Summary
3. Byzantine Fault Tolerance

Byzantine faults affect distributed systems in which components being actually faulty can appear as faulty to some network nodes and non-faulty to others.
Byzantine Failures are characterized by multiple Byzantine faults hindering the correct functioning of the system. Since they are among the most general failure modes, Byzantine Fault Tolerance (BFT) is particularly difficult to achieve (Wikipedia.org).
The paper by Castro and Liskov (1999) presents an algorithm enabling state machine replication that achieves BFT in the presence of (n-1)/3 faulty nodes which was proven to be the maximum amount of faulty nodes not degrading the system performance. Furthermore, it is particularly relevant that the algorithm doesn't assume synchrony of the network.
The paper also describes a practical implementation of a distributed file system implementing the algorithm, and reports experimental results concerning its performance evaluation.
These show that the system delivers performances that are close to unreplicated systems.

Vukolić (2016) documents the adoption of BFT state-machine replication in several blockchains to overcome the low performance of Proof-of-Work protocols caused by high latency and low throughput of the system. Such aspects are considered as critical by the author, due to the rapidly evolving requirements of blockchains.
Vukolić (2016) provides an overview of existing alternative consensus protocols and proposals to increase blockchain scalability.
The author highlights that the standard BFT protocols are demonstrated to deliver better performances compared to the PoW protocols, but face potentially limited scalability in terms of number of nodes.
Other main divergences between the two consensus protocols concern the node identity management (the BFT consensus relies on a list of authorized IDs, while PoW is permissionless), the consensus finality, tolerance to adversary attacks (up to 25% computing power for PoW, and up to 33% voting power for BFT protocols), network synchrony and correctness proofs.

References

Castro M., Liskov. B. (1999) A Correctness Proof for a Practical Byzantine-Fault-Tolerant Replication Algorithm. Technical Memo MIT/LCS/TM-590, MIT Laboratory for Computer Science.

Vukolić M. (2016) The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In: Camenisch J., Kesdoğan D. (eds) Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science, vol 9591. Springer, Cham. https://doi.org/10.1007/978-3-319-39028-4_9