This week the topic is alternative consensus to see how different mechanisms might improve some of the more general aspects previously investigated related to BFT and Nakamoto-consensus.

Concrete the chains Avalanche and Algorand propose alternative ways for reaching consensus and suggest that their mechanisms are also ideal for improving the scalability of their networks.

Avalanche guarantees liveness and scalability of consensus, no matter how many nodes participate in the network. The primary avalanche network has three inbuilt networks: X-chain, C-chain, and P-chain - each with a dedicated mission. X-chain is similar to a DAG, and its purpose is to secure the network or carry out the nodes' work. C-chain is a copy of the Ethereum EVM for smart contracts. Finally, the P-chain manages the subnets and users. Subnets are flexible in that they might append features for a specific use case. For example, it might be permissioned or permissionless, and it can also decide what consensus mechanism to use. As far as I understand, the Avalanche network uses something called the Snowman protocol combined with the Avalanche protocol to achieve the promised benefits of the network. It is supposed to follow the same mechanics in a linear flow. Not sure how this can be implemented and carried out in practice.

Algorand is the second network with another alternative to reach consensus. It presents what they call a pure proof of stake, where participants' incentives in the network are aligned to keep the network honest, based on their staked value in the network. For each transaction in the network, there is a semi-random function, based on the tokens staked, that decides which nodes are selected to carry out the wanted task. This function, VFR, considers nodes with a higher amount of staked tokens to proportionally get a higher probability of executing operations.