NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 32: Safety and Liveness of PBFT

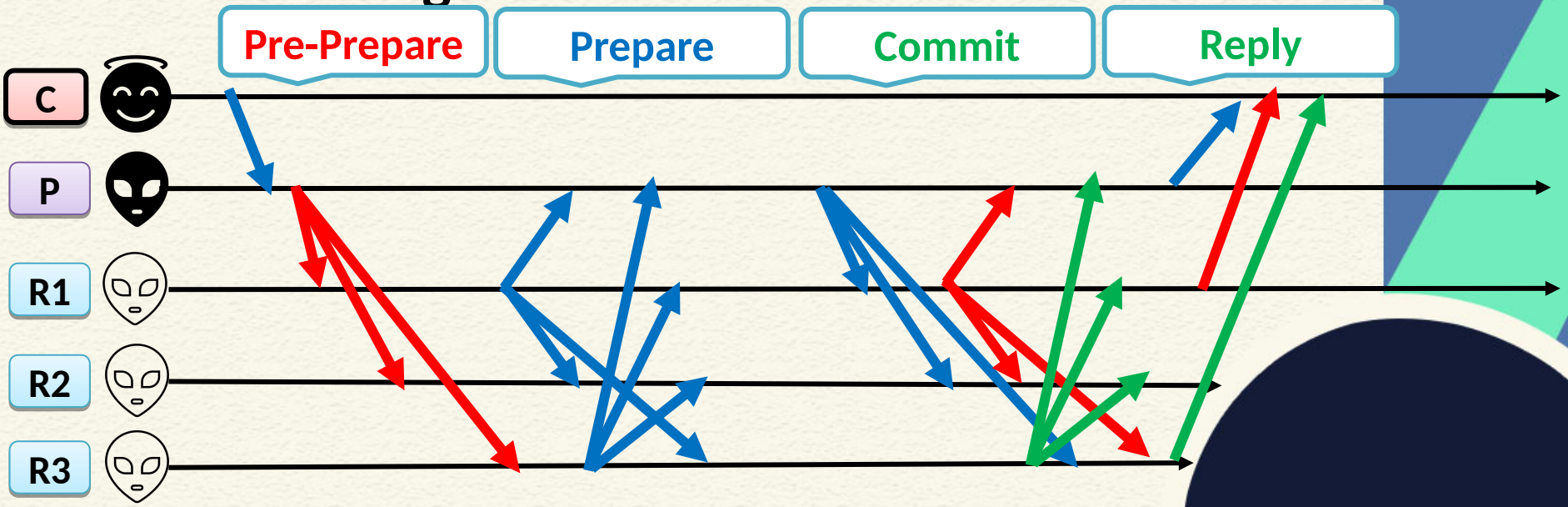
CONCEPTS COVERED

- Safety and Liveness of PBFT
- PBFT View Change

KEYWORDS

- Weak Synchrony assumptions
- The view change protocol

PBFT – The Algorithm



Safety in PBFT

- Unlike multiple Paxos proposers, **PBFT works with a single Primary**
  - Ping-pong does not arise from the proposals from multiple replicas
  - However, a replica needs to wait for ***2f + 1*** votes (Prepare and Commit messages)

Safety in PBFT

- PBFT is safe with **2f+1** quorum
  - The leader can always have the majority votes to support its proposal

- The leader can reach to the consensus even when it does not receive messages from some of the replicas due to asynchronous nature of the channel

Liveness in PBFT

- However, a primary may fail – the liveness gets hampered as the protocol cannot progress any further
  - Primary failure cannot be handled in a pure asynchronous system – you do not know whether it is a message delay from the primary, or a primary failure

Weak Synchrony Assumption

- **Weak Synchrony:**
  - (1) Both sender and the receiver is correct,
  - (2) Sender keeps retransmitting the messages until it is received,
  - (3) There is an **asymptotic upper bound** on the message transmission delay

The View Change Protocol

- What if the **primary** is **faulty** ?
  - Non-faulty replicas detect the fault
  - Replicas together start view change operation

- View-change protocol provides **eventual liveness** -- Allows the system to make progress when primary fails

The View Change Protocol

- If the primary fails, backups will not receive any message or will receive faulty messages from the primary

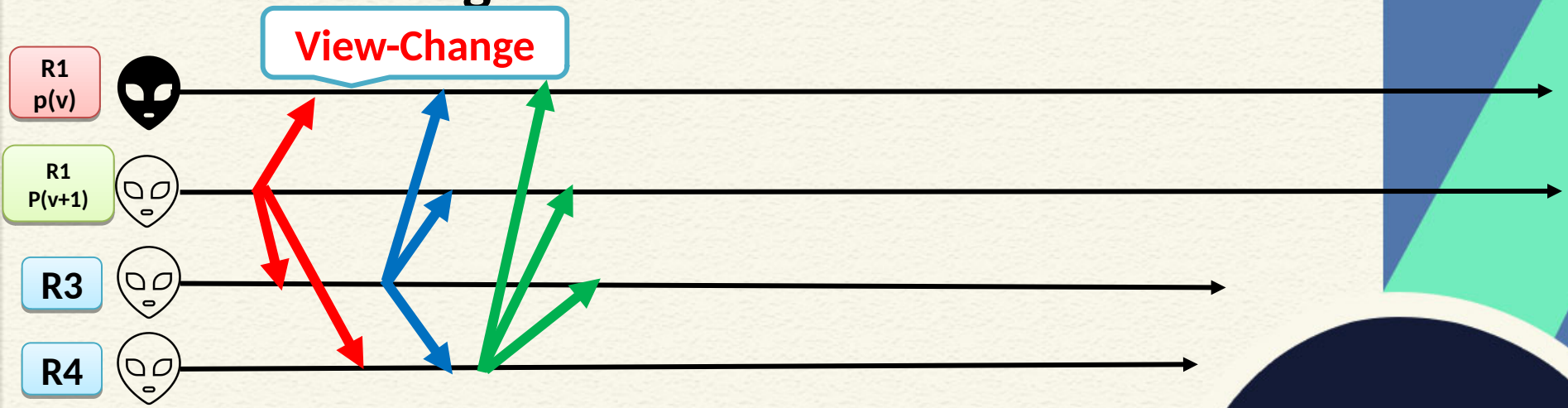
- View changes are triggered by timeouts (weak synchrony assumption)
  - Prevent backups from waiting indefinitely for requests to execute

The View Change Protocol

- Backup starts a timer when it receives a request, and the timer is not already running
  - The timer is stopped when the request is executed
  - Restarts when some new request comes

- If the timer expires at view *v*, backup starts a **View Change** to move to the view *v + 1*

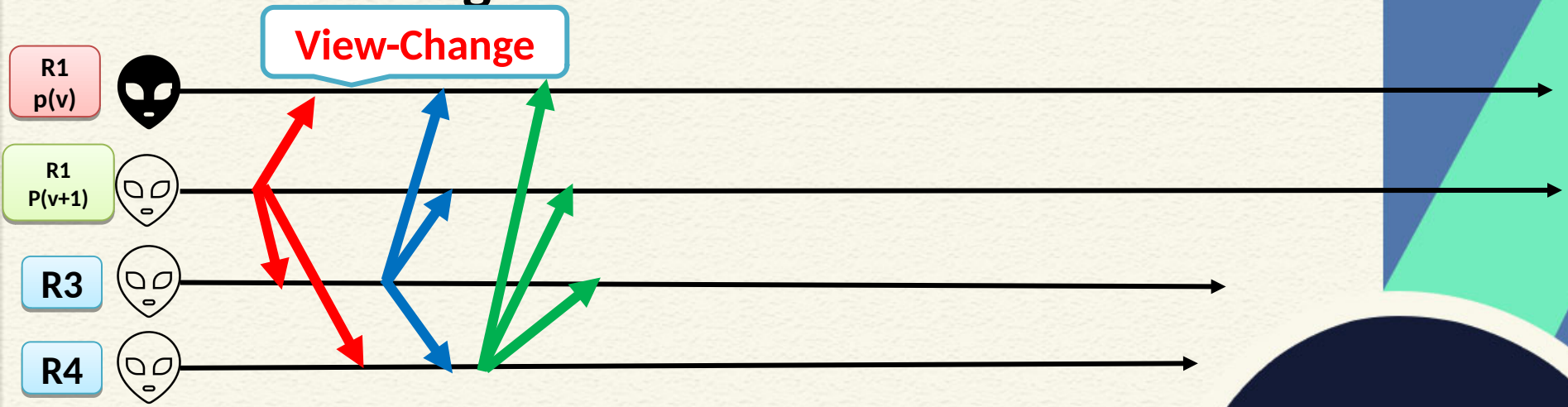
The View Change Protocol



Multicast the View Change message <VIEW-CHANGE, *v+1*, *n*, *C*, *P*, *k*>β_k

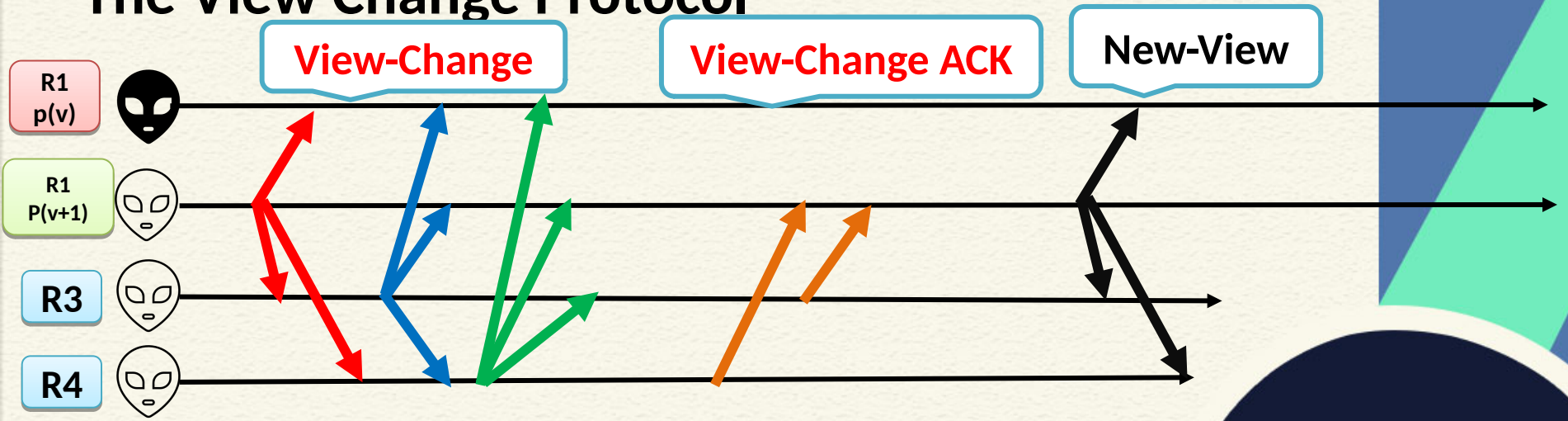
- *n* is the sequence number of last stable checkpoint *s* known to *k*
- *C* is a set of *2f + 1* valid checkpoint messages corresponding to *s*
- *P* is a set containing a set *Pm* for each request *m* that prepared at *k* with a sequence number higher than *n*

The View Change Protocol



- The new view is initiated after receiving *2f + 1* View Change messages
- Next primary selection
  - Round Robin (Hyperledger Sawtooth)
  - Leader election (Hyperledger Fabric)

The View Change Protocol



- Replicas send a View Change ACK – quorum is formed on these messages
- New View message to initiate a new view

Conclusion

- PBFT is safe under 2f+1 quorum over an asynchronous environment
- Liveness if affected when the primary is faulty
- View change to elect a new primary when the primary is detected as faulty
  - Weak synchrony assumption


Thank
you