MODULE *BrokenDistributedLock*

CONSTANT *Client* The set of client

VARIABLES
clientState, *clientState*[*c*] is the state of client *c*.
lockLeaseState

TypeOK $\triangleq$
$\land$ *clientState* $\in [Client \to \{$"init", "gotLockLease", "WritingData", "WroteData"$\}]$
$\land$ *lockLeaseState* $\in \{$"unlock", "locked"$\}$

Init $\triangleq$
"" ""
$\land$ *clientState* $= [c \in Client \mapsto$ "init"$]$
$\land$ *lockLeaseState* $=$ "unlock"

ClientLocking(*c*) $\triangleq$
c
$\land$ *lockLeaseState* $=$ "unlock"
$\land$ *clientState*$[c]$ $=$ "init"
$\land$ *lockLeaseState*$'$ $=$ "locked"
$\land$ *clientState*$' = [$*clientState* EXCEPT $![c] =$ "gotLockLease"$]$

ClientWritingData(*c*) $\triangleq$
c
$\land$ *clientState*$[c] =$ "gotLockLease"
$\land$ *clientState*$' = [$*clientState* EXCEPT $![c] =$ "WritingData"$]$

ClientWroteData(*c*) $\triangleq$
c
$\land$ *clientState*$[c] =$ "WritingData"
$\land$ *clientState*$' = [$*clientState* EXCEPT $![c] =$ "WroteData"$]$
$\land$ *lockLeaseState*$'$ $=$ "unlock"

LockExpire $\triangleq$

$\land$ *lockLeaseState* $=$ "locked"
$\land$ *lockLeaseState*$'$ $=$ "unlock"

Next $\triangleq$
$\lor$ *LockExpire*
$\lor \exists\, c \in Client$:
ClientLocking(*c*) $\lor$ *ClientWritingData*(*c*) $\lor$ *ClientWroteData*(*c*)

Spec $\triangleq$ *Init* $\land \Box[Next]_{\langle clientState,\, lockLeaseState \rangle}$

$$Consistent \triangleq$$
$$\forall\, c \in Client : \neg(\, \wedge\, clientState[c] = \text{“WritingData”}$$
$$\wedge\, \neg lockLeaseState = \text{“locked”}\,)$$

THEOREM $Spec \Rightarrow \Box(TypeOK \wedge Consistent)$

* Modification History
* Last modified Sun *Jul* 17 22:34:45 *CST* 2022 by *wengjialin*
* Created Sun *Jul* 17 20:46:46 *CST* 2022 by *wengjialin*