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

$Msgs \triangleq \langle M\_read, M\_read\_resp, M\_lock, M\_lock\_resp, M\_unlock, M\_unlock\_resp \rangle$

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

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

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

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

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

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

$ReplicaRead(r) \triangleq$
$\land\ Replicas[r].locked = \text{FALSE}$
$\land\ \exists\, m \in M\_read :$
$\quad \land\ \neg \exists\, m1 \in M\_read\_resp : m1.src = r \land m1.dst = m.src$
$\quad \land\ M\_read\_resp' = M\_read\_resp \cup \{[src \mapsto r, dst \mapsto m.src, ver \mapsto Replicas[r].version]\}$
$\quad \land\ \text{UNCHANGED } \langle M\_read, M\_lock, M\_lock\_resp, M\_unlock, M\_unlock\_resp \rangle$
$\land\ \text{UNCHANGED } \langle Replicas, Coordinator\_state, Coordinator\_txn\_state, Linearisability\_rt \rangle$

$CoordinatorRead(t) \triangleq$
$\land\ Coordinator\_state[t] = \text{"Read"}$
$\land\ \forall\, k \in Txns[t] : \exists\, m \in M\_read\_resp : KeyLookup[m.src] = k$
$\land\ \exists\, F \in [Txns[t] \to RIDs] :$
$\quad \land\ \forall\, k \in Txns[t] : \land\ k = KeyLookup[F[k]]$
$\qquad\qquad\qquad\qquad\ \land\ \exists\, m \in M\_read\_resp : m.dst = t \land m.src = F[k]$

$\land$ $Coordinator\_txn\_state' = [Coordinator\_txn\_state$ EXCEPT $![t] = [$
$k \in Txns[t] \mapsto ($CHOOSE $m \in M\_read\_resp : m.dst = t \land m.src = F[k]).ver$
$]]$
$\land$ $Coordinator\_state' = [Coordinator\_state$ EXCEPT $![t] =$ "Lock"$]$
$\land$ UNCHANGED $\langle Replicas, Msgs, Linearisability\_rt\rangle$

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

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

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

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

$\land$ UNCHANGED $\langle Replicas,\ Coordinator\_txn\_state,\ Linearisability\_rt\rangle$

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

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

$Next \triangleq$
$\lor \exists\, r \in RIDs :\ \lor ReplicaRead(r)$
$\lor ReplicaLock(r)$
$\lor ReplicaUnlock(r)$
$\lor \exists\, t \in TIDs :\ \lor CoordinatorStart(t)$
$\lor CoordinatorRead(t)$
$\lor CoordinatorLock(t)$
$\lor CoordinatorCommit(t)$
$\lor CoordinatorStartAbort(t)$
$\lor CoordinatorAbort(t)$

$Spec \triangleq Init \land \Box[Next]_{\langle Replicas,\ Coordinator\_state,\ Coordinator\_txn\_state,\ Msgs,\ Linearisability\_rt\rangle}$

$Serialisability(C) \triangleq$
$\lor\ Cardinality(C) < 2$
$\lor \exists\, R \in$ SUBSET $(C \times C) :$
Irreflexive
$\land \forall\, t1 \in C : \langle t1,\ t1\rangle \notin R$
Transitive
$\land \forall\, t1,\ t2,\ t3 \in C : (\langle t1,\ t2\rangle \in R \land \langle t2,\ t3\rangle \in R) \Rightarrow \langle t1,\ t3\rangle \in R$
Above 2 ensure there are no cycles
R respects observed order
$\land \forall\, t1,\ t2 \in C :$

$(\exists\, k \in Txns[t2] : Coordinator\_txn\_state[t2][k] = t1) \Rightarrow \langle t1,\, t2\rangle \in R$

If two transactions interfere, there is an order

$\wedge\, \forall\, t1,\, t2 \in C :$

$(t1 \neq t2 \wedge Txns[t1] \cap Txns[t2] \neq \{\}) \Rightarrow \langle t1,\, t2\rangle \in R \vee \langle t2,\, t1\rangle \in R$

Strict serialisability / *Linearisability* check

$\wedge\, \forall\, t1,\, t2 \in C :$

$(t1 \in Linearisability\_rt[t2]) \Rightarrow \langle t1,\, t2\rangle \in R$

$CommittedTIDs \triangleq \{t \in TIDs : Coordinator\_state[t] = \text{“Commit”}\}$

$AbortedTIDs \triangleq \{t \in TIDs : Coordinator\_state[t] = \text{“Abort”}\}$

$Safety\_non\_recovery \triangleq Serialisability(CommittedTIDs)$