```
──────────────── MODULE FastConsensus ────────────────
EXTENDS Integers, FiniteSets

CONSTANTS
    V  the set of values to decide on
,   P  the set of processes (typically $3f + 1$ nodes)
,   Quorum  the set of quorums (typically sets of $2f + 1$ nodes out of $3f + 1$)
,   Blocking  the set of blocking sets (typically sets $f + 1$ nodes out of $3f + 1$)
,   B  the set of malicious nodes (typically f nodes)
,   Leader(_)  assigns a leader to each round

$Round \triangleq Nat$  the set of rounds

 Each round consists of 3 voting phases:
$Phase \triangleq 1 \,..\, 3$
 A votes is cast in a phase of a round and for a value:
$Vote \triangleq [round : Round, phase : Phase, value : V]$
 A proposal is for a round and a value:
$Proposal \triangleq [round : Round, value : V]$

  --algorithm FastConsensus{
    variables
        $proposals = \{\}$ ;
        $votes \;= [p \in P \mapsto \{\}]$ ;
        $round = [p \in P \mapsto 0]$ ;
    define {
        $Decided \triangleq \{v \in V : \exists Q \in Quorum, r \in Round : \forall p \in Q \setminus B :$
            $[round \mapsto r, phase \mapsto 3, value \mapsto v] \in votes[p]\}$
        $Safety \triangleq Cardinality(Decided) \leq 1$
        $Proposable(v, r, HO) \triangleq$   HO is intended to be the set of processes the leader hears of
            $\lor\; r = 0$  no constraint if it's round 0
            $\lor\; \land\; \forall p \in HO \setminus B \;: round[p] \geq r$
               $\land\; \exists Q \in Quorum : Q \subseteq HO$
               $\land\; \exists r2 \in 0 \,..\, (r - 1) : \forall p \in HO \setminus B : \forall vt \in votes[p] :$
                     $vt.round < r \land vt.phase = 3 \Rightarrow$
                         $\land\; vt.round \leq r2$
                         $\land\; vt.round = r2 \Rightarrow vt.value = v$
                         $\land\; \exists Bl \in Blocking :$
                             $\land\; Bl \subseteq HO$
                             $\land\; \forall p2 \in Bl \setminus B : \exists vt2 \in votes[p2] :$
                                    $\land\; vt2.round = r2$
                                    $\land\; vt2.phase \;= 2$
                                    $\land\; vt2.value \;= v$
    $Safe(v, r) \triangleq$
        $\lor\ r = 0$
        $\lor\ \exists\, r2 \in 0 \,..\, (r-1) : \exists\, Q \in Quorum :$
            $\forall\, p \in Q \setminus B \quad : \forall\, vt \in votes[p] :$
              $vt.round < r \land vt.phase = 3 \Rightarrow$
                $\land\ vt.round \leq r2$
                $\land\ vt.round = r2 \Rightarrow vt.value = v$
                $\land\ \exists\, Bl \in Blocking : \forall\, p2 \in Bl \setminus B : \exists\, vt2 \in votes[p2] :$
                    $\land\ vt2.round = r2$
                    $\land\ vt2.phase = 1$
                    $\land\ vt2.value \ = v$
  }
  macro $vote(\ p,\ v,\ r,\ ph\ )$ {
    $votes[p] := votes[p] \cup \{[round \mapsto r,\ phase \mapsto ph,\ value \mapsto v]\}$ ;
  }
  process ( $proc \in (P \setminus B)$ ) {
$l0$:  while ( TRUE )
        either {
          when $Leader(round[self]) = self$ ;
          with ( $v \in V$ ) {
            if ( $self \notin B$ )
                with ( $HO \in$ SUBSET $P$ )
                    when $Proposable(v,\ round[self],\ HO)$ ;
            $proposals := proposals \cup \{[round \mapsto round[self],\ value \mapsto v]\}$
           }
        }
        or with ( $v \in V,\ Q \in Quorum$ ) {
          when $Leader(round[self]) \notin B \Rightarrow [round \mapsto round[self],\ value \mapsto v] \in proposals$ ;
          when $Safe(v,\ round[self])$ ;
          when $\forall\, vt \in votes[self] : \neg(vt.round = round[self])$ ;
          $vote(self,\ v,\ round[self],\ 1)$ ;
        }
        or with ( $v \in V,\ Q \in Quorum$ ) {
          when $\forall\, p \in Q \setminus B$ :
              $[round \mapsto round[self],\ phase \mapsto 1,\ value \mapsto v] \in votes[p]$ ;
          when $\forall\, vt \in votes[self] : \neg(vt.round = round[self] \land vt.phase \geq 2)$ ;
          $vote(self,\ v,\ round[self],\ 2)$ ;
        }
        or with ( $v \in V,\ Q \in Quorum,\ Bl \in Blocking$ ) {
          when $\forall\, vt \in votes[self] : \neg(vt.round = round[self] \land vt.phase = 3)$ ;
          when
              $\lor\ \ \forall\, p \in Q \setminus B$ :
                  $[round \mapsto round[self],\ phase \mapsto 2,\ value \mapsto v] \in votes[p]$
              $\lor\ \ \forall\, p \in Bl \setminus B$ :
                    $[round \mapsto round[self],\ phase \mapsto 3,\ value \mapsto v] \in votes[p]$ **;**
           $vote(self,\ v,\ round[self],\ 3)$ **;**
        **}**
        **or {**
           $round[self] := round[self] + 1$ **;**
        **}**
    **}**
**}**
```