MIDDLEWARE SYSTEMS
RESEARCH GROUP
MSRG.ORG

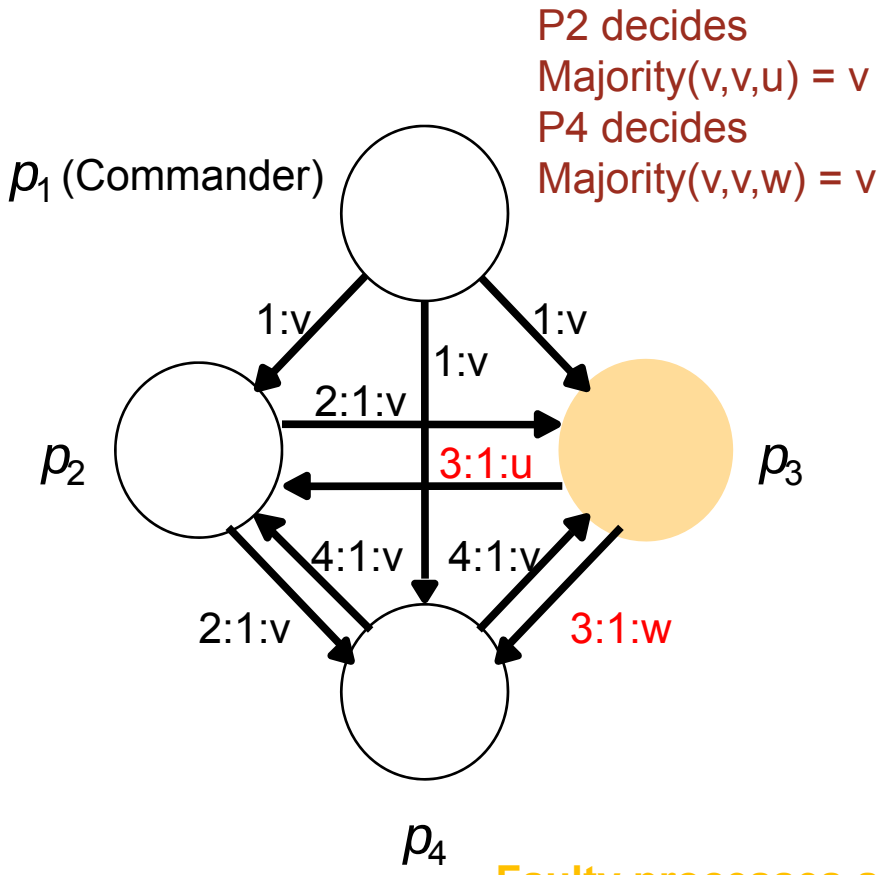
Deconstructing Blockchains: Concepts, Systems and Applications

BACKGROUND: BYZANTINE GENERALS PROBLEM

Origin: Byzantine Generals

- Devised by Lamport, 1982; a model and thought experiment
- A *distinguished process* (the ***commander***) proposes initial value (e.g., "attack", "retreat")
- Other processes, the ***lieutenants***, *communicate the commander's value*
- *Malicious processes* can lie about the value (i.e., *are faulty*)
- *Correct processes* report the truth (i.e., are *correct*)
- Commander or lieutenants may be faulty
- **Consensus** means
  - If the commander is correct, then correct processes should agree on commander's proposed value
  - If the commander is faulty, then all correct processes agree on a value *(any value, could be the faulty commander's value!)*

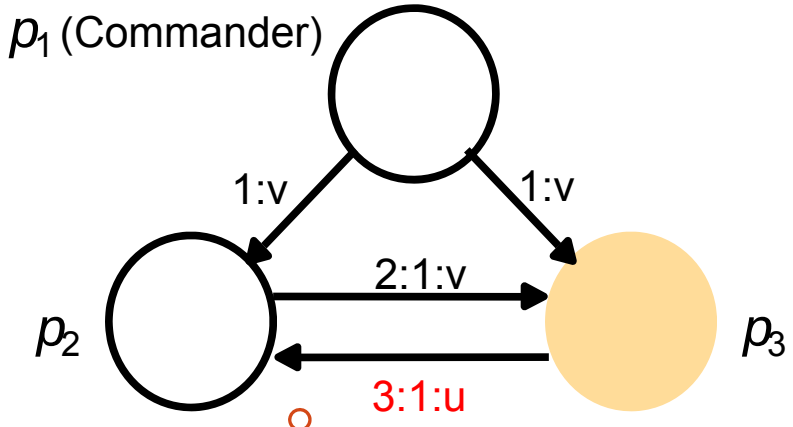
3f+1 Condition (1 failure, 4 nodes)

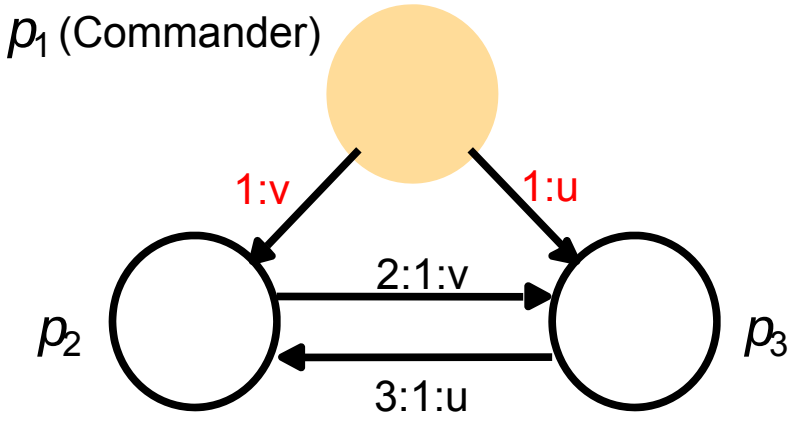


Faulty processes are shown coloured

Source: Tanenbaum, Steen.

Counter-Example
(1 failure, 3 nodes)

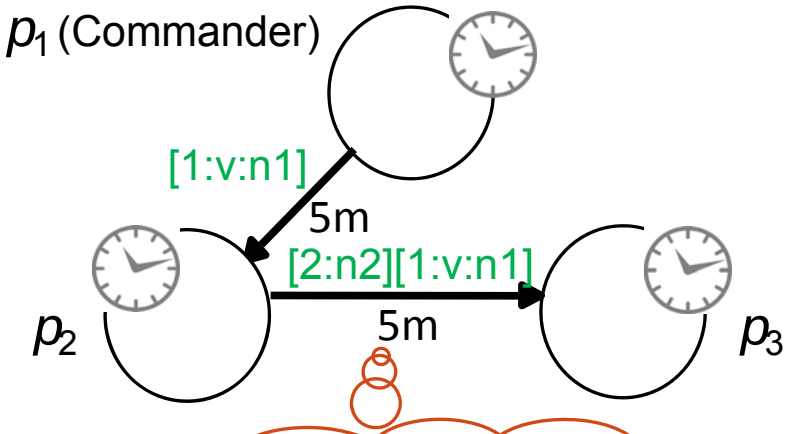




Faulty processes are shown coloured

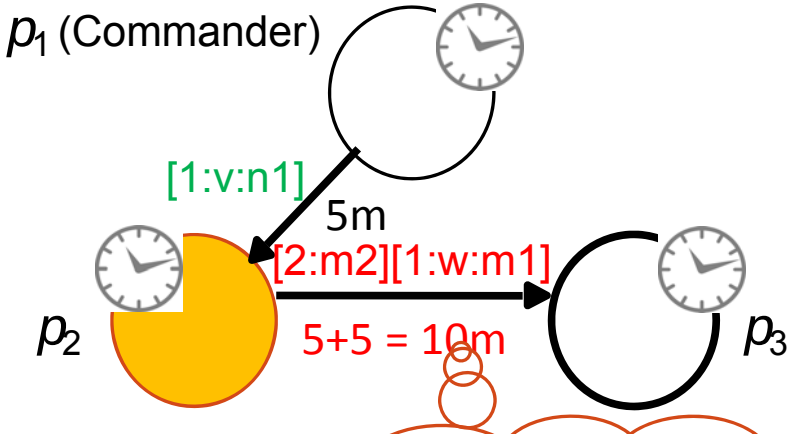
Trust commander or p3?
Can't tell the difference
between both situations!

With Blockchains
(Proof-of-Work – Thought Experiment)



P3 verifies each block and receives them in time.

Idea #1:
Each message takes exactly 5 minutes to create by any process. (“*Magic Block*”)



P2 tries to forge P1’s block and writes its own block, but it

Idea #2:
Each process can accurately measure the amount of time taken by a process to create a message. (“*Magic Watch*”)

Consensus in the Bitcoin Blockchain

The peers need to agree on

- Which recently broadcast transactions go into the blockchain
- In what order they go into a block

The general anatomy of consensus:

Tough problem

- Dozens of **impossibility results** since 1983
- **Does not scale** beyond ~30-100 participants
- Takes long time to converge