MODULE $U2PC$

EXTENDS $FiniteSets$, $Integers$, $Apalache$, TLC

@$typeAlias$: $key = Str$;
@$typeAlias$: rid $= Str$;
@$typeAlias$: $tid = Str$;
@$typeAlias$: $version =$ \$$tid$;
@$typeAlias$: $txn = Set($\$$key)$;
@$typeAlias$: $txnstate =$ \$$key \to$ \$version;
$U2PC\_ALIAS \triangleq$ TRUE

CONSTANTS
@type: \$$key \to Set($\$$rid)$;
$Shards$,
@type: \$$tid \to$ \$$txn$;
$Txns$

ASSUME $\forall k1, k2 \in$ DOMAIN $Shards : k1 \neq k2 \Rightarrow Shards[k1] \cap Shards[k2] = \{\}$
ASSUME "Init" $\notin$ DOMAIN $Txns$

$msg\_read = Str$;
$msg\_read\_resp = \{key :$ \$$key, ver :$ \$$version\}$;
$msg\_lock = \{txn :$ \$$txn, key :$ \$$key, ver :$ \$$version\}$;
$msg\_lock\_resp = Bool$;
$msg\_unlock = Bool$;
$msg\_unlock\_resp = Bool$;

VARIABLES
@type: \$rid $\to \{locked : Bool, version :$ \$$version, logged :$ \$$version\}$;
$Replicas$,
@type: \$$tid \to Str$;
$Coordinator\_state$,
@type: \$$tid \to$ \$txnstate;
$Coordinator\_txn\_state$,
@type: $Set(\{src :$ \$$tid, key :$ \$$key\})$;
M_read,
@type: $Set(\{src :$ \$$rid, dst :$ \$$tid, ver :$ \$$version\})$;
M_read_resp,
@type: $Set(\{tid :$ \$$tid, txn :$ \$$txn, state :$ \$$txnstate\})$;
M_lock,
@type: $Set(\{src :$ \$$rid, dst :$ \$$tid, locked : Bool\})$;
M_lock_resp,
@type: $Set(\{src :$ \$$tid, apply : Bool\})$;
M_unlock,
@type: $Set(\{src :$ \$$rid, tid :$ \$$tid\})$;
M_unlock_resp,

@type: $tid → Set($tid);
Linearisability_rt

$$Vars \triangleq \langle Replicas, Coordinator\_state, Coordinator\_txn\_state, M\_read, M\_read\_resp, M\_lock, M\_lock\_resp, M\_unlock, M\_unlock\_resp, Linearisability\_rt\rangle$$

$$Var\_M\_read \triangleq \langle M\_read, M\_read\_resp\rangle$$
$$Var\_M\_lock \triangleq \langle M\_lock, M\_lock\_resp\rangle$$
$$Var\_M\_unlock \triangleq \langle M\_unlock, M\_unlock\_resp\rangle$$

$$Var\_Msgs \triangleq \langle Var\_M\_read, Var\_M\_lock, Var\_M\_unlock\rangle$$

@type: (a → b) ⇒ Set(b);
$$Range(F) \triangleq \{F[x] : x \in \text{DOMAIN } F\}$$

@type: Set($rid);
$$RIDs \triangleq \text{UNION } Range(Shards)$$
$$TIDs \triangleq \text{DOMAIN } Txns$$

$$KeyLookup \triangleq [r \in RIDs \mapsto \text{CHOOSE } k \in \text{DOMAIN } Shards : r \in Shards[k]]$$

$$Init \triangleq$$
$$\wedge\ Replicas = [r \in RIDs \mapsto [locked \mapsto \text{FALSE}, version \mapsto \text{"Init"}, logged \mapsto \text{"NULL"}]]$$
$$\wedge\ Coordinator\_state = [t \in TIDs \mapsto \text{"Start"}]$$
$$\wedge\ Coordinator\_txn\_state = [t \in TIDs \mapsto SetAsFun(\{\})]$$
$$\wedge\ M\_read = \{\} \wedge M\_read\_resp = \{\}$$
$$\wedge\ M\_lock = \{\} \wedge M\_lock\_resp = \{\}$$
$$\wedge\ M\_unlock = \{\} \wedge M\_unlock\_resp = \{\}$$
$$\wedge\ Linearisability\_rt = [t \in TIDs \mapsto \{\}]$$

$$RelevantReplicas(t) \triangleq \text{UNION } \{Shards[k] : k \in Txns[t]\}$$

$$CoordinatorStart(t) \triangleq$$
$$\wedge\ Coordinator\_state[t] = \text{"Start"}$$
$$\wedge\ M\_read' = M\_read \cup \{[src \mapsto t, key \mapsto k] : k \in Txns[t]\}$$
$$\wedge\ \text{UNCHANGED } \langle M\_read\_resp, Var\_M\_lock, Var\_M\_unlock\rangle$$
$$\wedge\ Coordinator\_state' = [Coordinator\_state \text{ EXCEPT } ![t] = \text{"Read"}]$$
$$\wedge\ \text{UNCHANGED } \langle Coordinator\_txn\_state, Replicas\rangle$$
$$\wedge\ Linearisability\_rt' = [Linearisability\_rt \text{ EXCEPT } ![t] = \{t1 \in TIDs : Coordinator\_state[t1] = \text{"Commit"}\}]$$

$$ReplicaRead(r) \triangleq$$
$$\wedge\ Replicas[r].locked = \text{FALSE}$$

$\land \exists\, m \in M\_read :$
$\quad \land \neg\exists\, m1 \in M\_read\_resp : m1.src = r \land m1.dst = m.src$
$\quad \land M\_read\_resp' = M\_read\_resp \cup$
$\qquad \{[src \mapsto r,\ dst \mapsto m.src,\ ver \mapsto Replicas[r].version]\}$
$\quad \land$ UNCHANGED $\langle M\_read,\ Var\_M\_lock,\ Var\_M\_unlock\rangle$
$\land$ UNCHANGED $\langle Replicas\rangle$
$\land$ UNCHANGED $\langle Coordinator\_state,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

$CoordinatorRead(t) \triangleq$
$\land\ Coordinator\_state[t] =$ "Read"
$\land \forall\, k \in Txns[t] : \exists\, m \in M\_read\_resp : KeyLookup[m.src] = k$
$\land \exists\, F \in [Txns[t] \to RIDs] :$
$\quad \land \forall\, k \in Txns[t] : \land k = KeyLookup[F[k]]$
$\qquad\qquad\qquad\qquad \land \exists\, m \in M\_read\_resp : m.dst = t \land m.src = F[k]$
$\quad \land Coordinator\_txn\_state' = [Coordinator\_txn\_state$ EXCEPT $![t] = [$
$\qquad k \in Txns[t] \mapsto$
$\qquad\ (\text{CHOOSE}\ m \in M\_read\_resp : m.dst = t \land m.src = F[k]).ver$
$\qquad]]$
$\land\ Coordinator\_state' = [Coordinator\_state$ EXCEPT $![t] =$ "Lock"$]$
$\land$ UNCHANGED $\langle Replicas,\ Var\_Msgs,\ Linearisability\_rt\rangle$

$CoordinatorLock(t) \triangleq$
$\land\ Coordinator\_state[t] =$ "Lock"
$\land\ M\_lock' = M\_lock \cup$
$\quad \{[tid \mapsto t,\ txn \mapsto Txns[t],\ state \mapsto Coordinator\_txn\_state[t]]\}$
$\land$ UNCHANGED $\langle M\_lock\_resp,\ Var\_M\_read,\ Var\_M\_unlock\rangle$
$\land\ Coordinator\_state' = [Coordinator\_state$ EXCEPT $![t] =$ "Decide"$]$
$\land$ UNCHANGED $\langle Coordinator\_txn\_state,\ Replicas,\ Linearisability\_rt\rangle$

$ReplicaLock(r) \triangleq$
$\land \exists\, m \in M\_lock :$
$\quad \land\ KeyLookup[r] \in m.txn$
$\quad \land \neg\exists\, m1 \in M\_lock\_resp : m1.src = r \land m1.dst = m.tid$
$\quad \land$ IF $(\neg Replicas[r].locked) \land Replicas[r].version = m.state[KeyLookup[r]]$
$\qquad$ THEN
$\qquad\quad \land\ Replicas' = [Replicas$ EXCEPT $![r] = [$
$\qquad\qquad\ locked \mapsto$ TRUE, $version \mapsto Replicas[r].version,\ logged \mapsto m.tid]]$
$\qquad\quad \land\ M\_lock\_resp' = M\_lock\_resp \cup$
$\qquad\qquad\ \{[src \mapsto r,\ dst \mapsto m.tid,\ locked \mapsto$ TRUE$]\}$
$\qquad$ ELSE
$\qquad\quad \land\ M\_lock\_resp' = M\_lock\_resp \cup$
$\qquad\qquad\ \{[src \mapsto r,\ dst \mapsto m.tid,\ locked \mapsto$ FALSE$]\}$
$\qquad\quad \land$ UNCHANGED $Replicas$
$\land$ UNCHANGED $\langle M\_lock,\ Var\_M\_read,\ Var\_M\_unlock\rangle$
$\land$ UNCHANGED $\langle Coordinator\_state,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

$CoordinatorCommit(t) \triangleq$
$\land\ Coordinator\_state[t] = \text{“Decide”}$
$\land\ \forall\, k \in Txns[t] : \forall\, r \in Shards[k] : \exists\, m \in M\_lock\_resp :$
$\quad \land\ m.src = r \land m.dst = t$
$\quad \land\ m.locked$
$\land\ Coordinator\_state' = [Coordinator\_state \text{ EXCEPT } ![t] = \text{“Commit”}]$
$\land\ M\_unlock' = M\_unlock \cup \{[src \mapsto t,\ apply \mapsto \text{TRUE}]\}$
$\land\ \text{UNCHANGED } \langle Var\_M\_read,\ Var\_M\_lock,\ M\_unlock\_resp\rangle$
$\land\ \text{UNCHANGED } \langle Replicas,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

$CoordinatorStartAbort(t) \triangleq$
$\land\ Coordinator\_state[t] = \text{“Decide”}$
$\land\ \exists\, k \in Txns[t] : \exists\, r \in Shards[k] : \exists\, m \in M\_lock\_resp :$
$\quad \land\ m.src = r \land m.dst = t$
$\quad \land\ \neg m.locked$
$\land\ Coordinator\_state' = [Coordinator\_state \text{ EXCEPT } ![t] = \text{“TryAbort”}]$
$\land\ M\_unlock' = M\_unlock \cup \{[src \mapsto t,\ apply \mapsto \text{FALSE}]\}$
$\land\ \text{UNCHANGED } \langle Var\_M\_read,\ Var\_M\_lock,\ M\_unlock\_resp\rangle$
$\land\ \text{UNCHANGED } \langle Replicas,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

$ReplicaUnlock(r) \triangleq$
$\exists\, m \in M\_unlock :$
$\land\ Replicas[r].locked$
$\land\ m.src = Replicas[r].logged$
$\land\ \text{IF } m.apply$
$\quad \text{THEN } Replicas' = [Replicas \text{ EXCEPT } ![r] = [$
$\qquad locked \mapsto \text{FALSE},\ version \mapsto Replicas[r].logged,\ logged \mapsto \text{“NULL”}]]$
$\quad \text{ELSE } Replicas' = [Replicas \text{ EXCEPT } ![r] = [$
$\qquad locked \mapsto \text{FALSE},\ version \mapsto Replicas[r].version,\ logged \mapsto \text{“NULL”}]]$
$\land\ M\_unlock\_resp' = M\_unlock\_resp \cup \{[src \mapsto r,\ tid \mapsto Replicas[r].logged]\}$
$\land\ \text{UNCHANGED } \langle Var\_M\_read,\ Var\_M\_lock,\ M\_unlock\rangle$
$\land\ \text{UNCHANGED } \langle Coordinator\_state,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

$CoordinatorAbort(t) \triangleq$
$\land\ Coordinator\_state[t] = \text{“TryAbort”}$
$\land\ \exists\, k \in Txns[t] : \forall\, r \in Shards[k] :$
$\quad \lor\ \exists\, m \in M\_unlock\_resp : m.src = r \land m.tid = t$
$\quad \lor\ \exists\, m \in M\_lock\_resp : m.src = r \land m.dst = t \land \neg m.locked$
$\land\ Coordinator\_state' = [Coordinator\_state \text{ EXCEPT } ![t] = \text{“Abort”}]$
$\land\ \text{UNCHANGED } \langle Replicas,\ Var\_Msgs,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

$Next \triangleq$
$\lor\ \exists\, r \in RIDs :\ \lor\ ReplicaRead(r)$
$\qquad\qquad\qquad\qquad\ \lor\ ReplicaLock(r)$
$\qquad\qquad\qquad\qquad\ \lor\ ReplicaUnlock(r)$

$$
\begin{array}{l}
\lor\ \exists\, t \in \mathit{TIDs} :\ \lor\ \mathit{CoordinatorStart}(t) \\
\qquad\qquad\qquad\qquad\ \lor\ \mathit{CoordinatorRead}(t) \\
\qquad\qquad\qquad\qquad\ \lor\ \mathit{CoordinatorLock}(t) \\
\qquad\qquad\qquad\qquad\ \lor\ \mathit{CoordinatorCommit}(t) \\
\qquad\qquad\qquad\qquad\ \lor\ \mathit{CoordinatorStartAbort}(t) \\
\qquad\qquad\qquad\qquad\ \lor\ \mathit{CoordinatorAbort}(t)
\end{array}
$$

$$\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\mathit{Vars}}$$

$$
\begin{array}{l}
\mathit{Serialisability}(C) \triangleq \\
\quad \lor\ \mathit{Cardinality}(C) < 2 \\
\quad \lor\ \exists\, R \in \text{SUBSET}\ (C \times C) : \\
\qquad \text{Irreflexive} \\
\qquad \land\ \forall\, t1 \in C : \langle t1,\ t1 \rangle \notin R \\
\qquad \text{Transitive} \\
\qquad \land\ \forall\, t1,\ t2,\ t3 \in C : (\langle t1,\ t2 \rangle \in R \land \langle t2,\ t3 \rangle \in R) \Rightarrow \langle t1,\ t3 \rangle \in R \\
\qquad \text{Above 2 ensure there are no cycles} \\
\qquad R \text{ respects observed order} \\
\qquad \land\ \forall\, t1,\ t2 \in C : \\
\qquad\quad (\exists\, k \in \mathit{Txns}[t2] : \mathit{Coordinator\_txn\_state}[t2][k] = t1) \Rightarrow \langle t1,\ t2 \rangle \in R \\
\qquad \text{If two transactions interfere, there is an order} \\
\qquad \land\ \forall\, t1,\ t2 \in C : \\
\qquad\quad (t1 \neq t2 \land \mathit{Txns}[t1] \cap \mathit{Txns}[t2] \neq \{\}) \Rightarrow \langle t1,\ t2 \rangle \in R \lor \langle t2,\ t1 \rangle \in R \\
\qquad \text{Strict serialisability / } \textit{Linearisability} \text{ check} \\
\qquad \land\ \forall\, t1,\ t2 \in C : \\
\qquad\quad (t1 \in \mathit{Linearisability\_rt}[t2]) \Rightarrow \langle t1,\ t2 \rangle \in R
\end{array}
$$

$$
\begin{array}{l}
\mathit{CommittedTIDs} \triangleq \{t \in \mathit{TIDs} : \mathit{Coordinator\_state}[t] = \text{“Commit”}\} \\
\mathit{AbortedTIDs} \triangleq \{t \in \mathit{TIDs} : \mathit{Coordinator\_state}[t] = \text{“Abort”}\}
\end{array}
$$

$$\mathit{Safety\_non\_recovery} \triangleq \mathit{Serialisability}(\mathit{CommittedTIDs})$$