```
──────────────── MODULE BB_FA ────────────────
EXTENDS Naturals, FiniteSets, TLAPS, FiniteSetTheorems

  ***************************************************************************
   SPECIFICATION
  ***************************************************************************
──────────────────────────────────────────────
  *** Set up
CONSTANT W,                  Uninterpreted set of BB contents, except that it contains a phase, see below
         B0,                 A fixed, initial BB content in W
         extendsB(_, _),     Extension relation (will be axiomatized, could be interpretted as ⊆ )
         peersH,             Set of Honest BB peers
         peersD,             Set of Dishonest (malicious) BB peers
         readers,            Set of readers
         threshold,          threshold \gamma
         n,                  total number of peers (in peersH ∪ peersD)
         nh,                 number of honest peers (in peersH)
         pf                  final phase (in Nat)

VARIABLE fr,       [readers → SUBSET (W)]: For each reader, set of BB contents that have been read through Read-nonFinal
         nfr,      [readers → SUBSET (W)]: For each reader, set of BB contents that have been read through Read-Final
         Pv,       [peersH → W]: For each honest BB peer, its curent view (BB content)
         signed    [peers → SUBSET W]: Set of BB contents that have been signed by each peer

  *** Assumptions
Phases ≜ 1 .. pf                 Set of all the phases
Wb ≜ {B[1] : B ∈ W}              We eventually assume that elements in W are in Wb × Phases
peers ≜ peersH ∪ peersD
  We assume that extends(., .) is transitive, reflexive, and anti-symmetric.
ExtendsOK ≜ ∧ ∀ B1, B2, B3 ∈ Wb : extendsB(B1, B2) ∧ extendsB(B2, B3) ⇒ extendsB(B1, B3)
            ∧ ∀ B ∈ Wb : extendsB(B, B)
            ∧ ∀ B1, B2 ∈ Wb : extendsB(B1, B2) ∧ extendsB(B2, B1) ⇒ B1 = B2
  We assume threshold meets the conditions of \gamma, see the paper
ThresholdOK ≜ ∧ threshold ∈ Nat              threshold is a natural number
              ∧ nh > 2 * (n − threshold)     \gamma requirement (sanity check: TLC finds an attack without this)
              ∧ threshold ≤ n                thereshold cannot be greater than the number of peers
WOK ≜ ∧ W ⊆ Wb × Phases                      BB contents are represented as a content in Wb with a phase in Phases
      ∧ B0 ∈ W                               the initial BB content is in W
      ∧ B0[2] = 1                            and has 1 as phase: the initial phase
      ∧ ∀ B1, B2 ∈ W : B1[1] = B2[1] ⇒ B1 = B2   equally of BB contents implies equality of their phases
PeersOK ≜ ∧ n ∈ Nat ∧ nh ∈ Nat
          ∧ IsFiniteSet(peersD) ∧ IsFiniteSet(peersH)
          ∧ nh = Cardinality(peersH)         nh is the number of honest peers (in peersH)
          ∧ n = Cardinality(peers)           n is the number of all peers (in peersH ∪ peersD)
          ∧ peersH ∩ peersD = {}             a peers is honest XOR dishonest (malicious)
PhasesOK ≜ ∧ pf ∈ Nat                        there is a final phase
```

$\quad\quad\quad\land\ pf > 1$ which is not the initial phase (1)

ASSUME $ExtendsOK$

ASSUME $ThresholdOK$

ASSUME WOK

ASSUME $PeersOK$

ASSUME $PhasesOK$

*** Type correctness invariant

$TypeOK \triangleq \land\ fr \in [readers \rightarrow \text{SUBSET } W]$

$\quad\quad\quad\quad \land\ nfr \in [readers \rightarrow \text{SUBSET } W]$

$\quad\quad\quad\quad \land\ Pv \in [peersH \rightarrow W]$

$\quad\quad\quad\quad \land\ signed \in [peers \rightarrow \text{SUBSET } W]$

*** Helping functions

$phase(B) \triangleq B[2]$ Phase of a BB content

$extends(B1, B2) \triangleq extendsB(B1[1], B2[1])$ Lift $extendsB$ to W

*** *Inital* states specification

$Init \triangleq \land\ fr\ = [r \in readers \mapsto \{\}]$

$\quad\quad\quad \land\ nfr = [r \in readers \mapsto \{\}]$

$\quad\quad\quad \land\ Pv\ = [P \in peersH \mapsto B0]$ the initial honest peers's view is $B0$

$\quad\quad\quad \land\ signed = [P \in peers \mapsto \{\}]$

*** Guards

The GuR guard expresses the main condition that readers check when reading BB contents

$GuR(B) \triangleq \exists\, peersS \in \text{SUBSET } peers :$

$\quad\quad\quad\quad \land\ Cardinality(peersS) \geq threshold$

$\quad\quad\quad\quad \land\ \forall\, P \in peersS : B \in signed[P]$

*** Events

UpdatePH: An honest BB peer updates his view (to bu) and must follow the specification

$UpdatePH \triangleq \exists\, P \in peersH : \exists\, bu \in W :$

$\quad\quad\quad\quad \land\ extends(Pv[P], bu)$ this encodes the restriction on \cup_B; *i.e.*, $extends(B, B \cup B')$

$\quad\quad\quad\quad \land\ phase(Pv[P]) \neq pf$ no more update once a final BB content has been reached

$\quad\quad\quad\quad \land\ Pv' = [Pv \text{ EXCEPT } ![P] = bu]$

$\quad\quad\quad\quad \land\ \text{UNCHANGED } \langle fr, nfr, signed \rangle$

SignPH: An honest BB peer signs a content (bs) computed from *partial*() and his view. He must follow the specification.

$SignPH \triangleq \exists\, P \in peersH : \exists\, bs \in W :$

The following conjunct encodes the restrictions on partial: *e.g.*, $\forall\, b' \in partial(b)$: $extends(b', b)$. It is a strict generalization.

$\quad\quad\quad\quad \land\ extends(bs, Pv[P]) \land phase(bs) = phase(Pv[P])$

$\quad\quad\quad\quad \land\ (phase(Pv[P]) = pf \Rightarrow bs = Pv[P])$

$\quad\quad\quad\quad \land\ signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$

$\quad\quad\quad\quad \land\ \text{UNCHANGED } \langle fr, nfr, Pv \rangle$

SignPD: An dishonest *BB* peer can sign ANY content (*bs*) since he does not have to follow the specification.

$SignPD \triangleq \exists P \in peersD : \exists bs \in W :$
$\quad \land signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$
$\quad \land \text{UNCHANGED } \langle fr, nfr, Pv \rangle$

ReadNonFinal: A reader reads through Read-NonFinal and obtains *bu*. There is no explicit label *w.l.o.g.* (see above).

$ReadNonFinal \triangleq \exists bu \in W : \exists R \in readers : \exists p \in Nat :$
$\quad \land GuR(bu)$ — this is the test that each reader performs when reading
$\quad \land p = phase(bu)$ — additionally, the reader checks that the read *BB* contents has the requested
$\quad \land nfr' = [nfr \text{ EXCEPT } ![R] = nfr[R] \cup \{bu\}]$
$\quad \land \text{UNCHANGED } \langle fr, Pv, signed \rangle$

ReadFinal: A reader reads through Read-Final.

$ReadFinal \triangleq \exists bu \in W : \exists R \in readers :$
$\quad \land GuR(bu)$ — this is the test that each reader performs when reading
$\quad \land phase(bu) = pf$ — additionally, the reader checks that the read *BB* contents has the phase *pf*
$\quad \land fr' = [fr \text{ EXCEPT } ![R] = fr[R] \cup \{bu\}]$
$\quad \land \text{UNCHANGED } \langle nfr, Pv, signed \rangle$

*** State evolutions specification

$Next \triangleq \lor UpdatePH$
$\quad \lor SignPH$
$\quad \lor SignPD$
$\quad \lor ReadNonFinal$
$\quad \lor ReadFinal$

*** The protocol is defined with *Init* describing initial states and with *Next* describing state evolutions (plus stuttering steps).

$Protocol \triangleq Init \land \Box[Next]_{\langle fr, nfr, Pv, signed \rangle}$

*** We prove below that final-agreement (*FA*) is an invariant of Spec. *FA* is encoded as follows (see *FA*).

$BSfr \triangleq \text{UNION } \{fr[R] : R \in readers\}$ — set of all final read *BB* contents
$BSnfr \triangleq \text{UNION } \{nfr[R] : R \in readers\}$ — set of all read *BB* contents
$FA \triangleq \land (BSfr = \{\} \lor \exists Bf \in BSfr : BSfr = \{Bf\})$ — *FA* (*i*)
$\quad \land \forall Bf \in BSfr : \forall B \in BSnfr : extends(B, Bf)$ — *FA* (ii)

PROOFS .

****
PROPERTY STATEMENTS
****

Parametrized *FA* (will help *w.r.t.* modularity)

$FA\_param(FR, NFR) \triangleq \land (FR = \{\} \lor \exists Bf \in FR : FR = \{Bf\})$
$\quad \land \forall Bf \in FR : \forall B \in NFR : extends(B, Bf)$

$FinalW \triangleq \{B \in W : phase(B) = pf\}$ — *BB* contents having the final phase *pf*

$NFRP(P) \triangleq signed[P] \cup \{Pv[P]\}$ — non-final content from a peer's perspective (P)

$FRP(P) \triangleq NFRP(P) \cap FinalW$ — final content from a peer's perspective (P)

*** Key invariants and properties for the final proof

(for LEMMA 2) [Invariant] Honest peers locally enforce *FC*

$PeersLocalFC \triangleq$

$\quad \forall P \in peersH : \land \forall B \in signed[P] : extends(B, Pv[P])$

$\quad\quad\quad\quad\quad\quad\quad\quad \land \forall B \in FRP(P) : B = Pv[P]$

(for LEMMA 3) [Invariant] Honest peers locally enforce *FA*

$PeersLocalFA \triangleq$

$\quad \forall P \in peersH : FA\_param(FRP(P),$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad NFRP(P))$

(for LEMMA 4,7) [Invariant] Any reader's read enforces *GuR* and phase restriction

$ReadersLocalGu \triangleq$

$\quad \forall R \in readers : \land \forall B \in nfr[R] : GuR(B)$

$\quad\quad\quad\quad\quad\quad\quad\quad \land \forall B \in fr[R] : GuR(B) \land phase(B) = pf$

(for LEMMA 1) Threshold asumptions make it so that there always is an honest peer in two valid sets of peers

$IntersecPeers \triangleq$

$\quad \forall peersS1, peersS2 \in \text{SUBSET } peers :$

$\quad\quad (\land Cardinality(peersS1) \geq threshold$

$\quad\quad\;\; \land Cardinality(peersS2) \geq threshold$

$\quad\quad) \Rightarrow \exists Ph \in (peersS1 \cap peersS2 \cap peersH) : \text{TRUE}$ — this gives us some honest peer *Ph* in the intersection

(for LEMMA $5-7$) [Invariant] Any final *BB* read content extends any other read *BB* content.

$ReaderAgreement \triangleq$

$\quad \forall R1, R2 \in readers :$

$\quad\quad \forall B1 \in (BSfr \cup BSnfr) :$

$\quad\quad \forall B2 \in BSfr : extends(B1, B2)$

*** Basic and simple invariants

$Inv1 \triangleq TypeOK$

$InvGuPreservation \triangleq \forall B \in W : (Inv1 \land GuR(B) \land [Next]_{\langle fr, nfr, Pv, signed \rangle} \Rightarrow GuR(B)')$

****

CLAIMS AND PROOFS

****

** Basic properties

PROPOSITION $eqSingleton \triangleq$ ASSUME NEW $S1 \in$ SUBSET W, NEW $S2 \in$ SUBSET W, NEW $B1 \in S1$, NEW $B2$

$\quad$ OBVIOUS

PROPOSITION $antiSymEx \triangleq$ ASSUME NEW $B1 \in W$, NEW $B2 \in W$, $extends(B1, B2)$, $extends(B2, B1)$PROV

BY $ExtendsOK$, WOK DEF $ExtendsOK$, $extends$, Wb, WOK

PROPOSITION $equSets \triangleq$ ASSUME NEW $BS1 \in$ SUBSET W, NEW $BS2 \in$ SUBSET W PROVE $(BS1 \neq \{\} \land BS2$
  $\langle 1 \rangle$ SUFFICES ASSUME $BS1 \neq \{\} \land BS2 \neq \{\} \land \forall B1 \in BS1 : \forall B2 \in BS2 : B1 = B2$
    PROVE $BS1 = BS2$
    OBVIOUS
 $\langle 1 \rangle 1$ $\forall B1 \in BS1 : B1 \in BS2$ OBVIOUS
 $\langle 1 \rangle 2$ $\forall B1 \in BS1 : B1 \in BS2$ OBVIOUS
 $\langle 1 \rangle$f QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$
PROPOSITION $CardPeers \triangleq IsFiniteSet(peers) \land Cardinality(peers) = n$
  $\langle 1 \rangle 1.$ $IsFiniteSet(peers)$
    BY $PeersOK$, FS_Union DEF $PeersOK$, $peers$
  $\langle 1 \rangle 2.$ $Cardinality(peers) = n$
    BY $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$, $peers$
  $\langle 1 \rangle 3.$ QED
    BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$
PROPOSITION $ExtendsRefl \triangleq$ ASSUME NEW $B \in W$ PROVE $extends(B, B)$
 BY $ExtendsOK$, WOK DEF $ExtendsOK$, $extends$, Wb, WOK
PROPOSITION $ExtendsRefl2 \triangleq$ ASSUME NEW $B1 \in W$, NEW $B2 \in W$ PROVE $B1 = B2 \Rightarrow extends(B2, B1)$
 BY $ExtendsOK$, WOK DEF $ExtendsOK$, $extends$, Wb, WOK
PROPOSITION $ExtendsTrans \triangleq$ ASSUME NEW $B1 \in W$, NEW $B2 \in W$, NEW $B3 \in W$, $extends(B1, B2)$, $exte$
 BY $ExtendsOK$ DEF $ExtendsOK$, $extends$, Wb
PROPOSITION $TExistsPeer \triangleq \exists P \in peersH :$ TRUE
  $\langle 1 \rangle 1$ $nh > 0$
    $\langle 2 \rangle$ $n \geq threshold$
      BY $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
    $\langle 2 \rangle$f QED
      BY $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
  $\langle 1 \rangle$f QED
    BY $\langle 1 \rangle 1$, $PeersOK$, $FS\_EmptySet$ DEF $ThresholdOK$, $PeersOK$

PROPOSITION $Invariance1 \triangleq Protocol \Rightarrow \Box Inv1$
$\langle 1 \rangle$ USE DEF $Inv1$, $TypeOK$
$\langle 1 \rangle$init $Init \Rightarrow TypeOK$ BY WOK DEF $Init$, WOK
$\langle 1 \rangle$induction $TypeOK \land [Next]_{\langle fr,\, nfr,\, Pv,\, signed \rangle} \Rightarrow TypeOK'$
  $\langle 2 \rangle$ SUFFICES ASSUME $TypeOK$,
      $[Next]_{\langle fr,\, nfr,\, Pv,\, signed \rangle}$
    PROVE $TypeOK'$
    OBVIOUS
  $\langle 2 \rangle 1.$ ASSUME NEW $P \in peersH$,
      NEW $bu \in W$,
      $\land\ extends(Pv[P], bu)$
      $\land\ phase(Pv[P]) \neq pf$
      $\land\ Pv' = [Pv$ EXCEPT $![P] = bu]$
      $\land$ UNCHANGED $\langle fr, nfr, signed \rangle$
    PROVE $TypeOK'$
    BY $\langle 2 \rangle 1$, WOK DEF $Init$, WOK

```
  ⟨2⟩2. ASSUME NEW P ∈ peersH,
                NEW bs ∈ W,
                ∧ extends(bs, Pv[P])
                ∧ (phase(Pv[P]) = pf ⇒ bs = Pv[P])
                ∧ signed' = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
                ∧ UNCHANGED ⟨fr, nfr, Pv⟩
        PROVE  TypeOK'
    BY ⟨2⟩2, WOK DEF Init, WOK
  ⟨2⟩3. ASSUME NEW P ∈ peersD,
                NEW bs ∈ W,
                ∧ signed' = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
                ∧ UNCHANGED ⟨fr, nfr, Pv⟩
        PROVE  TypeOK'
    BY ⟨2⟩3, WOK DEF Init, WOK
  ⟨2⟩4. ASSUME NEW bu ∈ W,
                NEW R ∈ readers,
                ∧ GuR(bu)
                ∧ nfr' = [nfr EXCEPT ![R] = nfr[R] ∪ {bu}]
                ∧ UNCHANGED ⟨fr, Pv, signed⟩
        PROVE  TypeOK'
    BY ⟨2⟩4, WOK DEF Init, WOK
  ⟨2⟩5. ASSUME NEW bu ∈ W,
                NEW R ∈ readers,
                ∧ GuR(bu) ∧ phase(bu) = pf
                ∧ fr' = [fr EXCEPT ![R] = fr[R] ∪ {bu}]
                ∧ UNCHANGED ⟨nfr, Pv, signed⟩
        PROVE  TypeOK'
    BY ⟨2⟩5, WOK DEF Init, WOK
  ⟨2⟩6.CASE UNCHANGED ⟨fr, nfr, Pv, signed⟩
    BY ⟨2⟩6, WOK DEF Init, WOK
  ⟨2⟩7. QED
    BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6  DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH
⟨1⟩ QED BY ⟨1⟩init, ⟨1⟩induction, PTL DEF Protocol

PROPOSITION GuPreservation ≜ ∀ B ∈ W : (Inv1 ∧ GuR(B) ∧ [Next]_⟨fr, nfr, Pv, signed⟩ ⇒ GuR(B)')
⟨1⟩ USE  DEF Inv1, TypeOK, GuR
⟨1⟩ QED
  ⟨2⟩ SUFFICES ASSUME NEW B ∈ W,
                      Inv1,
                      NEW peersS ∈ SUBSET peers,
                      ∧ Cardinality(peersS) ≥ threshold
                      ∧ ∀ P ∈ peersS : B ∈ signed[P],
                      [Next]_⟨fr, nfr, Pv, signed⟩
               PROVE  GuR(B)'
    BY  DEF GuR
```

```
⟨2⟩1. ASSUME NEW P ∈ peersH,
              NEW bu ∈ W,
              ∧ extends(Pv[P], bu)
              ∧ phase(Pv[P]) ≠ pf
              ∧ Pv′ = [Pv EXCEPT ![P] = bu]
              ∧ UNCHANGED ⟨fr, nfr, signed⟩
       PROVE  GuR(B)′
  BY ⟨2⟩1
⟨2⟩2. ASSUME NEW P ∈ peersH,
              NEW bs ∈ W,
              ∧ extends(bs, Pv[P])
              ∧ (phase(Pv[P]) = pf ⇒ bs = Pv[P])
              ∧ signed′ = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
              ∧ UNCHANGED ⟨fr, nfr, Pv⟩
       PROVE  GuR(B)′
  BY ⟨2⟩2
⟨2⟩3. ASSUME NEW P ∈ peersD,
              NEW bs ∈ W,
              ∧ signed′ = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
              ∧ UNCHANGED ⟨fr, nfr, Pv⟩
       PROVE  GuR(B)′
  BY ⟨2⟩3
⟨2⟩4. ASSUME NEW bu ∈ W,
              NEW R ∈ readers,
              ∧ GuR(bu)
              ∧ nfr′ = [nfr EXCEPT ![R] = nfr[R] ∪ {bu}]
              ∧ UNCHANGED ⟨fr, Pv, signed⟩
       PROVE  GuR(B)′
  BY ⟨2⟩4
⟨2⟩5. ASSUME NEW bu ∈ W,
              NEW R ∈ readers,
              ∧ GuR(bu) ∧ phase(bu) = pf
              ∧ fr′ = [fr EXCEPT ![R] = fr[R] ∪ {bu}]
              ∧ UNCHANGED ⟨nfr, Pv, signed⟩
       PROVE  GuR(B)′
  BY ⟨2⟩5
⟨2⟩6.CASE UNCHANGED ⟨fr, nfr, Pv, signed⟩
  BY ⟨2⟩6
⟨2⟩7. QED
  BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6 DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH

** Key invariants and properties
Two sets of peers satisfying the guard GuR do have an honest peer in common
LEMMA TIntersecPeers ≜ IntersecPeers
⟨1⟩2. (threshold < 0) ∨ (threshold ≥ 0)BY ThresholdOK DEF ThresholdOK
```

$\langle 1\rangle$a.CASE $(threshold < 0)$ This case quickly leads to a contradiction
  BY $\langle 1\rangle$a, $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
$\langle 1\rangle$b.CASE $(threshold \geq 0)$ This is the interesting case
  $\langle 2\rangle$00 SUFFICES ASSUME NEW $peersS1 \in$ SUBSET $peers$, NEW $peersS2 \in$ SUBSET $peers$,
    $\land\ Cardinality(peersS1) \geq threshold$
    $\land\ Cardinality(peersS2) \geq threshold$
    PROVE $\exists P \in (peersS1 \cap peersS2 \cap peersH)$: TRUE
    BY DEF $IntersecPeers$
Proof strategy: 1. We first prove that the intersection between $peersS1$ and $peersS2$ has at least threshold-2n peers
  $\langle 2\rangle$0. $n \in Nat \land threshold \in Nat \land nh \in Nat$
      BY $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
  $\langle 2\rangle$1. $Cardinality(peersS1 \cap peersS2) \geq (2 * threshold - n)$
    $\langle 3\rangle$0 $IsFiniteSet(peersH \cup peersD)$BY FS_Union, $FS\_Intersection$, $ThresholdOK$, $PeersOK$ DEF $Thresh$
    $\langle 3\rangle$00 $IsFiniteSet(peersS1) \land IsFiniteSet(peersS2)$BY $\langle 3\rangle$0, FS_Subset DEF $peers$
    $\langle 3\rangle$ $IsFiniteSet(peersS1) \land IsFiniteSet(peersS2) \land IsFiniteSet(peersS1 \cup peersS2) \land IsFiniteSet(peersS1$
      BY $\langle 3\rangle$00, $\langle 3\rangle$0, FS_Union, $FS\_Intersection$, $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$,
    $\langle 3\rangle$ $n \in Nat \land threshold \in Nat \land Cardinality(peersS1 \cup peersS2) \in Nat \land Cardinality(peersS1) \in Nat \land$
      BY $ThresholdOK$, $PeersOK$, $FS\_CardinalityType$ DEF $ThresholdOK$, $PeersOK$, $FS\_CardinalityType$
    $\langle 3\rangle$1 $Cardinality(peersS1 \cup peersS2) = Cardinality(peersS1) + Cardinality(peersS2) - Cardinality(peers$
    $\langle 3\rangle$2 $Cardinality(peersS1 \cup peersS2) \leq Cardinality(peers)$
      $\langle 4\rangle$1 $peersS1 \cup peersS2 \subseteq peers$BY DEF $peers$
      $\langle 4\rangle$ QED BY $\langle 4\rangle$1, FS_Subset
    $\langle 3\rangle$3 $Cardinality(peersS1) \geq threshold \land Cardinality(peersS2) \geq threshold$BY $\langle 2\rangle$00
    $\langle 3\rangle$4 $Cardinality(peersS1 \cap peersS2) \geq 2 * threshold - n$ BY $\langle 3\rangle$3, $\langle 3\rangle$2, $\langle 3\rangle$1, $PeersOK$ DEF $PeersOK$
    $\langle 3\rangle$ QED BY $\langle 3\rangle$4, $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
Proof strategy: 2. We now use $\langle 2\rangle$1 and assuptions about the threshold, n, and nh to conclude
  $\langle 2\rangle$2 $\land IsFiniteSet(peersS1 \cap peersS2) \land IsFiniteSet(peersS1 \cap peersS2 \cap peersH) \land IsFiniteSet(peers) \land Is$
    $\langle 3\rangle$1 $IsFiniteSet(peersH) \land IsFiniteSet(peersD)$BY $PeersOK$ DEF $PeersOK$
    $\langle 3\rangle$2 $IsFiniteSet(peers)$BY $\langle 3\rangle$1, FS_Union DEF $peers$
    $\langle 3\rangle$3 $IsFiniteSet(peersS1) \land IsFiniteSet(peersS2)$BY $\langle 3\rangle$2, FS_Subset
    $\langle 3\rangle$f. QED BY $FS\_Intersection$, $\langle 3\rangle$3, $\langle 3\rangle$2, $\langle 3\rangle$1
  $\langle 2\rangle$3. $Cardinality(peersS1 \cap peersS2) > n - nh$
    $\langle 3\rangle$ $(2 * threshold - n) > n - nh$
      BY $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
    $\langle 3\rangle$ $Cardinality(peersS1 \cap peersS2) \in Nat$BY $FS\_CardinalityType$, $\langle 2\rangle$2
    $\langle 3\rangle$ $threshold \in Nat \land n \in Nat \land nh \in Nat$BY $ThresholdOK$, $PeersOK$ DEF $ThresholdOK$, $PeersOK$
      $\langle 3\rangle$f QED BY $\langle 2\rangle$1
  $\langle 2\rangle$4. $(peersS1 \cap peersS2) \cap peersH \neq \{\}$
    $\langle 3\rangle$0 $(peersS1 \cap peersS2) \subseteq peers \land peersH \subseteq peers$BY $PeersOK$, $ThresholdOK$ DEF $peers$, $PeersOK$, T
    $\langle 3\rangle$1 $Cardinality(peers) = n \land Cardinality(peersH) = nh$BY $PeersOK$ DEF $PeersOK$
    $\langle 3\rangle$2 $Cardinality(peersS1 \cap peersS2) \in Nat \land Cardinality(peersH) \in Nat \land Cardinality(peers) \in Nat$BY
    $\langle 3\rangle$3 $Cardinality(peersS1 \cap peersS2) + Cardinality(peersH) > Cardinality(peers)$BY $\langle 3\rangle$1, $\langle 2\rangle$3, $\langle 3\rangle$2
    $\langle 3\rangle$f QED
      BY $\langle 3\rangle$0, $\langle 2\rangle$0, $\langle 3\rangle$3, $\langle 3\rangle$1, $FS\_MajoritiesIntersect$, $CardPeers$
  $\langle 2\rangle$f. QED

```
        BY ⟨2⟩2, ⟨2⟩4, FS_EmptySet
  ⟨1⟩f. QED
        BY ⟨1⟩a, ⟨1⟩b, ⟨1⟩2  DEF Cardinality

 Peers locally enforce FC
LEMMA TPeersLocalFC ≜ Protocol ⇒ □PeersLocalFC
⟨1⟩ USE  DEF PeersLocalFC, Inv1, TypeOK
⟨1⟩b. Init ∧ TypeOK ⇒ PeersLocalFC
  ⟨2⟩ SUFFICES ASSUME Init ∧ TypeOK,
                          NEW P ∈ peersH
                 PROVE   ∧ ∀ B ∈ signed[P] : extends(B, Pv[P])
                          ∧ ∀ B ∈ FRP(P) : B = Pv[P]
      BY  DEF PeersLocalFC
  ⟨2⟩ P ∈ peersBY  DEF peers
  ⟨2⟩ signed[P] = {} ∧ (FRP(P) ∩ FinalW) = {}
    ⟨3⟩1. signed[P] = {}
        BY  DEF Init
    ⟨3⟩2. FRP(P) = {}
      ⟨4⟩1 (signed[P] ∪ {Pv[P]}) = {B0}BY  DEF Init
      ⟨4⟩qed QED BY ⟨4⟩1, PhasesOK, WOK DEF Init, FinalW, FRP, PhasesOK, WOK, NFRP, phase
    ⟨3⟩3. QED
        BY ⟨3⟩1, ⟨3⟩2
  ⟨2⟩1. ∀ B ∈ signed[P] : extends(B, Pv[P])
      BY ExtendsRefl DEF Init, FRP, NFRP, FinalW
  ⟨2⟩2. ∀ B ∈ FRP(P) : B = Pv[P]
      BY ExtendsRefl DEF Init, FRP, NFRP, FinalW
  ⟨2⟩3. QED
      BY ⟨2⟩1, ⟨2⟩2
⟨1⟩i. TypeOK ∧ PeersLocalFC ∧ [Next]_⟨fr, nfr, Pv, signed⟩ ⇒ PeersLocalFC′
 ⟨2⟩ USE  DEF PeersLocalFC
 ⟨2⟩qed QED
   ⟨3⟩ SUFFICES ASSUME TypeOK ∧ PeersLocalFC ∧ [Next]_⟨fr, nfr, Pv, signed⟩,
                           NEW P ∈ peersH′
                  PROVE   ( ∧ ∀ B ∈ signed[P] : extends(B, Pv[P])
                             ∧ ∀ B ∈ FRP(P) : B = Pv[P])′
       BY  DEF PeersLocalFC
   ⟨3⟩ P ∈ peersH ∧ P ∈ peersBY  DEF peers
   ⟨3⟩ QED
     ⟨4⟩1. ASSUME NEW P_1 ∈ peersH,
                  NEW bu ∈ W,
                    ∧ extends(Pv[P_1], bu)
                  ∧ phase(Pv[P_1]) ≠ pf
                  ∧ Pv′ = [Pv EXCEPT ![P_1] = bu]
                  ∧ UNCHANGED ⟨fr, nfr, signed⟩
           PROVE   ( ∧ ∀ B ∈ signed[P] : extends(B, Pv[P])
```

$\land \forall B \in FRP(P) : B = Pv[P])'$

$\langle 5 \rangle\ P_1 \in peers$BY DEF $peers$

$\langle 5 \rangle$CASE $P\_1 = P$

$\langle 6 \rangle$CASE $FRP(P) = \{\}$

$\langle 7 \rangle$CASE $phase(bu) = pf$

$\langle 8 \rangle\ FRP(P)' = \{bu\}$BY $\langle 4 \rangle 1$ DEF FRP, $FinalW$, $NFRP$

$\langle 8 \rangle$qed QED

$\langle 9 \rangle 1.\ (\forall B \in signed[P] : extends(B, Pv[P]))'$

BY $\langle 4 \rangle 1$, $ExtendsTrans$ DEF FRP, $FinalW$, $NFRP$

$\langle 9 \rangle 2.\ (\forall B \in FRP(P) : B = Pv[P])'$

BY $\langle 4 \rangle 1$ DEF FRP, $FinalW$, $NFRP$

$\langle 9 \rangle 3.$ QED

BY $\langle 9 \rangle 1$, $\langle 9 \rangle 2$

$\langle 7 \rangle$CASE $phase(bu) \neq pf$

$\langle 8 \rangle\ FRP(P)' = \{\}$BY $\langle 4 \rangle 1$ DEF FRP, $FinalW$, $NFRP$

$\langle 8 \rangle$qed QED

$\langle 9 \rangle 1.\ (\forall B \in signed[P] : extends(B, Pv[P]))'$

BY $\langle 4 \rangle 1$, $ExtendsTrans$ DEF FRP, $FinalW$, $NFRP$

$\langle 9 \rangle 2.\ (\forall B \in FRP(P) : B = Pv[P])'$

BY $\langle 4 \rangle 1$ DEF FRP, $FinalW$, $NFRP$

$\langle 9 \rangle 3.$ QED

BY $\langle 9 \rangle 1$, $\langle 9 \rangle 2$

$\langle 7 \rangle$qed QED OBVIOUS

$\langle 6 \rangle$CASE $FRP(P) \neq \{\}$

$\langle 7 \rangle\ \exists B \in FRP(P) :$ TRUEOBVIOUS

$\langle 7 \rangle\ \exists B \in FRP(P) : B = Pv[P] \land phase(Pv[P]) = pf$BY DEF FRP, $FinalW$

$\langle 7 \rangle$qed QED BY $\langle 4 \rangle 1$

$\langle 6 \rangle$qed QED BY DEF FRP, $NFRP$, $FinalW$

$\langle 5 \rangle$qed QED BY $\langle 4 \rangle 1$ DEF FRP, $NFRP$, $FinalW$

$\langle 4 \rangle 2.$ ASSUME NEW $P\_1 \in peersH$,

NEW $bs \in W$,

$\land extends(bs, Pv[P\_1]) \land phase(bs) = phase(Pv[P\_1])$

$\land (phase(Pv[P\_1]) = pf \Rightarrow bs = Pv[P\_1])$

$\land signed' = [signed$ EXCEPT $![P\_1] = signed[P\_1] \cup \{bs\}]$

$\land$ UNCHANGED $\langle fr, nfr, Pv \rangle$

PROVE $(\land \forall B \in signed[P] : extends(B, Pv[P])$

$\land \forall B \in FRP(P) : B = Pv[P])'$

$\langle 5 \rangle\ P_1 \in peers$BY DEF $peers$

$\langle 5 \rangle$CASE $P\_1 \neq P$

$\langle 6 \rangle 1\ signed[P] = signed[P]'$BY $\langle 4 \rangle 2$ DEF FRP, $FinalW$, $NFRP$

$\langle 6 \rangle\ FRP(P) = FRP(P)' \land signed[P] = signed[P]' \land Pv[P] = Pv[P]'$BY $\langle 4 \rangle 2$, $\langle 6 \rangle 1$ DEF FRP, $FinalW$

$\langle 6 \rangle$ QED BY $\langle 4 \rangle 2$

$\langle 5 \rangle$CASE $P\_1 = P$

$\langle 6 \rangle$CASE $FRP(P) = \{\}$

$\langle 7 \rangle$CASE $phase(Pv[P\_1]) = pf$

$\langle 8 \rangle$ $phase(bs) = pf$ BY $\langle 4 \rangle 2$
$\langle 8 \rangle$ $bs = Pv[P_1]$BY $\langle 4 \rangle 2$
$\langle 8 \rangle$ $FRP(P)' = \{bs\}$BY $\langle 4 \rangle 1$ DEF FRP, $FinalW$, $NFRP$
$\langle 8 \rangle$qed QED
$\langle 9 \rangle 1.$ $(\forall\, B \in signed[P] : extends(B,\, Pv[P]))'$
BY $\langle 4 \rangle 2$, $ExtendsTrans$ DEF FRP, $FinalW$, $NFRP$
$\langle 9 \rangle 2.$ $(\forall\, B \in FRP(P) : B = Pv[P])'$
BY $\langle 4 \rangle 2$ DEF FRP, $FinalW$, $NFRP$
$\langle 9 \rangle 3.$ QED
BY $\langle 9 \rangle 2$, $\langle 4 \rangle 2$
$\langle 7 \rangle$CASE $phase(Pv[P\_1]) \neq pf$
$\langle 8 \rangle$ $phase(bs) \neq pf$BY $\langle 4 \rangle 2$
$\langle 8 \rangle$ $FRP(P)' = \{\}$BY $\langle 4 \rangle 2$ DEF FRP, $FinalW$, $NFRP$
$\langle 8 \rangle$qed QED
$\langle 9 \rangle 1.$ $(\forall\, B \in signed[P] : extends(B,\, Pv[P]))'$
BY $\langle 4 \rangle 2$, $ExtendsTrans$ DEF FRP, $FinalW$, $NFRP$
$\langle 9 \rangle 2.$ $(\forall\, B \in FRP(P) : B = Pv[P])'$
BY $\langle 4 \rangle 2$ DEF FRP, $FinalW$, $NFRP$
$\langle 9 \rangle 3.$ QED
BY $\langle 9 \rangle 1$, $\langle 4 \rangle 2$
$\langle 7 \rangle$qed QED OBVIOUS
$\langle 6 \rangle$CASE $FRP(P) \neq \{\}$
$\langle 7 \rangle$ $Pv[P] = Pv[P]'$BY $\langle 4 \rangle 2$
$\langle 7 \rangle$ $\exists\, B \in FRP(P) : \forall\, Bf \in FRP(P) : B = Bf \land B = Pv[P] \land phase(Pv[P]) = pf \land phase(bs) = pf$
$\langle 7 \rangle$ $extends(bs,\, Pv[P]')$BY $\langle 4 \rangle 2$
$\langle 7 \rangle$ $signed[P]' = signed[P] \cup \{bs\}$BY $\langle 4 \rangle 2$
$\langle 7 \rangle$qed QED
$\langle 8 \rangle 1.$ $(\forall\, B \in signed[P] : extends(B,\, Pv[P]))'$
$\langle 9 \rangle$ SUFFICES ASSUME NEW $B \in (signed[P])'$
PROVE $extends(B,\, Pv[P])'$
OBVIOUS
$\langle 9 \rangle$ QED
BY $\langle 4 \rangle 2$
$\langle 8 \rangle 2.$ $(\forall\, B \in FRP(P) : B = Pv[P])'$
$\langle 9 \rangle$ SUFFICES ASSUME NEW $B \in FRP(P)'$
PROVE $(B = Pv[P])'$
OBVIOUS
$\langle 9 \rangle$ $B = Pv[P]$BY $\langle 4 \rangle 2$ DEF FRP, $FinalW$, $NFRP$
$\langle 9 \rangle$ QED
BY $\langle 4 \rangle 2$
$\langle 8 \rangle 3.$ QED
BY $\langle 8 \rangle 1$, $\langle 8 \rangle 2$
$\langle 6 \rangle$qed QED BY DEF FRP, $NFRP$, $FinalW$
$\langle 5 \rangle$qed QED BY $\langle 4 \rangle 2$ DEF FRP, $NFRP$, $FinalW$
$\langle 4 \rangle 3.$ ASSUME NEW $P\_1 \in peersD$,

```
                      NEW bs ∈ W,
                        ∧ signed′ = [signed EXCEPT ![P_1] = signed[P_1] ∪ {bs}]
                      ∧ UNCHANGED ⟨fr, nfr, Pv⟩
              PROVE  ( ∧ ∀ B ∈ signed[P] : extends(B, Pv[P])
                       ∧ ∀ B ∈ FRP(P) : B = Pv[P])′
          ⟨5⟩ P_1 ∉ peersH BY PeersOK DEF PeersOK
          ⟨5⟩qed QED BY ⟨4⟩3  DEF FRP, NFRP, FinalW
        ⟨4⟩4. ASSUME NEW bu ∈ W,
                      NEW R ∈ readers,
                      ∧ GuR(bu)
                      ∧ nfr′ = [nfr EXCEPT ![R] = nfr[R] ∪ {bu}]
                      ∧ UNCHANGED ⟨fr, Pv, signed⟩
              PROVE  ( ∧ ∀ B ∈ signed[P] : extends(B, Pv[P])
                       ∧ ∀ B ∈ FRP(P) : B = Pv[P])′
          BY ⟨4⟩4  DEF FRP, NFRP, FinalW
        ⟨4⟩5. ASSUME NEW bu ∈ W,
                      NEW R ∈ readers,
                      ∧ GuR(bu) ∧ phase(bu) = pf
                      ∧ fr′ = [fr EXCEPT ![R] = fr[R] ∪ {bu}]
                      ∧ UNCHANGED ⟨nfr, Pv, signed⟩
              PROVE  ( ∧ ∀ B ∈ signed[P] : extends(B, Pv[P])
                       ∧ ∀ B ∈ FRP(P) : B = Pv[P])′
          BY ⟨4⟩5  DEF FRP, NFRP, FinalW
        ⟨4⟩6.CASE UNCHANGED ⟨fr, nfr, Pv, signed⟩
          BY ⟨4⟩6  DEF FRP, NFRP, FinalW
        ⟨4⟩7. QED
          BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4, ⟨4⟩5, ⟨4⟩6  DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH
⟨1⟩qed QED BY ⟨1⟩b, ⟨1⟩i, Invariance1, PTL DEF Protocol, Inv1, TypeOK

 Peers locally enforce FA
LEMMA TPeersLocalFA ≜ Protocol ⇒ □PeersLocalFA
⟨1⟩ USE  DEF PeersLocalFA, Inv1, TypeOK
⟨1⟩b. Init ∧ TypeOK ⇒ PeersLocalFA
  ⟨2⟩ SUFFICES ASSUME Init ∧ TypeOK,
                            NEW P ∈ peersH
                     PROVE  FA_param(FRP(P),
                                      NFRP(P))
    BY  DEF PeersLocalFA
   ⟨2⟩ USE  DEF FRP, NFRP
   ⟨2⟩ P ∈ peers BY PeersOK DEF PeersOK, peers
   ⟨2⟩ signed[P] = {} BY  DEF Init
   ⟨2⟩ signed[P] ∩ {B ∈ W : phase(B) = pf} = {} BY  DEF Init
   ⟨2⟩1. (signed[P] ∩ {B ∈ W : phase(B) = pf}) = {}  ∨  ∃ Bf ∈ (signed[P] ∩ {B ∈ W : phase(B) = pf}) : (sig
     ⟨3⟩ QED BY  DEF Init, FA_param
   ⟨2⟩2. ∀ Bf ∈ (signed[P] ∩ {B ∈ W : phase(B) = pf}) : ∀ B ∈ (signed[P]) : extends(B, Bf)
```

$\langle 3 \rangle$ QED BY DEF $Init$, FA_param

$\langle 2 \rangle 11.\ FRP(P) = \{\} \ \lor\ \exists\, Bf \in FRP(P) : FRP(P) = \{Bf\}$

BY DEF FA_param

$\langle 2 \rangle 21.\ \forall\, Bf \in FRP(P) : \forall\, B \in NFRP(P) : extends(B,\ Bf)$

BY $ExtendsRefl$ DEF FA_param, $ExtendsRefl$

$\langle 2 \rangle 3.$ QED

BY $\langle 2 \rangle 11$, $\langle 2 \rangle 21$ DEF FA_param

$\langle 1 \rangle$i. $TypeOK \land PeersLocalFA \quad \land PeersLocalFC \land [Next]_{\langle fr,\ nfr,\ Pv,\ signed \rangle} \Rightarrow PeersLocalFA'$

$\langle 2 \rangle$ SUFFICES ASSUME $TypeOK \land PeersLocalFA \land PeersLocalFC \land [Next]_{\langle fr,\ nfr,\ Pv,\ signed \rangle}$,

NEW $P \in peersH'$

PROVE $FA\_param(FRP(P),$

$NFRP(P))'$

BY DEF $PeersLocalFA$

$\langle 2 \rangle\ P \in peersH \land P \in peers$BY DEF $peers$

$\langle 2 \rangle$ USE DEF $PeersLocalFC$

$\langle 2 \rangle$qed. QED

$\langle 3 \rangle 1.$ ASSUME NEW $P\_1 \in peersH$,

NEW $bu \in W$,

$\land\ extends(Pv[P\_1],\ bu)$

$\land\ phase(Pv[P\_1]) \neq pf$

$\land\ Pv' = [Pv$ EXCEPT $![P\_1] = bu]$

$\land$ UNCHANGED $\langle fr,\ nfr,\ signed \rangle$

PROVE $FA\_param(FRP(P),$

$NFRP(P))'$

$\langle 5 \rangle\ P_1 \in peers$BY DEF $peers$

$\langle 5 \rangle$CASE $P\_1 = P$

$\langle 6 \rangle$CASE $FRP(P) = \{\}$

$\langle 7 \rangle$CASE $phase(bu) = pf$

$\langle 8 \rangle\ FRP(P)' = \{bu\}$BY $\langle 3 \rangle 1$ DEF FRP, $FinalW$, $NFRP$

$\langle 8 \rangle$qed QED

$\langle 9 \rangle 1.\ (\forall\, B \in signed[P] : extends(B,\ Pv[P]))'$

BY $\langle 3 \rangle 1$, $ExtendsTrans$ DEF FRP, $FinalW$, $NFRP$

$\langle 9 \rangle 2.\ (\forall\, B \in FRP(P) : B = Pv[P])'$

BY $\langle 3 \rangle 1$ DEF FRP, $FinalW$, $NFRP$

$\langle 9 \rangle\ FRP(P)' = \{bu\}$BY $\langle 9 \rangle 1$, $\langle 9 \rangle 2$, $\langle 3 \rangle 1$

$\langle 9 \rangle\ \forall\, B \in NFRP(P)' : extends(B,\ bu)$

$\langle 10 \rangle\ NFRP(P)' \subseteq NFRP(P) \cup \{bu\}$BY $\langle 3 \rangle 1$ DEF $NFRP$, FRP, $FinalW$

$\langle 10 \rangle\ \forall\, B \in NFRP(P) : extends(B,\ bu)$

$\langle 11 \rangle$ SUFFICES ASSUME NEW $B \in NFRP(P)$

PROVE $extends(B,\ bu)$

OBVIOUS

$\langle 11 \rangle\ B \in W \land Pv[P] \in W$BY DEF $NFRP$

$\langle 11 \rangle\ extends(B,\ Pv[P])$

$\langle 12 \rangle$CASE $B = Pv[P]$BY $ExtendsRefl$

$\langle 12 \rangle$CASE $B \in NFRP(P)$BY DEF $NFRP$

$\langle 12\rangle$ QED BY DEF $PeersLocalFA$, $ExtendsTrans$, FA_param
$\langle 11\rangle$ QED BY $ExtendsTrans$, $\langle 3\rangle 1$
$\langle 10\rangle$ $extends(bu, bu)$BY $ExtendsRefl$
$\langle 10\rangle$qed QED BY $\langle 9\rangle 1$, $\langle 9\rangle 2$, $\langle 3\rangle 1$ DEF $PeersLocalFC$
$\langle 9\rangle 3.$ QED
BY $\langle 9\rangle 1$, $\langle 9\rangle 2$ DEF FA_param
$\langle 7\rangle$CASE $phase(bu) \neq pf$
$\langle 8\rangle$ $FRP(P)' = \{\}$BY $\langle 3\rangle 1$ DEF FRP, $FinalW$, $NFRP$
$\langle 8\rangle$qed QED
$\langle 9\rangle 1.$ $(\forall B \in signed[P] : extends(B, Pv[P]))'$
BY $\langle 3\rangle 1$, $ExtendsTrans$ DEF FRP, $FinalW$, $NFRP$
$\langle 9\rangle 2.$ $(\forall B \in FRP(P) : B = Pv[P])'$
BY $\langle 3\rangle 1$ DEF FRP, $FinalW$, $NFRP$
$\langle 9\rangle 3.$ QED
BY $\langle 9\rangle 1$, $\langle 9\rangle 2$ DEF FA_param
$\langle 7\rangle$qed QED OBVIOUS
$\langle 6\rangle$CASE $FRP(P) \neq \{\}$
$\langle 7\rangle$ $\exists B \in FRP(P) :$ TRUEOBVIOUS
$\langle 7\rangle$ $\exists B \in FRP(P) : B = Pv[P] \wedge phase(Pv[P]) = pf$BY DEF FRP, $FinalW$
$\langle 7\rangle$qed QED BY $\langle 3\rangle 1$
$\langle 6\rangle$qed QED BY DEF FRP, $NFRP$, $FinalW$
$\langle 5\rangle$qed QED BY $\langle 3\rangle 1$ DEF FRP, $NFRP$, $FinalW$
$\langle 3\rangle 2.$ ASSUME NEW $P\_1 \in peersH$,
NEW $bs \in W$,
$\wedge\ extends(bs, Pv[P\_1]) \wedge phase(bs) = phase(Pv[P\_1])$
$\wedge\ (phase(Pv[P\_1]) = pf \Rightarrow bs = Pv[P\_1])$
$\wedge\ signed' = [signed$ EXCEPT $![P\_1] = signed[P\_1] \cup \{bs\}]$
$\wedge$ UNCHANGED $\langle fr, nfr, Pv\rangle$
PROVE $FA\_param(FRP(P),$
$NFRP(P))'$
BY $\langle 3\rangle 2$ DEF FRP, $NFRP$, $FinalW$, FA_param
$\langle 3\rangle 3.$ ASSUME NEW $P\_1 \in peersD$,
NEW $bs \in W$,
$\wedge\ signed' = [signed$ EXCEPT $![P\_1] = signed[P\_1] \cup \{bs\}]$
$\wedge$ UNCHANGED $\langle fr, nfr, Pv\rangle$
PROVE $FA\_param(FRP(P),$
$NFRP(P))'$
$\langle 4\rangle$ $P_1 \notin peersH$BY $PeersOK$ DEF $PeersOK$
$\langle 4\rangle$qed QED BY $\langle 3\rangle 3$ DEF FRP, $NFRP$, $FinalW$
$\langle 3\rangle 4.$ ASSUME NEW $bu \in W$,
NEW $R \in readers$,
$\wedge\ GuR(bu)$
$\wedge\ nfr' = [nfr$ EXCEPT $![R] = nfr[R] \cup \{bu\}]$
$\wedge$ UNCHANGED $\langle fr, Pv, signed\rangle$
PROVE $FA\_param(FRP(P),$

```
                              NFRP(P))′
    BY ⟨3⟩4  DEF FRP, NFRP, FinalW, FA_param
  ⟨3⟩5. ASSUME NEW bu ∈ W,
               NEW R ∈ readers,
               ∧ GuR(bu) ∧ phase(bu) = pf
               ∧ fr′ = [fr EXCEPT ![R] = fr[R] ∪ {bu}]
               ∧ UNCHANGED ⟨nfr, Pv, signed⟩
        PROVE  FA_param(FRP(P),
                              NFRP(P))′
    BY ⟨3⟩5  DEF FRP, NFRP, FinalW, FA_param
  ⟨3⟩6.CASE UNCHANGED ⟨fr, nfr, Pv, signed⟩
    BY ⟨3⟩6  DEF FRP, NFRP, FinalW, FA_param
  ⟨3⟩7. QED
    BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6  DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH
⟨1⟩f. QED BY ⟨1⟩b, ⟨1⟩i, Invariance1, PTL, TPeersLocalFC DEF Protocol, Inv1, TypeOK

 Preservation of Gu for all read contents and final contents have phase pf
LEMMA TReadersLocalGu ≜ Protocol ⇒ □ReadersLocalGu
⟨1⟩ USE DEF ReadersLocalGu, Inv1, TypeOK
⟨1⟩b. Init ∧ TypeOK ⇒ ReadersLocalGuBY DEF Init
⟨1⟩i. TypeOK ∧ ReadersLocalGu ∧ [Next]_⟨fr, nfr, Pv, signed⟩ ⇒ ReadersLocalGu′
 ⟨2⟩ SUFFICES ASSUME TypeOK,
                     ReadersLocalGu,
                     NEW R ∈ readers′,
                     [Next]_⟨fr, nfr, Pv, signed⟩
              PROVE  ( ∧ ∀ B ∈ nfr[R] : GuR(B)
                       ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf)′
   BY DEF ReadersLocalGu
 ⟨2⟩1. ASSUME NEW P ∈ peersH,
                          ∃ bu ∈ W :
              ∧ extends(Pv[P], bu)
              ∧ phase(Pv[P]) ≠ pf
              ∧ Pv′ = [Pv EXCEPT ![P] = bu]
              ∧ UNCHANGED ⟨fr, nfr, signed⟩
       PROVE  ( ∧ ∀ B ∈ nfr[R] : GuR(B)
                ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf)′
   BY ⟨2⟩1 DEF GuR
 ⟨2⟩2. ASSUME NEW P ∈ peersH,
                          ∃ bs ∈ W :
              ∧ extends(bs, Pv[P]) ∧ phase(bs) = phase(Pv[P])
              ∧ (phase(Pv[P]) = pf ⇒ bs = Pv[P])
              ∧ signed′ = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
              ∧ UNCHANGED ⟨fr, nfr, Pv⟩
       PROVE  ( ∧ ∀ B ∈ nfr[R] : GuR(B)
                ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf)′
```

```
    BY ⟨2⟩2  DEF GuR
  ⟨2⟩3. ASSUME NEW P ∈ peersD,
                          ∃ bs ∈ W :
               ∧ signed′ = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
               ∧ UNCHANGED ⟨fr, nfr, Pv⟩
        PROVE  ( ∧ ∀ B ∈ nfr[R] : GuR(B)
                 ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf )′
    BY ⟨2⟩3  DEF GuR
  ⟨2⟩4. ASSUME NEW bu ∈ W,
               NEW R_1 ∈ readers,
               ∧ GuR(bu)
               ∧ nfr′ = [nfr EXCEPT ![R_1] = nfr[R_1] ∪ {bu}]
               ∧ UNCHANGED ⟨fr, Pv, signed⟩
        PROVE  ( ∧ ∀ B ∈ nfr[R] : GuR(B)
                 ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf )′
    BY ⟨2⟩4  DEF GuR
  ⟨2⟩5. ASSUME NEW bu ∈ W,
               NEW R_1 ∈ readers,
               ∧ GuR(bu) ∧ phase(bu) = pf
               ∧ fr′ = [fr EXCEPT ![R_1] = fr[R_1] ∪ {bu}]
               ∧ UNCHANGED ⟨nfr, Pv, signed⟩
        PROVE  ( ∧ ∀ B ∈ nfr[R] : GuR(B)
                 ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf )′
    BY ⟨2⟩5  DEF GuR
  ⟨2⟩6.CASE UNCHANGED ⟨fr, nfr, Pv, signed⟩
    BY ⟨2⟩6  DEF GuR
  ⟨2⟩7. QED
    BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6  DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH
⟨1⟩f. QED BY ⟨1⟩b, ⟨1⟩i, Invariance1, PTL, TPeersLocalFC DEF Protocol, Inv1, TypeOK

 The previous properties imply ReaderAgreement that boils down to FA applied between two readers
LEMMA soundReaderAgreement ≜ TypeOK ∧ ReadersLocalGu ∧ PeersLocalFC ∧ PeersLocalFA ⇒ ReaderAgre
⟨1⟩ USE  DEF ReaderAgreement, TypeOK, BSfr, BSnfr
⟨1⟩qed QED
  ⟨2⟩ SUFFICES ASSUME TypeOK ∧ ReadersLocalGu ∧ PeersLocalFC ∧ PeersLocalFA,
                      NEW R1 ∈ readers, NEW R2 ∈ readers,
                      NEW B1 ∈ BSfr ∪ BSnfr,
                      NEW B2 ∈ BSfr
               PROVE  extends(B1, B2)
    BY  DEF ReaderAgreement
  ⟨2⟩1 GuR(B1) ∧ GuR(B2)BY  DEF ReadersLocalGu
  ⟨2⟩2 (B1 ∈ fr[R1] ⇒ phase(B1) = pf) ∧ (B2 ∈ fr[R2] ⇒ phase(B2) = pf)BY  DEF ReadersLocalGu
  ⟨2⟩ B1 ∈ W ∧ B2 ∈ WBY  DEF TypeOK
  ⟨2⟩ QED
    ⟨3⟩ SUFFICES ASSUME NEW PS1 ∈ SUBSET peers,
```

$\wedge\ Cardinality(PS1) \geq threshold$
$\wedge\ \forall P1 \in PS1 : B1 \in signed[P1],$
NEW $PS2 \in$ SUBSET $peers,$
$\wedge\ Cardinality(PS2) \geq threshold$
$\wedge\ \forall P2 \in PS2 : B2 \in signed[P2]$
PROVE $extends(B1, B2)$
BY $\langle 2\rangle 1$ DEF GuR
$\langle 3\rangle\ \exists Ph \in peersH : Ph \in PS1 \wedge Ph \in PS2$BY $TIntersecPeers$ DEF $IntersecPeers$
$\langle 3\rangle$qed QED
$\langle 4\rangle$ SUFFICES ASSUME NEW $Ph \in peersH,$
$Ph \in PS1 \wedge Ph \in PS2$
PROVE $extends(B1, B2)$
OBVIOUS
$\langle 4\rangle\ Ph \in peers$BY DEF $peers$
$\langle 4\rangle\ B1 \in signed[Ph] \wedge B2 \in signed[Ph]$OBVIOUS
$\langle 4\rangle\ phase(B2) = pf$BY DEF $ReadersLocalGu$
$\langle 4\rangle$ QED BY DEF $PeersLocalFA,\ FA\_param,\ FRP,\ NFRP,\ FinalW$

Therefore, $ReaderAgreement$ is an invariant of $Protocol$.
LEMMA $TReaderAgreement \triangleq Protocol \Rightarrow \Box ReaderAgreement$
BY $Invariance1,\ PTL,\ TPeersLocalFC,\ TPeersLocalFA,\ TReadersLocalGu,\ soundReaderAgreement$ DEF $Proto$

$ReaderAgreement$ and some previous invariants imply FA.
LEMMA $soundFA \triangleq ReaderAgreement \wedge ReadersLocalGu \wedge TypeOK \Rightarrow FA$
$\langle 1\rangle$ USE DEF $BSfr,\ BSnfr$
$\langle 1\rangle$ SUFFICES ASSUME $ReaderAgreement \wedge ReadersLocalGu \wedge TypeOK$
PROVE FA
OBVIOUS
$\langle 1\rangle 1$ UNION $\{fr[R] : R \in readers\} = \{\} \vee$ UNION $\{fr[R] : R \in readers\} \neq \{\}$OBVIOUS
$\langle 1\rangle 2$CASE UNION $\{fr[R] : R \in readers\} = \{\}$
$\langle 2\rangle 1.\ BSfr = \{\}\ \vee\ \exists Bf \in BSfr : BSfr = \{Bf\}$
BY $\langle 1\rangle 2$ DEF FA
$\langle 2\rangle 2.\ \forall Bf \in BSfr : \forall B \in BSnfr : extends(B, Bf)$
BY $\langle 1\rangle 2$ DEF FA
$\langle 2\rangle 3.$ QED
BY $\langle 2\rangle 1,\ \langle 2\rangle 2$ DEF FA
$\langle 1\rangle 3$CASE UNION $\{fr[R] : R \in readers\} \neq \{\}$
$\langle 2\rangle 1\ \exists Bf \in$ UNION $\{fr[R] : R \in readers\} :$
$\wedge\ \forall B \in$ UNION $\{nfr[R] : R \in readers\} : extends(B, Bf)$ FA (ii)
$\wedge$ UNION $\{fr[R] : R \in readers\} = \{Bf\}$
$\langle 3\rangle 1$ ASSUME NEW $Bf \in$ UNION $\{fr[R] : R \in readers\}$
PROVE $\wedge\ \forall B \in$ UNION $\{nfr[R] : R \in readers\} : extends(B, Bf)$ FA (ii)
$\wedge$ UNION $\{fr[R] : R \in readers\} = \{Bf\}$ FA (i)
$\langle 4\rangle$qed QED
$\langle 5\rangle 1.\ \forall B \in$ UNION $\{nfr[R] : R \in readers\} : extends(B, Bf)$

```
                    BY ⟨1⟩3  DEF ReaderAgreement, FA, TypeOK, ReadersLocalGu
                  ⟨5⟩2. UNION {fr[R] : R ∈ readers} = {Bf}
                    ⟨6⟩ ∃ R ∈ readers : Bf ∈ fr[R]OBVIOUS
                    ⟨6⟩ ASSUME NEW B ∈ UNION {fr[R] : R ∈ readers}PROVE  B = Bf
                      ⟨7⟩ ∃ R2 ∈ readers : B ∈ fr[R2]OBVIOUS
                      ⟨7⟩qed QED
                        ⟨8⟩ SUFFICES ASSUME NEW R2 ∈ readers,
                                            B ∈ fr[R2],
                                            NEW R ∈ readers,
                                            Bf ∈ fr[R]
                                     PROVE  B = Bf
                          OBVIOUS
                        ⟨8⟩ phase(Bf) = pf BY  DEF ReadersLocalGu
                        ⟨8⟩ phase(B) = pf BY  DEF ReadersLocalGu
                        ⟨8⟩ extends(B, Bf) ∧ extends(Bf, B)
                          BY antiSymEx DEF ReaderAgreement
                        ⟨8⟩ QED BY antiSymEx DEF TypeOK
                    ⟨6⟩ QED
                    BY ⟨1⟩3  DEF  FA, TypeOK
                  ⟨5⟩3. QED
                    BY ⟨5⟩1, ⟨5⟩2
              ⟨3⟩2 ∃ Bf ∈ UNION {fr[R] : R ∈ readers} : TRUEBY ⟨1⟩3
              ⟨3⟩qed QED BY ⟨1⟩3, ⟨3⟩1, ⟨3⟩2  DEF FA, TypeOK
          ⟨2⟩f QED BY ⟨2⟩1, ⟨1⟩3  DEF FA
  ⟨1⟩ QED
    BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3

 ** Final theorem: final-agreement (FA) is an invariant of our protocol, specified as Spec.
THEOREM TFA ≜ Protocol ⇒ □FA
  BY soundFA, PTL, TReaderAgreement, TReadersLocalGu, Invariance1 DEF TReaderAgreement, TReadersL
```

\ * Modification History
\ * Last modified *Tue Oct* 22 19:06:22 *CEST* 2019 by *anonymous*
\ * Created *Thu Apr* 04 11:50:05 *CEST* 2019 by anonymous