

STEPS of SHA256 ~~OF~~ ALGORITHM

(I) Approved padding bits to messagr
(II) Append length to message
(III) Initialize hash buffer.
(IV) Message is proiessed in blocks, module consist of 64 rounds

SHA 256 has a block size of 512 bits, word size of 52 bits.

MERKLE TREE



18DCS007
RUDRA BARAD

DISTRIBUTED SYSTEM - It is similar to decentralized one in that it doesn't have single central owner. It diminates centralization. In this user have access to data, though user privileges can enable when needed.