- We looked into Byzantine Fault Tolerant systems, a presentation of a practical use case, and also looked at it as a consensus mechanism vs PoW.
- One of the papers looked into the differences between PoW and BFT as consensus protocols and argues what benefits and limitations exists for the two. Some proposals for possible synergies are also explored to circumvent bottlenecks and exploit the opposing consensus mechanisms qualities.
- Struggled to understand fully but the concept of BFT systems is a system that manages to work while not demanding trust. The BFT system should work while having Byzantine faults or Byzantine nodes in the system. There always needs to be made some assumptions about the adversary/adversaries to consider how the system might achieve the state of Byzantine fault tolerance. What kind of network do we consider, is there cryptography involved, etc. It seems to me that absolute BFT systems are hard to achieve because of the computation power needed. One of the papers describes a more practical solution, presenting a system that is functional and BFT. Tbh I struggled to comprehend everything from the paper.