MODULE *Config*

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

INSTANCE *TLC*

Nil $\triangleq$ "<nil>"

Change $\triangleq$ "Change"
Rollback $\triangleq$ "Rollback"

ReadCommitted $\triangleq$ "ReadCommitted"
Serializable $\triangleq$ "Serializable"

Initialize $\triangleq$ "Initialize"
Validate $\triangleq$ "Validate"
Abort $\triangleq$ "Abort"
Commit $\triangleq$ "Commit"
Apply $\triangleq$ "Apply"

InProgress $\triangleq$ "InProgress"
Complete $\triangleq$ "Complete"
Failed $\triangleq$ "Failed"

Pending $\triangleq$ "Pending"
Validated $\triangleq$ "Validated"
Committed $\triangleq$ "Committed"
Applied $\triangleq$ "Applied"
Aborted $\triangleq$ "Aborted"

Valid $\triangleq$ TRUE
Invalid $\triangleq$ FALSE

Success $\triangleq$ "Success"
Failure $\triangleq$ "Failure"

Node $\triangleq$ {"node-1"}

NumTransactions $\triangleq$ 3

Target $\triangleq$ [
  *target*1 $\mapsto$ [
    persistent $\mapsto$ FALSE,
    values $\mapsto$ [

$path1 \mapsto \{\text{“value1”}, \text{“value2”}\},$
$path2 \mapsto \{\text{“value2”}, \text{“value3”}\}]],$
$target2 \mapsto [$
$persistent \mapsto$ TRUE,
$values \mapsto [$
$path2 \mapsto \{\text{“value3”}, \text{“value4”}\},$
$path3 \mapsto \{\text{“value4”}, \text{“value5”}\}]]]$

A transaction log. Transactions may either request a set
of changes to a set of targets or rollback a prior change.

VARIABLE *transaction*

A record of per-target proposals

VARIABLE *proposal*

A record of per-target configurations

VARIABLE *configuration*

A record of target states

VARIABLE *target*

A record of target masterships

VARIABLE *mastership*

$vars \triangleq \langle transaction, proposal, configuration, mastership, target \rangle$

LOCAL $Transaction \triangleq$ INSTANCE *Transaction*

LOCAL $Proposal \triangleq$ INSTANCE *Proposal*

LOCAL $Configuration \triangleq$ INSTANCE *Configuration*

LOCAL $Mastership \triangleq$ INSTANCE *Mastership*

This section models configuration changes and rollbacks. Changes are appended to the transaction log and processed asynchronously.

$Value(s, t, p) \triangleq$
LET $value \triangleq$ CHOOSE $v \in s : v.target = t \land v.path = p$
IN
$[value \mapsto value.value,$
$delete \mapsto value.delete]$

$Paths(s, t) \triangleq$
$[p \in \{v.path : v \in \{v \in s : v.target = t\}\} \mapsto Value(s, t, p)]$

$Changes(s) \triangleq$
$[t \in \{v.target : v \in s\} \mapsto Paths(s, t)]$

$ValidValues(t, p) \triangleq$
UNION $\{\{[value \mapsto v, delete \mapsto \text{FALSE}] : v \in Target[t].values[p]\}, \{[value \mapsto Nil, delete \mapsto \text{TRUE}]\}\}$

$ValidPaths(t) \triangleq$
UNION $\{\{v \mathbin{@@} [path \mapsto p] : v \in ValidValues(t, p)\} : p \in \text{DOMAIN } Target[t].values\}$

$ValidTargets \triangleq$
UNION $\{\{p \mathbin{@@} [target \mapsto t] : p \in ValidPaths(t)\} : t \in \text{DOMAIN } Target\}$

The set of all valid sets of changes to all targets and their paths.
The set of possible changes is computed from the *Target* model value.

$ValidChanges \triangleq$
LET $changeSets \triangleq \{s \in \text{SUBSET } ValidTargets :$
$\forall t \in \text{DOMAIN } Target :$
$\forall p \in \text{DOMAIN } Target[t].values :$
$Cardinality(\{v \in s : v.target = t \land v.path = p\}) \leq 1\}$
IN
$\{Changes(s) : s \in changeSets\}$

$RequestChange(i, c) \triangleq$
$\land\ Transaction!RequestChange(i, c)$

$RequestRollback(i, j) \triangleq$
$\land\ Transaction!RequestRollback(i, j)$

$SetMaster(n, t) \triangleq$
$\land\ Mastership!SetMaster(n, t)$
$\land$ UNCHANGED $\langle transaction, proposal, configuration, target\rangle$

$UnsetMaster(t) \triangleq$
$\land\ Mastership!UnsetMaster(t)$
$\land$ UNCHANGED $\langle transaction, proposal, configuration, target\rangle$

$ReconcileTransaction(n, t) \triangleq$
$\land\ Transaction!ReconcileTransaction(n, t)$

$ReconcileProposal(n, t, i) \triangleq$
$\land\ Proposal!ReconcileProposal(n, t, i)$
$\land$ UNCHANGED $\langle transaction\rangle$

$ReconcileConfiguration(n, c) \triangleq$
$\land\ Configuration!ReconcileConfiguration(n, c)$
$\land$ UNCHANGED $\langle transaction, proposal\rangle$

Formal specification, constraints, and theorems.

$$
\begin{array}{l}
\mathit{Init} \triangleq \\
\quad \land\ \mathit{transaction} = [i \in \{\} \mapsto \\
\qquad\qquad [\mathit{type} \mapsto \mathit{Change}, \\
\qquad\qquad\ \mathit{phase} \mapsto \mathit{Initialize}, \\
\qquad\qquad\ \mathit{state} \mapsto \mathit{InProgress}, \\
\qquad\qquad\ \mathit{status} \mapsto \mathit{Pending}]] \\
\quad \land\ \mathit{proposal} = [t \in \text{DOMAIN}\ \mathit{Target} \mapsto \\
\qquad\qquad [i \in \{\} \mapsto \\
\qquad\qquad\ [\mathit{phase} \mapsto \mathit{Initialize}, \\
\qquad\qquad\ \mathit{state} \mapsto \mathit{InProgress}]]] \\
\quad \land\ \mathit{configuration} = [t \in \text{DOMAIN}\ \mathit{Target} \mapsto \\
\qquad\qquad [\mathit{state} \mapsto \mathit{InProgress}, \\
\qquad\qquad\ \mathit{config} \mapsto \\
\qquad\qquad\quad [\mathit{index} \mapsto 0, \\
\qquad\qquad\quad\ \mathit{term} \mapsto 0, \\
\qquad\qquad\quad\ \mathit{values} \mapsto \\
\qquad\qquad\quad\quad [\mathit{path} \in \{\} \mapsto \\
\qquad\qquad\quad\quad\ [\mathit{path} \mapsto \mathit{path}, \\
\qquad\qquad\quad\quad\ \mathit{value} \mapsto \mathit{Nil}, \\
\qquad\qquad\quad\quad\ \mathit{index} \mapsto 0, \\
\qquad\qquad\quad\quad\ \mathit{deleted} \mapsto \text{FALSE}]]], \\
\qquad\qquad\ \mathit{proposal} \mapsto [\mathit{index} \mapsto 0], \\
\qquad\qquad\ \mathit{commit} \mapsto [\mathit{index} \mapsto 0], \\
\qquad\qquad\ \mathit{target} \mapsto \\
\qquad\qquad\quad [\mathit{index} \mapsto 0, \\
\qquad\qquad\quad\ \mathit{term} \mapsto 0, \\
\qquad\qquad\quad\ \mathit{values} \mapsto \\
\qquad\qquad\quad\quad [\mathit{path} \in \{\} \mapsto \\
\qquad\qquad\quad\quad\ [\mathit{path} \mapsto \mathit{path}, \\
\qquad\qquad\quad\quad\ \mathit{value} \mapsto \mathit{Nil}, \\
\qquad\qquad\quad\quad\ \mathit{index} \mapsto 0, \\
\qquad\qquad\quad\quad\ \mathit{deleted} \mapsto \text{FALSE}]]]]] \\
\quad \land\ \mathit{target} = [t \in \text{DOMAIN}\ \mathit{Target} \mapsto \\
\qquad\qquad [\mathit{path} \in \{\} \mapsto \\
\qquad\qquad\ [\mathit{value} \mapsto \mathit{Nil}]]] \\
\quad \land\ \mathit{mastership} = [t \in \text{DOMAIN}\ \mathit{Target} \mapsto [\mathit{master} \mapsto \mathit{Nil},\ \mathit{term} \mapsto 0]]
\end{array}
$$

$$
\begin{array}{l}
\mathit{Next} \triangleq \\
\quad \lor\ \exists\, i \in 1 \mathinner{..} \mathit{NumTransactions} : \\
\qquad \exists\, c \in \mathit{ValidChanges} : \\
\qquad\ \mathit{RequestChange}(i,\ c) \\
\quad \lor\ \exists\, i \in 1 \mathinner{..} \mathit{NumTransactions} :
\end{array}
$$

$\exists\, j \in \text{DOMAIN } transaction :$
$RequestRollback(i,\, j)$
$\lor \exists\, n \in Node :$
$\exists\, t \in \text{DOMAIN } Target :$
$SetMaster(n,\, t)$
$\lor \exists\, t \in \text{DOMAIN } Target :$
$UnsetMaster(t)$
$\lor \exists\, n \in Node :$
$\exists\, t \in \text{DOMAIN } transaction :$
$ReconcileTransaction(n,\, t)$
$\lor \exists\, n \in Node :$
$\exists\, t \in \text{DOMAIN } proposal :$
$\exists\, i \in \text{DOMAIN } proposal[t] :$
$ReconcileProposal(n,\, t,\, i)$
$\lor \exists\, n \in Node :$
$\exists\, c \in \text{DOMAIN } configuration :$
$ReconcileConfiguration(n,\, c)$

$Spec \triangleq Init \land \Box[Next]_{vars} \land \text{WF}_{vars}(Next)$

$Order \triangleq$
$\forall\, t \in \text{DOMAIN } proposal :$
$\forall\, i \in \text{DOMAIN } proposal[t] :$
$\land\ \land\ proposal[t][i].phase = Commit$
$\land\ proposal[t][i].state\ = InProgress$
$\Rightarrow \neg\exists\, j \in \text{DOMAIN } proposal[t] :$
$\land\ j > i$
$\land\ proposal[t][j].phase = Commit$
$\land\ proposal[t][j].state\ = Complete$
$\land\ \land\ proposal[t][i].phase = Apply$
$\land\ proposal[t][i].state\ = InProgress$
$\Rightarrow \neg\exists\, j \in \text{DOMAIN } proposal[t] :$
$\land\ j > i$
$\land\ proposal[t][j].phase = Apply$
$\land\ proposal[t][j].state\ = Complete$

$Consistency \triangleq$
$\forall\, t \in \text{DOMAIN } target :$
LET
Compute the transaction indexes that have been applied to the target
$targetIndexes \triangleq \{i \in \text{DOMAIN } transaction :$
$\land\ i \in \text{DOMAIN } proposal[t]$
$\land\ proposal[t][i].phase = Apply$
$\land\ proposal[t][i].state\ = Complete$
$\land\ t \in transaction[i].targets$
$\land \neg\exists\, j \in \text{DOMAIN } transaction :$

$$
\begin{array}{l}
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, j > i \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, transaction[j].type = Rollback \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, transaction[j].rollback = i \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, transaction[j].phase = Apply \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, transaction[j].state\ = Complete\}
\end{array}
$$

Compute the set of paths in the target that have been updated by transactions

$$
appliedPaths \quad \triangleq \text{ UNION } \{\text{DOMAIN } proposal[t][i].change.values : i \in targetIndexes\}
$$

Compute the highest index applied to the target for each path

$$
\begin{array}{l}
pathIndexes \quad \triangleq\ [p \in appliedPaths \mapsto \text{CHOOSE } i \in targetIndexes : \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \forall\, j \in targetIndexes : \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, i \geq j \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\, p \in \text{DOMAIN } proposal[t][i].change.values]
\end{array}
$$

Compute the expected target configuration based on the last indexes applied to the target for each path.

$$
expectedConfig \ \triangleq\ [p \in \text{DOMAIN } pathIndexes \mapsto proposal[t][pathIndexes[p]].change.values[p]]
$$

IN

$$
target[t] = expectedConfig
$$

$$
\begin{array}{l}
Isolation \ \triangleq \\
\quad \forall\, i \in \text{DOMAIN } transaction : \\
\quad\quad \land\ \land\, transaction[i].phase = Commit \\
\quad\quad\quad\ \land\, transaction[i].state\ = InProgress \\
\quad\quad\quad\ \land\, transaction[i].isolation = Serializable \\
\quad\quad\quad\ \Rightarrow \neg\exists\, j \in \text{DOMAIN } transaction : \\
\quad\quad\quad\quad\quad\quad\ \land\, j > i \\
\quad\quad\quad\quad\quad\quad\ \land\, transaction[j].targets \cap transaction[i].targets \neq \{\} \\
\quad\quad\quad\quad\quad\quad\ \land\, transaction[j].phase = Commit \\
\quad\quad \land\ \land\, transaction[i].phase = Apply \\
\quad\quad\quad\ \land\, transaction[i].state\ = InProgress \\
\quad\quad\quad\ \land\, transaction[i].isolation = Serializable \\
\quad\quad\quad\ \Rightarrow \neg\exists\, j \in \text{DOMAIN } transaction : \\
\quad\quad\quad\quad\quad\quad\ \land\, j > i \\
\quad\quad\quad\quad\quad\quad\ \land\, transaction[j].targets \cap transaction[i].targets \neq \{\} \\
\quad\quad\quad\quad\quad\quad\ \land\, transaction[j].phase = Apply
\end{array}
$$

$$
Safety \ \triangleq\ \Box(Order \land Consistency \land Isolation)
$$

THEOREM $Spec \Rightarrow Safety$

$$
\begin{array}{l}
Terminated(i) \ \triangleq \\
\quad \land\, i \in \text{DOMAIN } transaction \\
\quad \land\, transaction[i].phase \in \{Apply,\ Abort\} \\
\quad \land\, transaction[i].state\ = Complete
\end{array}
$$

$$
\begin{array}{l}
Termination \ \triangleq \\
\quad \forall\, i \in 1\,..\,NumTransactions : Terminated(i)
\end{array}
$$

$Liveness \triangleq \Diamond Termination$

THEOREM $Spec \Rightarrow Liveness$

* Modification History
* Last modified *Thu Feb* 10 15:59:15 *PST* 2022 by *jordanhalterman*
* Created *Wed Sep* 22 13:22:32 *PDT* 2021 by *jordanhalterman*