Chapter 2 and Chapter 3 Summary:

Bitcoin introduced new concepts that made it different from previous distributed agreement solutions. Distributed consensus plays an integral role in Bitcoin's decentralization idea. The nodes in this network have to reach consensus on which transactions are broadcast and the sequence of happened transactions. Hence, they need a single, global ledger for maintaining this view. In order to agree on on a block of transactions in Bitcoin, every node in the network tries to present its own transaction pool to be the next block and it must be done at regular intervals. One of the novel ideas about Bitcoin is its incentive to the owner of the proposed block. The other assumption of Bitcoin is that its consensus algorithm depends on randomization. The consensus takes for a long period of time and even at the end of it there is no confident that any certain block is confirmed. The probability of being confirmed is increased as time goes on. Bitcoin nodes can have different identities. Although, this feature introduces the risk of Sybil attacks, it brings somehow privacy for Bitcoin's participants. Bitcoin provides implicit consensus. That is to say, if a block has been extended in the blockchian it means that it has been accepted by the network, otherwise the block is rejected. Also, it should be mentioned that double spending cannot happen in the network, since if the next node extend the double spend block, this chain will be longer that the other block with the malicious use, so just one of the blocks and transactions will be accepted and the other will be ignored. This is the reason that Bitcoin suggests to wait for several confirmations and after that being confident about a valid transaction. Incentive mechanism of Bitcoin depends on block reward which is given to the producer of a block, and transaction fee which is spent from owner of a transaction to the miner as a reward. These are given to the miner because it has done a lot of computation work which is called proof of work. The difficulty of work and solving the puzzle and finally finding a block is going to increase. In Bitcoin, every other node compute and verify proof of work of the node that has been computed before. It has also considered that 51 percent attack is not possible in Bitcoin and if it happens the developers will notice and react to this attack.

Instead of using account-based model, Bitcoin just keeps track of transactions which have inputs and outputs. The inputs are coins that want to be consumed and the outputs are the created coins. Whenever a new transaction is added to the network, it should be validated by checking that it has not been spent before, and this is done by the help of the hash pointers. All the transactions will go into blocks in order to reach an optimized condition for miners, so they do not need to reach consensus on each transaction individually. Blockchain comprises two hash-based data structures. It has a hash chain of blocks and a tree data structure for each block that contains the transactions in that block. The latter data structure is called Merkle tree that compacts all transactions of a block efficiently. For publishing transactions, Bitcoin uses a flooding algorithm which is called gossip protocol to be sure that all the nodes will hear about the transactions. However, due to the latency

or some other flaws in the network this cannot happen all the time. At the end trying to change features of Bitcoin protocol is possible by creating hard fork or soft work. Hard fork makes totally new chain, meanwhile, soft fork avoid the permanent split.