Kasper Borgbjerg
kasperib@uio.no

Byzantine fault tolerance

Concerning bitcoins consensus mechanism, there exists a threshold, more specifically a tolerance level of how to achieve overall system reliability when faulty processes can occur in the system. This tolerance is called Byzantine fault tolerance (BFT) and is based on a trust problem in which some of the parties of a group are malicious, thus, trusted communication between the honest parties cannot be achieved. BFT is used to characterize a system that tolerates a set of failures related to the Byzantine general's problem.

Byzantine general's problem (BGP) is based on a scenario of a commander to lieutenant setup, where to reach consensus all the lieutenants must agree on the decision received from the general. *Rules for the setup:*
1. the subordinate lieutenants must agree on the same order
2. if the general is loyal, then all the loyal lieutenants obey the order from the general.

In addition to the second rule, consensus must still be reached if the general is a traitor, as the lieutenants must take the majority vote.
To reach a consensus in regards to the BGP, an algorithm will achieve this if there are at least is 3m generals and at most *m* traitors. The point of this consensus is that the majority of the lieutenants choose the same decision, not a particular one.

To sum up, an algorithm is Byzantine fault-tolerant if the number of malicious nodes does not exceed 1/3 of the honest ones.