Summary topic 3

The Blockchain consensus technologies Proof-of-Work (PoW) and Byzantine fault (BFT) sits at two different ends of the scalability spectrum. PoW based blockchains offers good scalability but poor performance, while BFT offers good performance for smaller amount of nodes but poor scalability.
A big advantage of PoW is that in order to start participating in the protocol you only need to know one pier to start. These public blockchains are also called permissionless blockchains. BFT on the contrary needs every node to know the whole set of peer node in the consensus to reach. This also requires a centralized identity management which are trusted to issue identities and cryptographic certificates to nodes. This puts BFT at a disadvantage to PoW and BFT blockchains are often called permissionless blockchains. PoW and BFT consider different adversaries. In PoW protocols what matters is the computational power controlled by the adversary. It is shown that Bitcoin becomes vulnerable only by 25% of the computing power being in control by an adversary. BFT rather use a voting scheme that can tolerate up to n/3 corrupted nodes. This is only when the network is allowed to be asynchronous. If a network is synchronised this threshold can be raised. PoW protocols relies on the local time of a node to give it a timestamp. A block is generally accepted if it's timestamp is greater than the median of the last 11 blocks. Because of this a loose clock synchrony is needed. This has also allowed for timestamp manipulation to perform attacks against PoW blockchains.
BFT does not normally depend on a physical clock but it still need to sometimes to use synchronous communication to ensure liveness.