# Consensus

## PAXOS

* Phase 1

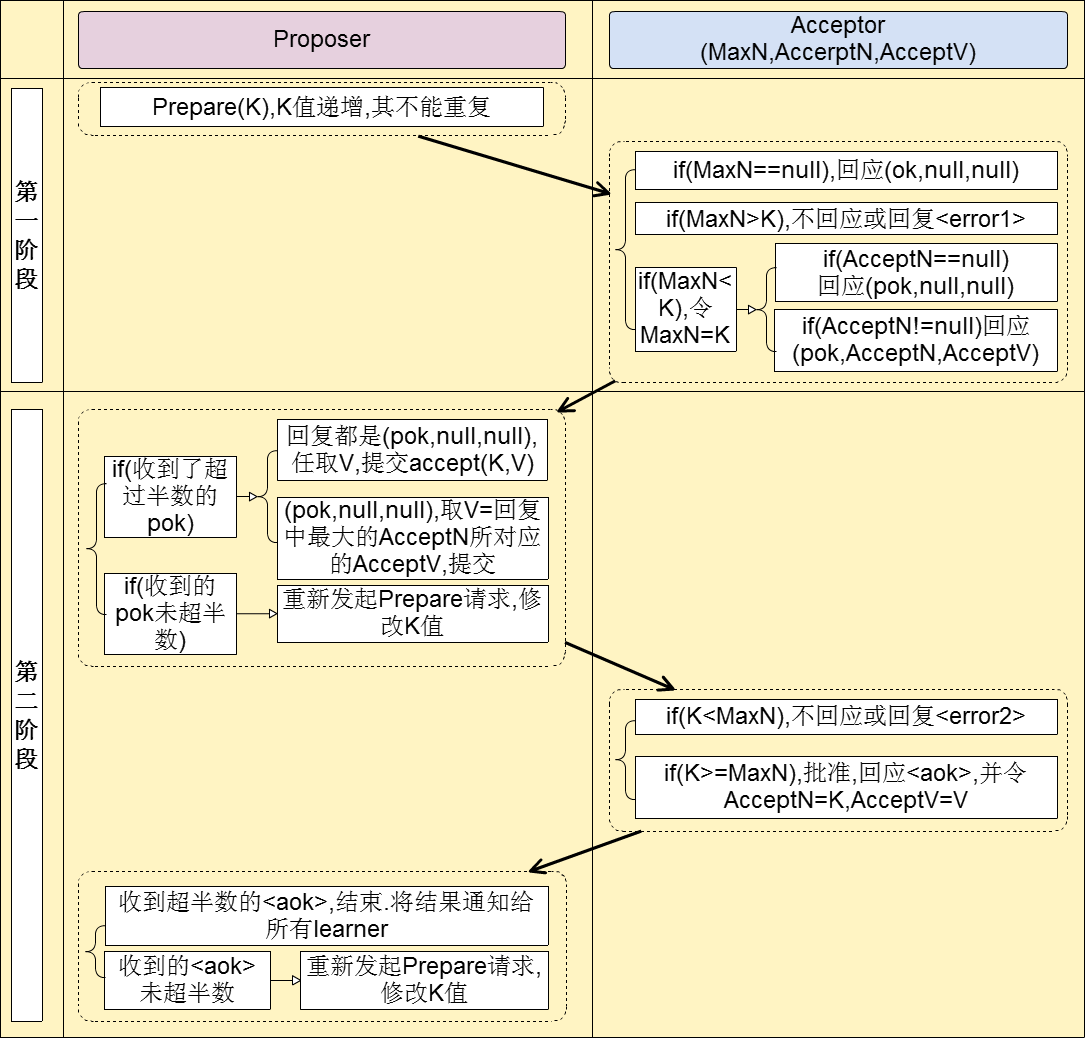
(a) A proposer selects a proposal number n and sends a prepare request with number n to a majority of acceptors.

(b) If an acceptor receives a prepare request with number n greater than that of any prepare request to which it has already responded, then it responds to the request with a promise not to accept any more proposals numbered less than n and with the highest-numbered pro-posal (if any) that it has accepted.

* Phase 2

(a) If the proposer receives a response to its prepare requests (numbered n) from a majority of acceptors, then it sends an accept request to each of those acceptors for a proposal numbered n with a value v , where v is the value of the highest-numbered proposal among the responses, or is any value if the responses reported no proposals.

(b) If an acceptor receives an accept request for a proposal numbered n, it accepts the proposal unless it has already responded to a prepare request having a number greater than n.



# Ethereum

* **Proof of Stake (PoS)**
  + [FAQ](https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ)
  + **a category of consensus algorithms for public blockchains that depend on a validator's economic stake in the network**
  + a set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its deposit (i.e. stake)
  + Process: anyone who holds the blockchain's base cryptocurrency can become a validator by sending a special type of transaction that locks up their ether into a deposit. The process of creating and agreeing to new blocks is then done through a consensus algorithm that all current validators can participate in.
  + two major types of consensus algorithms:
    - **chain-based proof of stake:** randomly selects a validator and assigns that validator the right to create a single block. this block must point to some previous block
      * 模型中有公认的“价值”，每个节点说话都需要一定代价，诚实节点会受到奖励，而恶意节点由于只付出代价而收不到奖励，变相受到了惩罚。由于给恶意节点的能力做了限制，恶意节点所能造成的破坏大大降低了**。**缺陷在于，得有个有价值的东西**，**最长链共识延迟问题
    - **BFT-style proof of stake:** validators are **randomly** assigned the right to propose blocks but agreeing on which block is canonical is done through a multi-round voting process
      * BFT算法没法应用于大量节点
  + **Benefits: Consume less energy, not as much need to issue as many new coins, discourage centralized cartels, Reduced centralization risks, make various forms of 51% attacks vastly more expensive**