- Focus on Merkle Trees and how the Bitcoin network leverage previous technology and thinking realizing what Satoshi described as a Peer-to-Peer Electronic Cash System. The Merkle tree is a hash-based data structure essential for a trustless and decentralized system. For the Bitcoin network, a binary Merkle tree is used where each sub-tree may consist of a root and two leaf. The hash of the root will be decided as a result of the two leaf's hashes combined. One might consider the combination of two leaf's hashes (or transactions) to form a block. Blocks appended to the chain - Blockchain - can by this be trusted by enabling verification based on the root has (the last block appended), as this will be a result of previous blocks.
- More specific for Bitcoin, I mentioned that it combines previous tech or ideas, such as the Byzantine Generals problem, together with the concept of Proof of Work (influenced by Hashcash - prevention of spam), overcoming difficulties related to a fully distributed and trustless system in need of coordination. In Bitcoin and Beyond the authors also go into some depth on the underlying mechanics of the Blockchain, and how Bitcoin prioritizes security and decentralization over scalability. This is perhaps what most critics argue is the weakness of the Bitcoin network. Although one might consider it a weakness, a chain must, according to the Blockchain trilemma, choose how to be valuable.
- For further research, it might be interesting to look more into the trilemma, and how scaling might be realized with a second layer on top of the main Bitcoin network