MODULE $U2PC\_MC$

EXTENDS $Apalache$, $U2PC$, TLC

@type: (a, b) $\Rightarrow \langle a, b \rangle$;
$Pair(A, B) \triangleq \langle A, B \rangle$

$T1 \triangleq SetAsFun(\{Pair(\text{“T1”}, \{\text{“X”}\})\})$
$T1\_2 \triangleq SetAsFun(\{Pair(\text{“T1”}, \{\text{“X”}\}), Pair(\text{“T2”}, \{\text{“X”}\})\})$
$S1 \triangleq SetAsFun(\{Pair(\text{“X”}, \{\text{“X1”}, \text{“X2”}\})\})$

$T3 \triangleq SetAsFun(\{Pair(\text{“T1”}, \{\text{“X”}, \text{“Y”}\}), Pair(\text{“T2”}, \{\text{“Y”}, \text{“Z”}\}), Pair(\text{“T3”}, \{\text{“Z”}, \text{“X”}\})\})$
$S3 \triangleq SetAsFun(\{Pair(\text{“X”}, \{\text{“X1”}, \text{“X2”}\}), Pair(\text{“Y”}, \{\text{“Y1”}, \text{“Y2”}\}), Pair(\text{“Z”}, \{\text{“Z1”}, \text{“Z2”}\})\})$

$CInit \triangleq$
  $\land\ Txns := T3$
  $\land\ Shards := S3$

$TransitiveClosure(R) \triangleq$
  LET $S \triangleq \{r[1] : r \in R\} \cup \{r[2] : r \in R\}$
      RECURSIVE $TCR(\_)$
      $TCR(T) \triangleq$ IF $T = \{\}$
                        THEN R
                        ELSE LET $r \triangleq$ CHOOSE $s \in T$: TRUE
                                 $RR \triangleq TCR(T \setminus \{r\})$
                             IN $RR \cup \{\langle s, t \rangle \in S \times S :$
                                  $\langle s, r \rangle \in RR \land \langle r, t \rangle \in RR\}$
  IN $TCR(S)$

$TransactionOrdering \triangleq$ LET
  $F(acc, tid) \triangleq acc \cup (Range(Coordinator\_txn\_state[tid]) \times \{tid\})$
  $Base \triangleq ApaFoldSet(F, \{\}, TIDs)$
  IN $TransitiveClosure(Base)$

$RecoveryCommitted(S) \triangleq$
  $\{t \in TIDs :$
    $\forall\, r \in S :$
    $KeyLookup[r] \in Txns[t]$
     $\Rightarrow \lor Replicas[r].locked \land Replicas[r].logged = t$
        $\lor Replicas[r].version = t$
        $\lor \langle t, Replicas[r].version \rangle \in TransactionOrdering$
  $\}$

$Safety\_recovery \triangleq$
  $\forall\, S \in$ SUBSET $RIDs :$
    Valid recovery
  $(\forall\, k \in$ DOMAIN $Shards : \exists\, r \in S : r \in Shards[k])$

$\Rightarrow$
IF $Serialisability(CommittedTIDs \cup RecoveryCommitted(S))$
THEN TRUE
ELSE $Print([rec \mapsto RecoveryCommitted(S),\ com \mapsto CommittedTIDs], \text{FALSE})$

$RecoveryAborted(S) \triangleq$
$\{t \in TIDs :$
$\exists\, r \in S :$
$\land\ KeyLookup[r] \in Txns[t]$
$\land\ \lor \neg Replicas[r].locked$
$\lor\ Replicas[r].locked \land Replicas[r].logged \neq t\}$

$Durability \triangleq$
$\forall\, S \in \text{SUBSET } RIDs :$
Valid recovery
$(\forall\, k \in \text{DOMAIN } Shards : \exists\, r \in S : r \in Shards[k])$
$\Rightarrow$
$\forall\, t \in TIDs :$
$\land\ t \in CommittedTIDs \Rightarrow t \in RecoveryCommitted(S)$
$\land\ t \in AbortedTIDs \Rightarrow t \in RecoveryAborted(S)$

$Invs \triangleq$
$\land\ Safety\_recovery$
$\land\ Durability$