```
──────────────────── MODULE ThreePhaseCommit ────────────────────
  Based on the TLA+ video course + in-class notes for three phase commit
CONSTANT SERVERS

VARIABLES
    coordState,
    servState,
    servReady,          in eyes of coordinator
    servPrecommit,      in eyes of coordinator
    msgs

Messages ≜ [type : {"ready", "precommit", "commit"}, server : SERVERS]
            ∪ [type : {"Ready", "Precommit", "Commit", "Abort"}]

TypeOK ≜
    ∧   servState ∈ [SERVERS → {"idle", "ready", "precommitted", "committed", "aborted"}]
    ∧   coordState ∈ {"init", "waitingR", "waitingP", "done"}
    ∧   servReady ⊆ SERVERS
    ∧   msgs ⊆ Messages

Init ≜
    ∧ servState = [s ∈ SERVERS ↦ "idle"]
    ∧ coordState = "init"
    ∧ servReady = {}
    ∧ servPrecommit = {}
    ∧ msgs = {}

─────────────────────────────────────────────────────────────────
  Define all of the actions that can be performed

  COORDINATOR ACTIONS
  Coordinator asks for ready responses
CoordReady ≜
    ∧ coordState = "init"
    ∧ coordState′ = "waitingR"
    ∧ servReady = {}
    ∧ servPrecommit = {}
    ∧ msgs′ = msgs ∪ {[type ↦ "Ready"]}
    ∧ UNCHANGED ⟨servState, servReady, servPrecommit⟩

  Coordinator receives ready message from server
CoordRecReady(s) ≜
    ∧ coordState = "waitingR"
    ∧ [type ↦ "ready", server ↦ s] ∈ msgs
    ∧ servReady′ = servReady ∪ {s}
    ∧ UNCHANGED ⟨coordState, servState, servPrecommit, msgs⟩
```

Coordinator broadcasts *precommit* message

$$
\begin{aligned}
&\mathit{CoordPrecommit} \triangleq \\
&\quad \land \mathit{coordState} = \text{“waitingR”} \\
&\quad \land \mathit{coordState}' = \text{“waitingP”} \\
&\quad \land \mathit{servReady} = \mathit{SERVERS} \\
&\quad \land \mathit{servPrecommit} = \{\} \\
&\quad \land \mathit{msgs}' = \mathit{msgs} \cup \{[\mathit{type} \mapsto \text{“Precommit”}]\} \\
&\quad \land \textsc{unchanged}\ \langle \mathit{servState}, \mathit{servReady}, \mathit{servPrecommit} \rangle
\end{aligned}
$$

Coordinator receives *precommit* message from server

$$
\begin{aligned}
&\mathit{CoordRecPrecommit}(s) \triangleq \\
&\quad \land \mathit{coordState} = \text{“waitingP”} \\
&\quad \land [\mathit{type} \mapsto \text{“precommit”}, \mathit{server} \mapsto s] \in \mathit{msgs} \\
&\quad \land \mathit{servPrecommit}' = \mathit{servPrecommit} \cup \{s\} \\
&\quad \land \textsc{unchanged}\ \langle \mathit{coordState}, \mathit{servState}, \mathit{servReady}, \mathit{msgs} \rangle
\end{aligned}
$$

Coordinator broadcasts commit message

$$
\begin{aligned}
&\mathit{CoordCommit} \triangleq \\
&\quad \land \mathit{coordState} = \text{“waitingP”} \\
&\quad \land \mathit{coordState}' = \text{“done”} \\
&\quad \land \mathit{servPrecommit} = \mathit{SERVERS} \\
&\quad \land \mathit{msgs}' = \mathit{msgs} \cup \{[\mathit{type} \mapsto \text{“Commit”}]\} \\
&\quad \land \textsc{unchanged}\ \langle \mathit{servState}, \mathit{servReady}, \mathit{servPrecommit} \rangle
\end{aligned}
$$

Coordinator broadcasts abort message

$$
\begin{aligned}
&\mathit{CoordAbort} \triangleq \\
&\quad \land \mathit{coordState} \in \{\text{“init”}, \text{“waitingR”}, \text{“waitingP”}\} \\
&\quad \land \mathit{coordState}' = \text{“done”} \\
&\quad \land \mathit{msgs}' = \mathit{msgs} \cup \{[\mathit{type} \mapsto \text{“Abort”}]\} \\
&\quad \land \textsc{unchanged}\ \langle \mathit{servState}, \mathit{servReady}, \mathit{servPrecommit} \rangle
\end{aligned}
$$

SERVER ACTIONS

Server receives + sends ready message

$$
\begin{aligned}
&\mathit{ServReady}(s) \triangleq \\
&\quad \land \mathit{servState}[s] = \text{“idle”} \\
&\quad \land \mathit{servState}' = [\mathit{servState}\ \textsc{except}\ ![s] = \text{“ready”}] \\
&\quad \land [\mathit{type} \mapsto \text{“Ready”}] \in \mathit{msgs} \\
&\quad \land \mathit{msgs}' = \mathit{msgs} \cup \{[\mathit{type} \mapsto \text{“ready”}, \mathit{server} \mapsto s]\} \\
&\quad \land \textsc{unchanged}\ \langle \mathit{coordState}, \mathit{servReady}, \mathit{servPrecommit} \rangle
\end{aligned}
$$

Server receives + sends *precommit* message

$$
\begin{aligned}
&\mathit{ServPrecommit}(s) \triangleq \\
&\quad \land \mathit{servState}[s] = \text{“ready”} \\
&\quad \land \mathit{servState}' = [\mathit{servState}\ \textsc{except}\ ![s] = \text{“precommitted”}] \\
&\quad \land [\mathit{type} \mapsto \text{“Precommit”}] \in \mathit{msgs} \\
&\quad \land \mathit{msgs}' = \mathit{msgs} \cup \{[\mathit{type} \mapsto \text{“precommit”}, \mathit{server} \mapsto s]\}
\end{aligned}
$$

$$\quad \land \text{UNCHANGED } \langle \mathit{coordState}, \mathit{servReady}, \mathit{servPrecommit} \rangle$$

Maybe separate these two ^^

Server receives commit message, commits

$$\begin{array}{l}
\mathit{ServRecCommit}(s) \triangleq \\
\quad \land \mathit{servState}[s] = \text{"precommitted"} \\
\quad \land [\mathit{type} \mapsto \text{"Commit"}] \in \mathit{msgs} \\
\quad \land \mathit{servState}' = [\mathit{servState} \text{ EXCEPT } ![s] = \text{"committed"}] \\
\quad \land \text{UNCHANGED } \langle \mathit{coordState}, \mathit{servReady}, \mathit{servPrecommit}, \mathit{msgs} \rangle
\end{array}$$

Server receives abort message, aborts

$$\begin{array}{l}
\mathit{ServRecAbort}(s) \triangleq \\
\quad \land [\mathit{type} \mapsto \text{"Abort"}] \in \mathit{msgs} \\
\quad \land \mathit{servState}' = [\mathit{servState} \text{ EXCEPT } ![s] = \text{"aborted"}] \\
\quad \land \text{UNCHANGED } \langle \mathit{coordState}, \mathit{servReady}, \mathit{servPrecommit}, \mathit{msgs} \rangle
\end{array}$$

MAKE SURE HANDLE CRASH AFTER *PRECOMMITTED*

Test with and without this

$$\begin{array}{l}
\mathit{ServCrash}(s) \triangleq \\
\quad \land \mathit{servState}[s] \in \{\text{"idle"}, \text{"ready"}, \text{"precommitted"}, \text{"committed"}\} \\
\quad \land \mathit{servState}' = [\mathit{servState} \text{ EXCEPT } ![s] = \text{"aborted"}] \\
\quad \land \text{UNCHANGED } \langle \mathit{coordState}, \mathit{servReady}, \mathit{servPrecommit}, \mathit{msgs} \rangle
\end{array}$$

$$\begin{array}{l}
\mathit{Next} \triangleq \\
\quad \lor \mathit{CoordReady} \lor \mathit{CoordPrecommit} \lor \mathit{CoordCommit} \lor \mathit{CoordAbort} \\
\quad \lor \exists\, s \in \mathit{SERVERS} : \\
\qquad \lor \mathit{CoordRecReady}(s) \lor \mathit{CoordRecPrecommit}(s) \\
\qquad \lor \mathit{ServReady}(s) \lor \mathit{ServPrecommit}(s) \lor \mathit{ServRecCommit}(s) \lor \mathit{ServRecAbort}(s) \;\; \lor \mathit{ServCrash}(s)
\end{array}$$

$$\begin{array}{l}
\mathit{Consistent} \triangleq \\
\quad \forall\, s1, s2 \in \mathit{SERVERS} : \neg \land \mathit{servState}[s1] = \text{"committed"} \\
\qquad\qquad\qquad\qquad\qquad\qquad\;\; \land \mathit{servState}[s2] = \text{"aborted"}
\end{array}$$

$$\mathit{Spec} \triangleq \mathit{Init} \land \quad \Box[\mathit{Next}]_{\langle \mathit{coordState}, \mathit{servState}, \mathit{servReady}, \mathit{servPrecommit}, \mathit{msgs} \rangle}$$

$$\text{THEOREM } \mathit{Spec} \Rightarrow \Box(\mathit{TypeOK} \land \mathit{Consistent})$$