MODULE *AbstractBallotingWithPrepare*

EXTENDS *DomainModel*

VARIABLES
ballot
, *h*
, *voteToPrepare*
, *acceptedPrepared*
, *voteToCommit*
, *acceptedCommitted*
, *externalized*
, *byz*

$$
\begin{aligned}
&\mathit{TypeOK} \triangleq \\
&\quad \land\ \mathit{ballot} \in [N \to \mathit{BallotOrNull}] \\
&\quad \land\ h \in [N \to \mathit{BallotOrNull}] \\
&\quad \land\ \mathit{voteToPrepare} \in [N \to \text{SUBSET } \mathit{Ballot}] \\
&\quad \land\ \mathit{acceptedPrepared} \in [N \to \text{SUBSET } \mathit{Ballot}] \\
&\quad \land\ \mathit{voteToCommit} \in [N \to \text{SUBSET } \mathit{Ballot}] \\
&\quad \land\ \mathit{acceptedCommitted} \in [N \to \text{SUBSET } \mathit{Ballot}] \\
&\quad \land\ \mathit{externalized} \in [N \to \text{SUBSET } \mathit{Ballot}] \\
&\quad \land\ \mathit{byz} \in \text{SUBSET } N
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{Init} \triangleq \\
&\quad \land\ \mathit{ballot} = [n \in N \mapsto \mathit{nullBallot}] \\
&\quad \land\ h = \ [n \in N \mapsto \mathit{nullBallot}] \\
&\quad \land\ \mathit{voteToPrepare} = [n \in N \mapsto \{\}] \\
&\quad \land\ \mathit{acceptedPrepared} = [n \in N \mapsto \{\}] \\
&\quad \land\ \mathit{voteToCommit} = [n \in N \mapsto \{\}] \\
&\quad \land\ \mathit{acceptedCommitted} \ = [n \in N \mapsto \{\}] \\
&\quad \land\ \mathit{externalized} = [n \quad \in N \mapsto \{\}] \\
&\quad \land\ \mathit{byz} \in \mathit{FailProneSet}
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{IncreaseBallotCounter}(n,\ c) \triangleq \\
&\quad \land\ c > 0 \\
&\quad \land\ c > \mathit{ballot}[n].\mathit{counter} \\
&\quad \land\ \text{IF } h[n] \neq \mathit{nullBallot} \\
&\qquad \text{THEN } \mathit{ballot}' = [\mathit{ballot} \text{ EXCEPT } ![n] = [\mathit{counter} \mapsto c,\ \mathit{value} \mapsto h[n].\mathit{value}]] \\
&\qquad \text{ELSE } \exists\, v \in V : \mathit{ballot}' = [\mathit{ballot} \text{ EXCEPT } ![n] = [\mathit{counter} \ \mapsto c,\ \mathit{value} \mapsto v]] \\
&\quad \land\ \mathit{voteToPrepare}' = [\mathit{voteToPrepare} \text{ EXCEPT } ![n] = @ \cup \{\mathit{ballot}[n]'\}] \\
&\quad \land\ \text{UNCHANGED } \langle h,\ \mathit{acceptedPrepared},\ \mathit{voteToCommit},\ \mathit{acceptedCommitted},\ \mathit{externalized},\ \mathit{byz}\rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{AcceptPrepared}(n,\ b) \triangleq \\
&\quad \land\ \ \lor \exists\, Q \in \mathit{Quorum} : \forall\, n2 \in Q \setminus \mathit{byz} : b \in \mathit{voteToPrepare}[n2] \cup \mathit{acceptedPrepared}[n2] \\
&\qquad \lor \exists\, \mathit{Bl} \in \mathit{BlockingSet} : \forall\, n2 \in \mathit{Bl} \setminus \mathit{byz} : b \qquad\qquad\quad \in \mathit{acceptedPrepared}[n2] \\
&\quad \land\ \mathit{acceptedPrepared}' = [\mathit{acceptedPrepared} \text{ EXCEPT } ![n] = @ \cup \{b\}]
\end{aligned}
$$

$\land$ UNCHANGED $\langle ballot,\ h,\ voteToPrepare,\ voteToCommit,\ acceptedCommitted,\ externalized,\ byz\rangle$

$ConfirmPrepared(n,\ b) \triangleq$
$\land\ h[n] \prec b$
$\land\ \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in acceptedPrepared[n2]$
$\land\ h' = [h \text{ EXCEPT } ![n] = b]$
$\land$ UNCHANGED $\langle ballot,\ voteToPrepare,\ acceptedPrepared,\ voteToCommit,\ acceptedCommitted,\ externalize$

$CanVoteToCommit(n,\ b) \triangleq$
$\land\ b = ballot[n]$
$\land\ \forall\, b2 \in Ballot : LessThanAndIncompatible(b,\ b2) \Rightarrow b2 \notin voteToPrepare[n] \cup acceptedPrepared[n]$
$\land\ \lor \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in acceptedPrepared[n2]$
$\lor \exists\, cnt \in BallotNumber :$
$\land\ cnt < b.counter$
$\land\ [counter \mapsto cnt,\ value \mapsto b.value] \in acceptedCommitted[n]$

$VoteToCommit(n,\ b) \triangleq$
$\land\ CanVoteToCommit(n,\ b)$
$\land\ voteToCommit' = [voteToCommit \text{ EXCEPT } ![n] = @ \cup \{b\}]$
$\land$ IF $h[n] \preceq b$
THEN $h' = [h \text{ EXCEPT } ![n] = b]$
ELSE UNCHANGED h
$\land$ UNCHANGED $\langle ballot,\ voteToPrepare,\ acceptedPrepared,\ acceptedCommitted,\ externalized,\ byz\rangle$

$AcceptCommitted(n,\ b) \triangleq$
$\land\ b = ballot[n]$
$\land\ \lor\ \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in voteToCommit[n2]$
$\lor\ \exists\, Bl \in BlockingSet : \forall\, n2 \in Bl \setminus byz : b \in acceptedCommitted[n2]$
$\land\ acceptedCommitted' = [acceptedCommitted \text{ EXCEPT } ![n] = @ \cup \{b\}]$
$\land$ UNCHANGED $\langle ballot,\ h,\ voteToPrepare,\ acceptedPrepared,\ voteToCommit,\ externalized,\ byz\rangle$

$Externalize(n,\ b) \triangleq$
$\land\ b = ballot[n]$
$\land\ \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in acceptedCommitted[n2]$
$\land\ externalized' = [externalized \text{ EXCEPT } ![n] = @ \cup \{b\}]$
$\land$ UNCHANGED $\langle ballot,\ h,\ voteToPrepare,\ acceptedPrepared,\ voteToCommit,\ acceptedCommitted,\ byz\rangle$

$ByzantineHavoc \triangleq$
$\land \exists\, x \in [byz \to \text{SUBSET } Ballot] :$
$voteToPrepare' = [n \in N \mapsto \text{IF } n \in byz \text{ THEN } x[n] \text{ ELSE } voteToPrepare[n]]$
$\land \exists\, x \in [byz \to \text{SUBSET } Ballot] :$
$acceptedPrepared' = [n \in N \mapsto \text{IF } n \in byz \text{ THEN } x[n] \text{ ELSE } acceptedPrepared[n]]$
$\land \exists\, x \in [byz \to \text{SUBSET } Ballot] :$
$voteToCommit' = [n \in N \mapsto \text{IF } n \in byz \text{ THEN } x[n] \text{ ELSE } voteToCommit[n]]$
$\land \exists\, x \in [byz \to \text{SUBSET } Ballot] :$
$acceptedCommitted' = [n \in N \mapsto \text{IF } n \in byz \text{ THEN } x[n] \text{ ELSE } acceptedCommitted[n]]$
$\land$ UNCHANGED $\langle h,\ externalized,\ byz\rangle$

$Next \triangleq$
$\quad \lor \exists\, n \in N \setminus byz,\, c \in BallotNumber,\, v \in V :$
$\qquad \text{LET } b \triangleq [counter \mapsto c,\, value \mapsto v] \text{IN}$
$\qquad\quad \lor IncreaseBallotCounter(n,\, c)$
$\qquad\quad \lor AcceptPrepared(n,\, b)$
$\qquad\quad \lor ConfirmPrepared(n,\, b)$
$\qquad\quad \lor VoteToCommit(n,\, b)$
$\qquad\quad \lor AcceptCommitted(n,\, b)$
$\qquad\quad \lor Externalize(n,\, b)$
$\quad \lor ByzantineHavoc$

$vars \triangleq \langle ballot,\, h,\, voteToPrepare,\, acceptedPrepared,\, voteToCommit,\, acceptedCommitted,\, externalized,\, byz \rangle$
$Spec \triangleq Init \land \Box[Next]_{vars}$

$Agreement \triangleq$
$\quad \forall\, n1,\, n2 \in N \setminus byz : \forall\, b1,\, b2 \in Ballot :$
$\qquad b1 \in externalized[n1] \land b2 \in externalized[n2] \Rightarrow b1.value = b2.value$

$Invariant \triangleq$
$\quad \land\ \forall\, n1,\, n2 \in N \setminus byz,\, c \in BallotNumber,\, v1,\, v2 \in V :$
$\qquad \land\ [counter \mapsto c,\, value \mapsto v1] \in acceptedPrepared[n1]$
$\qquad \land\ [counter \mapsto c,\, value \mapsto v2] \in acceptedPrepared[n2]$
$\qquad \Rightarrow v1 = v2$