```
MODULE TCS
See DISC'2018: Multi-Shot Distributed Transaction Commit
EXTENDS Naturals, Integers, FiniteSets, Sequences, Functions, TLC
```

CONSTANTS

- $Key$, the set of keys, ranged over by $k \in Key$
- $Tid$, the set of transaction identifiers, ranged over by $t \in Tid$
- $RSet$, $RSet[t]$: the read set of $t \in Tid$
- $WSet$, $WSet[t]$: the write set of $t \in Tid$
- $CVer$, $CVer[t]$: the commit version of $t \in Tid$
- $Shard$, the set of shards, ranged over by $s \in Shard$
- $Coord$, $Coord[t]$: the coordinator of $t \in Tid$
- $KeySharding$ $KeySharding[k]$: the shard that holds $k \in Key$

$$NotTid \triangleq \text{CHOOSE } t : t \notin Tid$$

$$Ver \triangleq 0 \,..\, Cardinality(Tid)$$ with a distinguished minimum version 0

$$Slot \triangleq 1 \,..\, Cardinality(Tid)$$

$$TKey(t) \triangleq WSet[t] \cup \{kv[1] : kv \in RSet[t]\}$$

$$TSharding \triangleq [t \in Tid \mapsto \{KeySharding[k] : k \in TKey(t)\}]$$

ASSUME

$$\land\ RSet \in [Tid \to \text{SUBSET } (Key \times Ver)]$$
$$\land\ \forall\, t \in Tid: RSet[t] \setminus * \ TODO\text{: one version per object}$$
$$\land\ WSet \in [Tid \to \text{SUBSET } Key]$$
$$\land\ \setminus * \ TODO\text{: "no blind update" assumption}$$
$$\land\ CVer \in [Tid \to Ver]$$
$$\land\ \setminus * \ TODO\text{: higher than any of the versions read}$$
$$\land\ Coord \in [Tid \to Shard]$$
$$\land\ KeySharding \in [Key \to Shard]$$

VARIABLES

- $next$, $next[s] \in Z$ points to the last filled slot
- $txn$, $txn[s][i]$ is the transaction (identifier) to certify in the $i$-th slot
- $vote$, $vote[s][i]$ is the vote for $txn[s][i]$
- $dec$, $dec[s][i]$ is the decision for $txn[s][i]$
- $phase$ $phase[s][i]$ is the phase for $txn[s][i]$

$$vars \triangleq \langle next, txn, vote, dec, phase \rangle$$

$$TypeOK \triangleq$$
$$\land\ next \in [Shard \to Int]$$
$$\land\ txn \in [Shard \to [Slot \to Tid \cup \{NotTid\}]]$$
$$\land\ vote \in [Shard \to [Slot \to \{\text{"COMMIT"}, \text{"ABORT"}, \text{"NULL"}\}]]$$
$$\land\ dec \in [Shard \to [Slot \to \{\text{"COMMIT"}, \text{"ABORT"}, \text{"NULL"}\}]]$$

```
49      ∧    phase ∈ [Shard → [Slot → {"START", "PREPARED", "DECIDED"}]]
50  ──────────────────────────────────────────────────────────────────────
51  Init ≜
52      ∧ next = [s ∈ Shard ↦ −1]
53      ∧ txn = [s ∈ Shard ↦ [i ∈ Slot ↦ NotTid]]
54      ∧ vote = [s ∈ Shard ↦ [i ∈ Slot ↦ "NULL"]]
55      ∧ dec = [s ∈ Shard ↦ [i ∈ Slot ↦ "NULL"]]
56      ∧ phase = [s ∈ Shard ↦ [i ∈ Slot ↦ "START"]]
57  ──────────────────────────────────────────────────────────────────────
58  Certify(t, s) ≜   Cerify t ∈ Tid on shard s ∈ Shard
59      ∧ FALSE
60  ──────────────────────────────────────────────────────────────────────
61  Next ≜ TRUE

63  Spec ≜ Init ∧ □[Next]_vars
64  ──────────────────────────────────────────────────────────────────────
    \* Modification History
    \* Last modified Sun Jun 13 10:22:37 CST 2021 by hengxin
    \* Created Sat Jun 12 21:01:57 CST 2021 by hengxin
```