Blockchain

* A block that contain Data (multiple transaction), Previous Hash (point to the previous block), Hash, Nonce (No. used only once) and Timestamp
* 1st block (Genesis block – no previous hash)
* Hash will change if someone tempered with the block causing the link to be broken
* An immutable ledger (cannot be easily changed) as need to change all the blocks because of the links.
* Distributes P2P network (blockchain is copied across all the computers in the network)
* Will sync with other computers to check if the blockchain is the same/tempered (make decision based on majority)

Consensus Protocol (Proof of work)

Consensus protocol provide system consistency even when some sub system is inconsistent. Because decision is made based on majority consensus (if the no. of traitors is not more than 30%)

* Attackers – add a malicious block at the end of the chain (Check if it satisfy all the criteria)
* Competing Chains – both computers add block (one purple, other orange) at once (wait for next block to be added, see which chain is longer), if orange chain is longer, throw away purple ones (orphaned blocks)

Nonce (No. used only once)

* A number that can be used to vary the hash just by changing that number
* Miners try different nonce in order to guess the correct hash that is below the target
* Even though Nonce only got 2^32 combination, which is not enough to figure out the hash, it can be reused every time the timestamp updates.

