**CONCLUSIONES DE PAPERS DE BFT Y DE INSTAMBUL BYZANTINE FAULT TOLERANCE ALGORITHMS**

Los BFT se van a suceder constantemente en todas las implementaciones de blockchain publica/permisionada. Se tienen en cuenta en blockchain públicas como la de Ethereum en su investigación para PoS. Del mismo modo se producen en permisionadas.

Las primeras lecturas son “Scaling Consensus for Enterprise\_ Explaining the IBFT Algorithm” y “IBFT\_Proposal”. Explican conceptos similares. Explican la base del funcionamiento de los algoritmos en blockchain permisionadas, aunque la explicación es muy cercana a Ethereum ya que explican que se podría llevar a cabo en Ethereum salvo por el problema de que los nodos no son conocidos en Ethereum, así que se extrapola a las permisionadas.

La siguiente lectura es como funciona el algoritmo Quorum de JPMorgan. En este algoritmo se basan dos de las blockchains permisionadas más importantes del momento (Hyperledger de IBM y Alastria).

**CONCLUSIONES DE TODO EL REPO + WHITEPAPER DE QUORUM**

El funcionamiento es muy similar a Ethereum, de hecho, es una rama de go-ethereum a la que le han incluido una capa encima. Permite transacciones y SmartContracts privados con una especie de Sharding para constelaciones de nodos incluidos en el “party”. Permite un mayor rendimiento que las públicas debido a que los nodos son conocidos. Utiliza etcd+raft. El protocolo es sencillo una vez se conoce el de Ethereum, por lo tanto, las mejoras anteriormente propuestas para Ethereum son extrapolables a quorum. Sin embargo, quorum tiene un throughput de decenas a cientos de transacciones por segundo por lo que esas mejoras pueden no ser necesarias. Hay que tenerlas presentes pero hasta el momento nada más que añadir.