Lecture blockchain

Wednesday, 18 October 2023 14:40

Byzantine generals problem

decide to attack or retreat, must reach consensus
↓
otherwise defeat

communicate via messengers
↳ unreliable

generals may be traitors

given
- variable x
- set of n nodes
  each node i has initial value x_i for x
  subset of f faulty nodes, $n-f$ correct nodes
- nodes communicate by sending messages

goal: have correct nodes agree on common value X for x.

consensus protocol must satisfy

agreement — if decide, same value

validity — if decides X, X was proposed

termination — eventually decide

original application of Bitcoin blockchain: distributed ledger

account = private/public key pair with current value

transaction: transfer of value from input to output accounts

fee $\Delta = \Sigma$ inputs $- \Sigma$ outputs

mining — limits communication overhead to $O(n)$ nodes
maintain integrity of blockchain