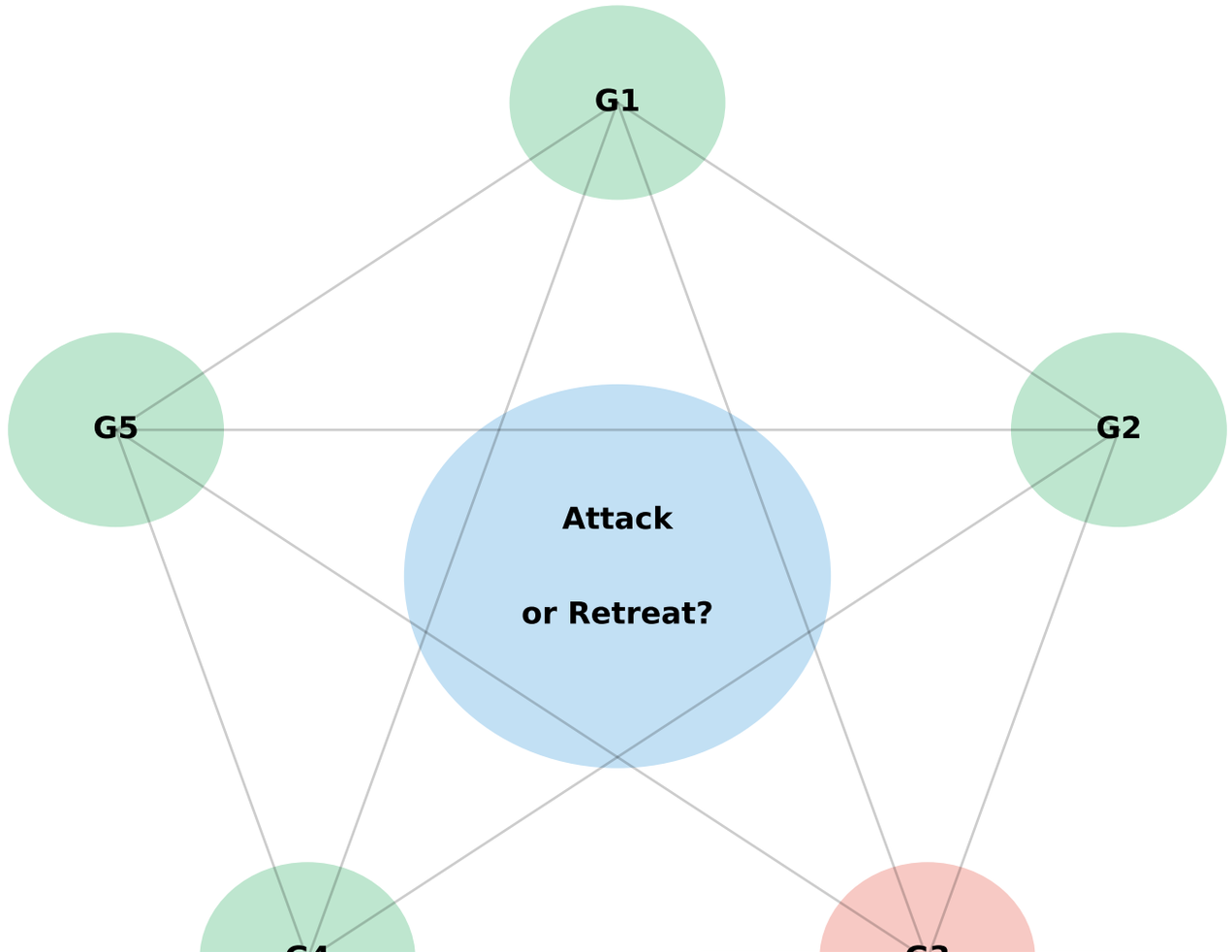
Byzantine Generals Problem

How do distributed nodes agree without trusting each other?



Byzantine Fault Tolerance (BFT)

Must tolerate f faulty nodes

Requires n >= 3f + 1 nodes

(Can tolerate up to 33% malicious)

Blockchain Solution

PoW: 51% honest hashpower

PoS: 2/3 honest stake

Economic incentives align behavior

Source: Lamport et al., "The Byzantine Generals Problem" (1982)