# **Assignment 1 & 2**

Q1: Satoshi nakamoto’s white paper

Observations:

1. A p2p network for transferring cash directly without depending upon intermediaries or third parties.
2. White paper discuss about the transactions between the parties

* Also prevent double spending problems – included a time stamp server
* In order to add a block , the transaction which are stored inside have to be verified by nodes using consensus mechanism (proof of work – which depends on the computational power of the local machine )
* The transaction stored inside a blocks are converted into root value using merkle tree method.
* For each successive block addition, will give the miner rewards .
* If suppose 2 blocks are added at the same time in the chain leads to longest chain rule ( the chain with larger computation power \_PoW\_ and doesn’t depend on total number of blocks )
* Privacy : By keeping public key anonymous, we can maintain privacy , shows all details except individual names

Q2: International Bank crisis 2008

Observations:

1. Banks provided loans only to the eligible person which means who can pay the loans and its interest (Prime Loans).
2. Investment banks starts giving subprime loans the people who are not having valid documents or jobs.
3. Mortgage Loans are increased and so as the interest rates.
4. For several years, the banks were doing good. when the interest was increasing, the people who does have any proper jobs are failing to repay the loans. Which makes the loans as NPAs.
5. This leads many investment banks and agencies to bankrupt. And most people lost their homes.

Q3: Try to get some idea about https://andersbrownworth.com/blockchain/ (self)

Observations:

1. Genesis block always has the previous hash value as 0’s because it is the first block of the blockchain.
2. Mining the block doesn't depends upon the data size, its depends upon the nonce value (number used once) to get the required number of leading zero’s.
3. Higher the nonce value (Higher the number of iterations) higher the time takes to mine a block.
4. In bitcoin, appx 14 mins time taken to create a block. If the block is created before 14 mins then the difficulty of the next block will be increased to manage the 14 mins mark.
5. Even a single space include in the block data can modify the hash value. Which makes the blocks gets disconnected with the previous block.