BLOCKCHAIN ESSENTIALS – DAY 1 ASSIGNMENT

Question 1:
What is your understanding of blockchain?

Sol- The classic definition of blockchain is "Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure chronological and immutable way in decentralized distributed network."

It is a mix of two technologies – distributed database and cryptography.

Basically, blockchain is encrypting data by creating many blocks and connecting them by using a HASH code. The hash code of the previous block is included in the new block which is then used to create a new hash code for that block and so on. The hash code changes with even the smallest of changes in the data, this prevents authenticity of the data.

Copies of this data is made, which is then used to verify whether the data is untampered. If the hash code in any of the copies differs, it is verified by using the other copies and that block of data is replaced entirely with the correct data.

If any updates have to be made then the existing data is not changed instead a new block is added with hash code of the previous block. This update is made in all the other copies too.

So, the data in blockchain is verifiable, unchangeable, tamper-proof and immutable.

Question 2:
What is the core problem Blockchain is trying to solve?

Sol- Blockchain is trying to eradicate the following problems of the internet:

- Authenticity : Anyone can update or delete or tamper the information on internet, blockchain tries to avoid this by using hash codes, so that even the slightest of tampering is noticed.

- Security : Information is vulnerable on the internet but because of the unique hash code in blockchain, information cannot be changed without a change in the hash code. Hence, the information is safe and immutable.

- Need of powerful third party for trust. Not everything on the internet can be trusted, there should be a third party that can be trusted. Blockchain tries to solve this problem by creating trust among the community(peer copies) rather than a third party.

Question 3:
What are the few features that blockchain will give you?

Sol- Blockchain gives the following features:

- No Hacking : The data cannot be hacked in blockchain as an internal network system is formed which prevents people from hacking into the system and even plagiarism can be prevented.

- Huge Security Boost : In blockchain, several copies of the data is made with peers. So, for every update to be made it's validity has to be checked. This highly boosts the security.

- Verifiable : In case there's any change in the data in any of the blocks, it can be verified with the peers and the data can be replaced from the nearest peer.

- Data transparency : There is assurance that the source of the data is official and is coming from the right place and it can be trusted.

- Decentralization : Instead of having a superior entity to manage and control data, it is distributed among many peers.

Question 4:
What all things does the block contain?

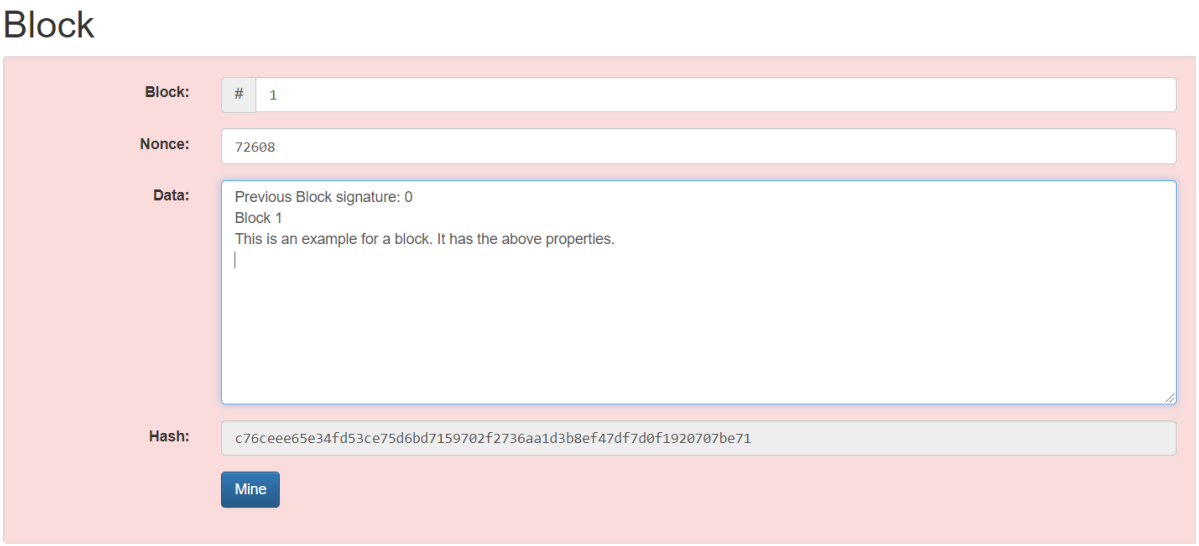
Sol- A block contains:

- Block number : The number of that particular block.
- Transaction records : All the transactions i.e. updates.
- Previous block signature : The signature of the previous block is added in the new block which helps to verify data.

Example :-

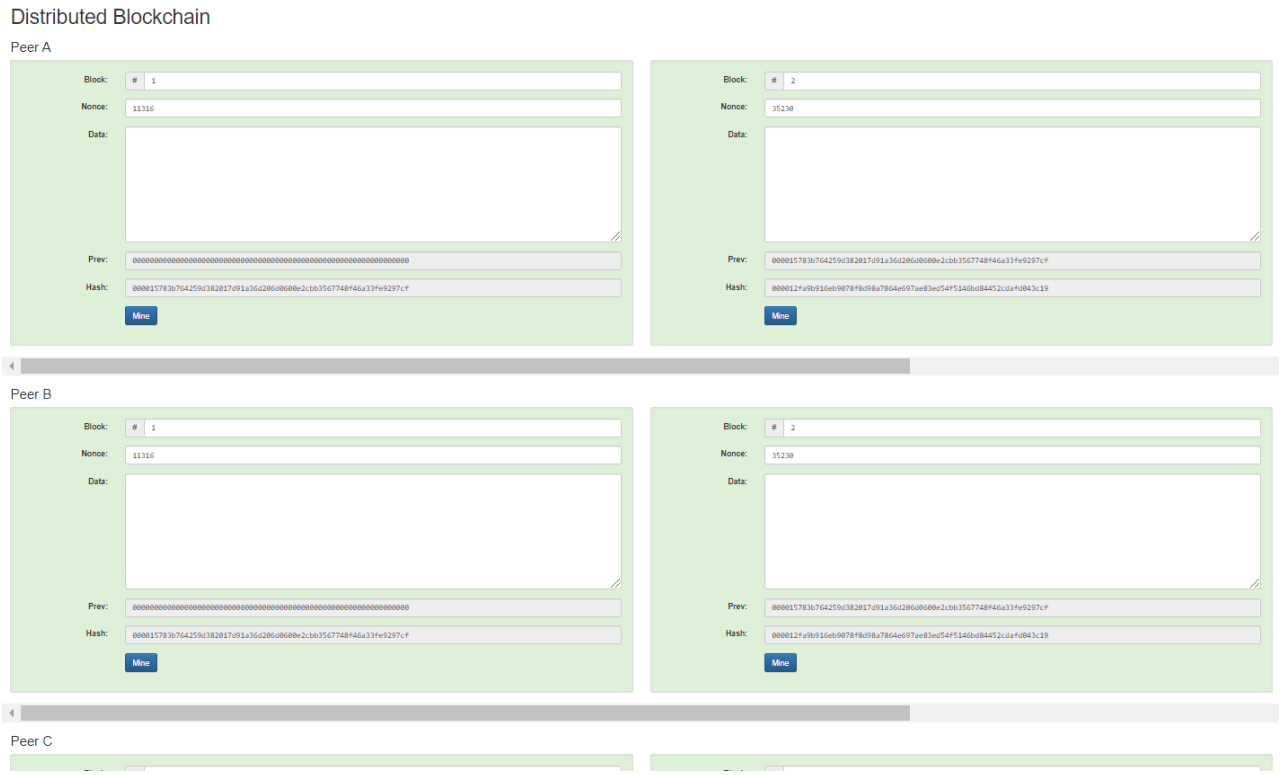
Previous Block signature: 0 Block 1 This is an example for a block. It has the above properties.

Signature :
c76ceee65e34fd53ce75d6bd7159702f2736aa1d3b8ef47df7d0f1920707be71



Question 5:
How verifiability of blockchain has been attained?

Sol- The verifiability in blockchain is achieved due it's distributed database as the signature/hash code of the previous blocks and current blocks is verified among the peers.



We can also see that the hash of block 1 and prev of block 2 matches.