DAY-1 Assignment

Q.1. What is your understanding of Blockchain?

Ans: It can be defined in just one line that "Blockchain is an immutable distributed ledger". Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority. Blockchain at a fundamental level maintains trust.

Characteristics: -

1. Replication
2. No Central Authority
3. Irreversibility
4. Accessibility
5. Time-stamping
6. Cryptography

Q.2. What is the core problem Blockchain is trying to solve?

Ans: Blockchain came into picture with the International banking crisis with the collapse of the investment in 2008 (culminated with the bankruptcy of Lehman Brothers).
Blockchain can solve various problems, few of them are mentioned below:

1. Cross-Border Payments
2. Supply Chain Management
3. Accountability Issues with Traditional Contracts and Agreements
4. Identity Theft
5. Managing and Protecting Patient Data in Health Care Organizations
6. Digital Copyright and Piracy
7. Government Systems and Public Sectors
8. Crowdfunding and Fundraising
9. Real Estate
10. Sports and E-Sports

Q.3. What are the few features that Blockchain will give you?

Ans: Data stored in blockchain is immutable and cannot be changed easily. Also, the data is added to the block after it is approved by everyone in the network and thus allowing secure transactions. Those who validate the transactions and add them in block are called miners. The basic advantages of Blockchain technology are decentralization, immutability, security and transparency. The blockchain technology allows for the verification without having to be dependent on third-parties. The data structure in a blockchain is append-only.

Basic features: -

1. Cannot be corrupted.
2. Decentralized Technology.
3. Enhanced Security.
4. Irreversible/Immutable.
5. Distributed Ledgers.
6. Consensus.
7. Faster Settlement.

Q.4. What all things does a Block in Blockchain contain?

Ans: A block contains:

- Block number.
- Transaction records.
- Previous block signatures.
- Mining Key.

Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

Blocks contain a block header, which is the metadata that helps verify the validity of a block.
Typical block metadata contains:

- version - the current version of the block structure.
- previous block header hash - the reference this block's parent block.
- merkle root hash - a cryptographic hash of all of the transactions included in this block.
- time - the time that this block was created.
- nBits - the current difficulty that was used to create this block.
- nonce ("number used once") - a random value that the creator of a block is allowed to manipulate however they so choose.

Q.5. How is the verifiability of Blockchain has been attained?

Ans: Generating trust from nothing is one of the first major feats blockchain is hyped to do, but blockchain itself doesn't generate trust out of nothing. It actually derives from the system in which blockchain is used. A blockchain is actually just a chain of blocks of data having a particular structure which ensures its self-integrity, it can only be used to guarantee the data written to the chain was done so in a certain way. Multiple blockchains can be created with the same data up to a certain point

Since the blockchain itself doesn't create trust, let's look at how Bitcoin creates trust around the blockchain. To create trust in the blockchain, one needs to verify relations between a few objects:

- Unique tokens, each containing a history of each previous owner.
- Transactions being broadcast to each node.
- The blockchain itself, containing a list of all past transactions and newly minted tokens. It serves as the distributed state of the network.
- Nodes, which only accept verifiable blocks from other nodes.

Trust Architectures: -

- ✓ Peer-to-peer trust
- ✓ Leviathan trust, which is institutional and involves contracts
- ✓ Intermediary trust, like PayPal or credit cards that make a transaction work
- ✓ Distributed trust, which is what blockchain enables — an emergent trust in the system without any individuals in the system trusting each other

==========