

```

1 |----- MODULE BB_FA -----|
2 | EXTENDS Naturals, FiniteSets, TLAPS, FiniteSetTheorems |

    *****
    SPECIFICATION
    *****

7 |-----|

8 | *** Set up |
9 | CONSTANT W, | Uninterpreted set of BB contents, except that it contains a phase, see below |
10 |    B0, | A fixed, initial BB content in W |
11 |    extendsB(-, -), | Extension relation (will be axiomatized, could be interpreted as  $\subseteq$ ) |
12 |    peersH, | Set of Honest BB peers |
13 |    peersD, | Set of Dishonest (malicious) BB peers |
14 |    readers, | Set of readers |
15 |    threshold, | threshold  $\backslash \gamma$  |
16 |    n, | total number of peers (in peersH  $\cup$  peersD) |
17 |    nh, | number of honest peers (in peersH) |
18 |    pf | final phase (in Nat) |

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

25 | *** Assumptions |
26 | Phases  $\triangleq$  1 .. pf | Set of all the phases |
27 | Wb  $\triangleq$  {B[1] : B  $\in$  W} | We eventually assume that elements in W are in Wb  $\times$  Phases |
28 | peers  $\triangleq$  peersH  $\cup$  peersD |
29 | We assume that extends(., .) is transitive, reflexive, and anti-symmetric. |
30 | ExtendsOK  $\triangleq$   $\wedge \forall B1, B2, B3 \in Wb : extendsB(B1, B2) \wedge extendsB(B2, B3) \Rightarrow extendsB(B1, B3)$  |
31 |     $\wedge \forall B \in Wb : extendsB(B, B)$  |
32 |     $\wedge \forall B1, B2 \in Wb : extendsB(B1, B2) \wedge extendsB(B2, B1) \Rightarrow B1 = B2$  |
33 | We assume threshold meets the conditions of  $\backslash \gamma$ , see the paper |
34 | ThresholdOK  $\triangleq$   $\wedge threshold \in Nat$  | threshold is a natural number |
35 |     $\wedge nh > 2 * (n - threshold)$  |  $\backslash \gamma$  requirement (sanity check: TLC finds an attack without this) |
36 |     $\wedge threshold \leq n$  | threshold cannot be greater than the number of peers |
37 | WOK  $\triangleq$   $\wedge W \subseteq Wb \times Phases$  | BB contents are represented as a content in Wb with a phase in Phases |
38 |     $\wedge B0 \in W$  | the initial BB content is in W |
39 |     $\wedge B0[2] = 1$  | and has 1 as phase: the initial phase |
40 |     $\wedge \forall B1, B2 \in W : B1[1] = B2[1] \Rightarrow B1 = B2$  | equality of BB contents implies equality of their phases |
41 | PeersOK  $\triangleq$   $\wedge n \in Nat \wedge nh \in Nat$  |
42 |     $\wedge IsFiniteSet(peersD) \wedge IsFiniteSet(peersH)$  |
43 |     $\wedge nh = Cardinality(peersH)$  | nh is the number of honest peers (in peersH) |
44 |     $\wedge n = Cardinality(peers)$  | n is the number of all peers (in peersH  $\cup$  peersD) |
45 |     $\wedge peersH \cap peersD = \{\}$  | a peers is honest XOR dishonest (malicious) |
46 | PhasesOK  $\triangleq$   $\wedge pf \in Nat$  | there is a final phase |

```

47 $\wedge pf > 1$ which is not the initial phase (1)

48 ASSUME *ExtendsOK*

49 ASSUME *ThresholdOK*

50 ASSUME *WOK*

51 ASSUME *PeersOK*

52 ASSUME *PhasesOK*

54 *** Type correctness invariant

55 $TypeOK \triangleq \wedge fr \in [readers \rightarrow \text{SUBSET } W]$

56 $\wedge nfr \in [readers \rightarrow \text{SUBSET } W]$

57 $\wedge Pv \in [peersH \rightarrow W]$

58 $\wedge signed \in [peers \rightarrow \text{SUBSET } W]$

60 *** Helping functions

61 $phase(B) \triangleq B[2]$ Phase of a *BB* content

62 $extends(B1, B2) \triangleq extendsB(B1[1], B2[1])$ Lift *extendsB* to *W*

64

66 *** Initial states specification

67 $Init \triangleq \wedge fr = [r \in readers \mapsto \{\}]$

68 $\wedge nfr = [r \in readers \mapsto \{\}]$

69 $\wedge Pv = [P \in peersH \mapsto B0]$ the initial honest peers's view is *B0*

70 $\wedge signed = [P \in peers \mapsto \{\}]$

72 *** Guards

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

74 $GuR(B) \triangleq \exists peersS \in \text{SUBSET } peers :$

75 $\wedge Cardinality(peersS) \geq threshold$

76 $\wedge \forall P \in peersS : B \in signed[P]$

78 *** Events

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

80 $UpdatePH \triangleq \exists P \in peersH : \exists bu \in W :$

81 $\wedge extends(Pv[P], bu)$ this encodes the restriction on $\backslash \text{cup_B}$; i.e., $extends(B, B \cup B')$

82 $\wedge phase(Pv[P]) \neq pf$ no more update once a final *BB* content has been reached

83 $\wedge Pv' = [Pv \text{ EXCEPT } ![P] = bu]$

84 $\wedge \text{UNCHANGED } \langle fr, nfr, signed \rangle$

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

87 $SignPH \triangleq \exists P \in peersH : \exists bs \in W :$

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

89 $\wedge extends(bs, Pv[P]) \wedge phase(bs) = phase(Pv[P])$

90 $\wedge (phase(Pv[P]) = pf \Rightarrow bs = Pv[P])$

91 $\wedge signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$

92 $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$

94 *SignPD*: An dishonest *BB* peer can sign ANY content (*bs*) since he does not have to follow the specification.
 95 $SignPD \triangleq \exists P \in peersD : \exists bs \in W :$
 96 $\quad \wedge signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$
 97 $\quad \wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$

99 *ReadNonFinal*: A reader reads through Read-NonFinal and obtains *bu*. There is no explicit label *w.l.o.g.* (see above).
 100 $ReadNonFinal \triangleq \exists bu \in W : \exists R \in readers : \exists p \in Nat :$
 101 $\quad \wedge GuR(bu)$ this is the test that each reader performs when reading
 102 $\quad \wedge p = phase(bu)$ additionally, the reader checks that the read *BB* contents has the requested
 103 $\quad \wedge nfr' = [nfr \text{ EXCEPT } ![R] = nfr[R] \cup \{bu\}]$
 104 $\quad \wedge \text{UNCHANGED } \langle fr, Pv, signed \rangle$

106 *ReadFinal*: A reader reads through Read-Final.
 107 $ReadFinal \triangleq \exists bu \in W : \exists R \in readers :$
 108 $\quad \wedge GuR(bu)$ this is the test that each reader performs when reading
 109 $\quad \wedge phase(bu) = pf$ additionally, the reader checks that the read *BB* contents has the phase *pf*
 110 $\quad \wedge fr' = [fr \text{ EXCEPT } ![R] = fr[R] \cup \{bu\}]$
 111 $\quad \wedge \text{UNCHANGED } \langle nfr, Pv, signed \rangle$

113 *** State evolutions specification
 114 $Next \triangleq \vee UpdatePH$
 115 $\quad \vee SignPH$
 116 $\quad \vee SignPD$
 117 $\quad \vee ReadNonFinal$
 118 $\quad \vee ReadFinal$

120 *** The protocol is defined with *Init* describing initial states and with *Next* describing state evolutions (plus stuttering steps).
 121 $Protocol \triangleq Init \wedge \Box [Next]_{\langle fr, nfr, Pv, signed \rangle}$

123 *** We prove below that final-agreement (*FA*) is an invariant of Spec. *FA* is encoded as follows (see *FA*).
 124 $BSfr \triangleq \text{UNION } \{fr[R] : R \in readers\}$ set of all final read *BB* contents
 125 $BSnfr \triangleq \text{UNION } \{nfr[R] : R \in readers\}$ set of all read *BB* contents
 126 $FA \triangleq \wedge (BSfr = \{\}) \vee \exists Bf \in BSfr : BSfr = \{Bf\})$ *FA* (i)
 127 $\quad \wedge \forall Bf \in BSfr : \forall B \in BSnfr : extends(B, Bf)$ *FA* (ii)

130 |-----|
 131 | PROOFS |
 132 |-----|

 PROPERTY STATEMENTS

137 |-----|
 138 | Parametrized *FA* (will help *w.r.t.* modularity)
 139 $FA_param(FR, NFR) \triangleq \wedge (FR = \{\}) \vee \exists Bf \in FR : FR = \{Bf\})$
 140 $\quad \wedge \forall Bf \in FR : \forall B \in NFR : extends(B, Bf)$

141 $FinalW \triangleq \{B \in W : phase(B) = pf\}$ BB contents having the final phase *pf*
 142 $NFRP(P) \triangleq signed[P] \cup \{Pv[P]\}$ non-final content from a peer's perspective (*P*)
 143 $FRP(P) \triangleq NFRP(P) \cap FinalW$ final content from a peer's perspective (*P*)

 145 *** Key invariants and properties for the final proof
 146 (for LEMMA 2) [Invariant] Honest peers locally enforce *FC*
 147 $PeersLocalFC \triangleq$
 148 $\forall P \in peersH : \wedge \forall B \in signed[P] : extends(B, Pv[P])$
 149 $\wedge \forall B \in FRP(P) : B = Pv[P]$

 151 (for LEMMA 3) [Invariant] Honest peers locally enforce *FA*
 152 $PeersLocalFA \triangleq$
 153 $\forall P \in peersH : FA_param(FRP(P),$
 154 $NFRP(P))$

 156 (for LEMMA 4,7) [Invariant] Any reader's read enforces *GuR* and phase restriction
 157 $ReadersLocalGu \triangleq$
 158 $\forall R \in readers : \wedge \forall B \in nfr[R] : GuR(B)$
 159 $\wedge \forall B \in fr[R] : GuR(B) \wedge phase(B) = pf$

 161 (for LEMMA 1) Threshold assumptions make it so that there always is an honest peer in two valid sets of peers
 162 $IntersecPeers \triangleq$
 163 $\forall peersS1, peersS2 \in SUBSET\ peers :$
 164 $(\wedge Cardinality(peersS1) \geq threshold$
 165 $\wedge Cardinality(peersS2) \geq threshold$
 166 $) \Rightarrow \exists Ph \in (peersS1 \cap peersS2 \cap peersH) : TRUE$ this gives us some honest peer *Ph* in the intersection

 168 (for LEMMA 5 – 7) [Invariant] Any final *BB* read content extends any other read *BB* content.
 169 $ReaderAgreement \triangleq$
 170 $\forall R1, R2 \in readers :$
 171 $\forall B1 \in (BSfr \cup BSnfr) :$
 172 $\forall B2 \in BSfr : extends(B1, B2)$

 174 *** Basic and simple invariants
 175 $Inv1 \triangleq TypeOK$
 176 $InvGuPreservation \triangleq \forall B \in W : (Inv1 \wedge GuR(B) \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle} \Rightarrow GuR(B)')$

 CLAIMS AND PROOFS

182 |-----|

183 ** Basic properties

184 PROPOSITION $eqSingleton \triangleq$ ASSUME NEW $S1 \in SUBSET\ W$, NEW $S2 \in SUBSET\ W$, NEW $B1 \in S1$, NEW $B2$
 185 OBVIOUS
 186 PROPOSITION $antiSymEx \triangleq$ ASSUME NEW $B1 \in W$, NEW $B2 \in W$, $extends(B1, B2)$, $extends(B2, B1)$ PROV
 187 BY $ExtendsOK$, WOK DEF $ExtendsOK$, $extends$, Wb , WOK

188 PROPOSITION $equSets \triangleq$ ASSUME NEW $BS1 \in SUBSET\ W$, NEW $BS2 \in SUBSET\ W$ PROVE $(BS1 \neq \{\} \wedge BS2$
189 $\langle 1 \rangle$ SUFFICES ASSUME $BS1 \neq \{\} \wedge BS2 \neq \{\} \wedge \forall B1 \in BS1 : \forall B2 \in BS2 : B1 = B2$
190 PROVE $BS1 = BS2$
191 OBVIOUS
192 $\langle 1 \rangle 1 \forall B1 \in BS1 : B1 \in BS2$ OBVIOUS
193 $\langle 1 \rangle 2 \forall B1 \in BS1 : B1 \in BS2$ OBVIOUS
194 $\langle 1 \rangle$ f QED BY $\langle 1 \rangle 1, \langle 1 \rangle 2$
195 PROPOSITION $CardPeers \triangleq IsFiniteSet(peers) \wedge Cardinality(peers) = n$
196 $\langle 1 \rangle 1. IsFiniteSet(peers)$
197 BY $PeersOK, FS_Union$ DEF $PeersOK, peers$
198 $\langle 1 \rangle 2. Cardinality(peers) = n$
199 BY $ThresholdOK, PeersOK$ DEF $ThresholdOK, PeersOK, peers$
200 $\langle 1 \rangle 3.$ QED
201 BY $\langle 1 \rangle 1, \langle 1 \rangle 2$
202 PROPOSITION $ExtendsRefl \triangleq$ ASSUME NEW $B \in W$ PROVE $extends(B, B)$
203 BY $ExtendsOK, WOK$ DEF $ExtendsOK, extends, Wb, WOK$
204 PROPOSITION $ExtendsRefl2 \triangleq$ ASSUME NEW $B1 \in W$, NEW $B2 \in W$ PROVE $B1 = B2 \Rightarrow extends(B2, B1)$
205 BY $ExtendsOK, WOK$ DEF $ExtendsOK, extends, Wb, WOK$
206 PROPOSITION $ExtendsTrans \triangleq$ ASSUME NEW $B1 \in W$, NEW $B2 \in W$, NEW $B3 \in W$, $extends(B1, B2), exte$
207 BY $ExtendsOK$ DEF $ExtendsOK, extends, Wb$
208 PROPOSITION $TExistsPeer \triangleq \exists P \in peersH : TRUE$
209 $\langle 1 \rangle 1\ nh > 0$
210 $\langle 2 \rangle\ n \geq threshold$
211 BY $ThresholdOK, PeersOK$ DEF $ThresholdOK, PeersOK$
212 $\langle 2 \rangle$ f QED
213 BY $ThresholdOK, PeersOK$ DEF $ThresholdOK, PeersOK$
214 $\langle 1 \rangle$ f QED
215 BY $\langle 1 \rangle 1, PeersOK, FS_EmptySet$ DEF $ThresholdOK, PeersOK$

217 PROPOSITION $Invariance1 \triangleq Protocol \Rightarrow \square Inv1$
218 $\langle 1 \rangle$ USE DEF $Inv1, TypeOK$
219 $\langle 1 \rangle$ init $Init \Rightarrow TypeOK$ BY WOK DEF $Init, WOK$
220 $\langle 1 \rangle$ induction $TypeOK \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle} \Rightarrow TypeOK'$
221 $\langle 2 \rangle$ SUFFICES ASSUME $TypeOK,$
222 $[Next]_{\langle fr, nfr, Pv, signed \rangle}$
223 PROVE $TypeOK'$
224 OBVIOUS
225 $\langle 2 \rangle 1.$ ASSUME NEW $P \in peersH,$
226 NEW $bu \in W,$
227 $\wedge extends(Pv[P], bu)$
228 $\wedge phase(Pv[P]) \neq pf$
229 $\wedge Pv' = [Pv\ EXCEPT\ ![P] = bu]$
230 $\wedge UNCHANGED\ \langle fr, nfr, signed \rangle$
231 PROVE $TypeOK'$
232 BY $\langle 2 \rangle 1, WOK$ DEF $Init, WOK$

233 $\langle 2 \rangle 2$. ASSUME NEW $P \in \text{peersH}$,
234 NEW $bs \in W$,
235 $\wedge \text{extends}(bs, Pv[P])$
236 $\wedge (\text{phase}(Pv[P]) = pf \Rightarrow bs = Pv[P])$
237 $\wedge \text{signed}' = [\text{signed} \text{ EXCEPT } ![P] = \text{signed}[P] \cup \{bs\}]$
238 $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$
239 PROVE TypeOK'
240 BY $\langle 2 \rangle 2$, WOK DEF Init , WOK
241 $\langle 2 \rangle 3$. ASSUME NEW $P \in \text{peersD}$,
242 NEW $bs \in W$,
243 $\wedge \text{signed}' = [\text{signed} \text{ EXCEPT } ![P] = \text{signed}[P] \cup \{bs\}]$
244 $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$
245 PROVE TypeOK'
246 BY $\langle 2 \rangle 3$, WOK DEF Init , WOK
247 $\langle 2 \rangle 4$. ASSUME NEW $bu \in W$,
248 NEW $R \in \text{readers}$,
249 $\wedge \text{GuR}(bu)$
250 $\wedge nfr' = [nfr \text{ EXCEPT } ![R] = nfr[R] \cup \{bu\}]$
251 $\wedge \text{UNCHANGED } \langle fr, Pv, \text{signed} \rangle$
252 PROVE TypeOK'
253 BY $\langle 2 \rangle 4$, WOK DEF Init , WOK
254 $\langle 2 \rangle 5$. ASSUME NEW $bu \in W$,
255 NEW $R \in \text{readers}$,
256 $\wedge \text{GuR}(bu) \wedge \text{phase}(bu) = pf$
257 $\wedge fr' = [fr \text{ EXCEPT } ![R] = fr[R] \cup \{bu\}]$
258 $\wedge \text{UNCHANGED } \langle nfr, Pv, \text{signed} \rangle$
259 PROVE TypeOK'
260 BY $\langle 2 \rangle 5$, WOK DEF Init , WOK
261 $\langle 2 \rangle 6$. CASE UNCHANGED $\langle fr, nfr, Pv, \text{signed} \rangle$
262 BY $\langle 2 \rangle 6$, WOK DEF Init , WOK
263 $\langle 2 \rangle 7$. QED
264 BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$ DEF Next , ReadFinal , ReadNonFinal , SignPD , SignPH , UpdatePH
265 $\langle 1 \rangle$ QED BY $\langle 1 \rangle \text{init}$, $\langle 1 \rangle \text{induction}$, PTL DEF Protocol

267 PROPOSITION $\text{GuPreservation} \triangleq \forall B \in W : (\text{Inv1} \wedge \text{GuR}(B) \wedge [\text{Next}]_{\langle fr, nfr, Pv, \text{signed} \rangle} \Rightarrow \text{GuR}(B)')$
268 $\langle 1 \rangle$ USE DEF Inv1 , TypeOK , GuR
269 $\langle 1 \rangle$ QED
270 $\langle 2 \rangle$ SUFFICES ASSUME NEW $B \in W$,
271 Inv1 ,
272 NEW $\text{peersS} \in \text{SUBSET } \text{peers}$,
273 $\wedge \text{Cardinality}(\text{peersS}) \geq \text{threshold}$
274 $\wedge \forall P \in \text{peersS} : B \in \text{signed}[P]$,
275 $[\text{Next}]_{\langle fr, nfr, Pv, \text{signed} \rangle}$
276 PROVE $\text{GuR}(B)'$
277 BY DEF GuR

```

278  ⟨2⟩1. ASSUME NEW  $P \in \text{peersH}$ ,
279          NEW  $bu \in W$ ,
280           $\wedge \text{extends}(Pv[P], bu)$ 
281           $\wedge \text{phase}(Pv[P]) \neq pf$ 
282           $\wedge Pv' = [Pv \text{ EXCEPT } ![P] = bu]$ 
283           $\wedge \text{UNCHANGED } \langle fr, nfr, signed \rangle$ 
284      PROVE  $GuR(B)'$ 
285      BY ⟨2⟩1
286  ⟨2⟩2. ASSUME NEW  $P \in \text{peersH}$ ,
287          NEW  $bs \in W$ ,
288           $\wedge \text{extends}(bs, Pv[P])$ 
289           $\wedge (\text{phase}(Pv[P]) = pf \Rightarrow bs = Pv[P])$ 
290           $\wedge signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$ 
291           $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$ 
292      PROVE  $GuR(B)'$ 
293      BY ⟨2⟩2
294  ⟨2⟩3. ASSUME NEW  $P \in \text{peersD}$ ,
295          NEW  $bs \in W$ ,
296           $\wedge signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$ 
297           $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$ 
298      PROVE  $GuR(B)'$ 
299      BY ⟨2⟩3
300  ⟨2⟩4. ASSUME NEW  $bu \in W$ ,
301          NEW  $R \in \text{readers}$ ,
302           $\wedge GuR(bu)$ 
303           $\wedge nfr' = [nfr \text{ EXCEPT } ![R] = nfr[R] \cup \{bu\}]$ 
304           $\wedge \text{UNCHANGED } \langle fr, Pv, signed \rangle$ 
305      PROVE  $GuR(B)'$ 
306      BY ⟨2⟩4
307  ⟨2⟩5. ASSUME NEW  $bu \in W$ ,
308          NEW  $R \in \text{readers}$ ,
309           $\wedge GuR(bu) \wedge \text{phase}(bu) = pf$ 
310           $\wedge fr' = [fr \text{ EXCEPT } ![R] = fr[R] \cup \{bu\}]$ 
311           $\wedge \text{UNCHANGED } \langle nfr, Pv, signed \rangle$ 
312      PROVE  $GuR(B)'$ 
313      BY ⟨2⟩5
314  ⟨2⟩6. CASE UNCHANGED  $\langle fr, nfr, Pv, signed \rangle$ 
315      BY ⟨2⟩6
316  ⟨2⟩7. QED
317      BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6 DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH

319  ** Key invariants and properties
320  Two sets of peers satisfying the guard  $GuR$  do have an honest peer in common
321  LEMMA  $TIntersecPeers \triangleq IntersecPeers$ 
322  ⟨1⟩2.  $(threshold < 0) \vee (threshold \geq 0)$  BY ThresholdOK DEF ThresholdOK

```

323 $\langle 1 \rangle$ a.CASE ($threshold < 0$) This case quickly leads to a contradiction
 324 BY $\langle 1 \rangle$ a, *ThresholdOK*, *PeersOK* DEF *ThresholdOK*, *PeersOK*
 325 $\langle 1 \rangle$ b.CASE ($threshold \geq 0$) This is the interesting case
 326 $\langle 2 \rangle$ 00 SUFFICES ASSUME NEW $peersS1 \in \text{SUBSET } peers$, NEW $peersS2 \in \text{SUBSET } peers$,
 327 $\wedge \text{Cardinality}(peersS1) \geq threshold$
 328 $\wedge \text{Cardinality}(peersS2) \geq threshold$
 329 PROVE $\exists P \in (peersS1 \cap peersS2 \cap peersH) : \text{TRUE}$
 330 BY DEF *IntersecPeers*
 331 Proof strategy: 1. We first prove that the intersection between $peersS1$ and $peersS2$ has at least $threshold - 2n$ peers
 332 $\langle 2 \rangle$ 0. $n \in \text{Nat} \wedge threshold \in \text{Nat} \wedge nh \in \text{Nat}$
 333 BY *ThresholdOK*, *PeersOK* DEF *ThresholdOK*, *PeersOK*
 334 $\langle 2 \rangle$ 1. $\text{Cardinality}(peersS1 \cap peersS2) \geq (2 * threshold - n)$
 335 $\langle 3 \rangle$ 0 *IsFiniteSet*($peersH \cup peersD$) BY *FS_Union*, *FS_Intersection*, *ThresholdOK*, *PeersOK* DEF *Thresh*
 336 $\langle 3 \rangle$ 00 *IsFiniteSet*($peersS1$) \wedge *IsFiniteSet*($peersS2$) BY $\langle 3 \rangle$ 0, *FS_Subset* DEF *peers*
 337 $\langle 3 \rangle$ *IsFiniteSet*($peersS1$) \wedge *IsFiniteSet*($peersS2$) \wedge *IsFiniteSet*($peersS1 \cup peersS2$) \wedge *IsFiniteSet*($peersS1$
 338 BY $\langle 3 \rangle$ 00, $\langle 3 \rangle$ 0, *FS_Union*, *FS_Intersection*, *ThresholdOK*, *PeersOK* DEF *ThresholdOK*, *PeersOK*,
 339 $\langle 3 \rangle$ $n \in \text{Nat} \wedge threshold \in \text{Nat} \wedge \text{Cardinality}(peersS1 \cup peersS2) \in \text{Nat} \wedge \text{Cardinality}(peersS1) \in \text{Nat} \wedge$
 340 BY *ThresholdOK*, *PeersOK*, *FS_CardinalityType* DEF *ThresholdOK*, *PeersOK*, *FS_CardinalityType*
 341 $\langle 3 \rangle$ 1 $\text{Cardinality}(peersS1 \cup peersS2) = \text{Cardinality}(peersS1) + \text{Cardinality}(peersS2) - \text{Cardinality}(peers$
 342 $\langle 3 \rangle$ 2 $\text{Cardinality}(peersS1 \cup peersS2) \leq \text{Cardinality}(peers)$
 343 $\langle 4 \rangle$ 1 $peersS1 \cup peersS2 \subseteq peers$ BY DEF *peers*
 344 $\langle 4 \rangle$ QED BY $\langle 4 \rangle$ 1, *FS_Subset*
 345 $\langle 3 \rangle$ 3 $\text{Cardinality}(peersS1) \geq threshold \wedge \text{Cardinality}(peersS2) \geq threshold$ BY $\langle 2 \rangle$ 00
 346 $\langle 3 \rangle$ 4 $\text{Cardinality}(peersS1 \cap peersS2) \geq 2 * threshold - n$ BY $\langle 3 \rangle$ 3, $\langle 3 \rangle$ 2, $\langle 3 \rangle$ 1, *PeersOK* DEF *PeersOK*
 347 $\langle 3 \rangle$ QED BY $\langle 3 \rangle$ 4, *ThresholdOK*, *PeersOK* DEF *ThresholdOK*, *PeersOK*
 348 Proof strategy: 2. We now use $\langle 2 \rangle$ 1 and assumptions about the threshold, n , and nh to conclude
 349 $\langle 2 \rangle$ 2 \wedge *IsFiniteSet*($peersS1 \cap peersS2$) \wedge *IsFiniteSet*($peersS1 \cap peersS2 \cap peersH$) \wedge *IsFiniteSet*($peers$) \wedge *Is*
 350 $\langle 3 \rangle$ 1 *IsFiniteSet*($peersH$) \wedge *IsFiniteSet*($peersD$) BY *PeersOK* DEF *PeersOK*
 351 $\langle 3 \rangle$ 2 *IsFiniteSet*($peers$) BY $\langle 3 \rangle$ 1, *FS_Union* DEF *peers*
 352 $\langle 3 \rangle$ 3 *IsFiniteSet*($peersS1$) \wedge *IsFiniteSet*($peersS2$) BY $\langle 3 \rangle$ 2, *FS_Subset*
 353 $\langle 3 \rangle$ f. QED BY *FS_Intersection*, $\langle 3 \rangle$ 3, $\langle 3 \rangle$ 2, $\langle 3 \rangle$ 1
 354 $\langle 2 \rangle$ 3. $\text{Cardinality}(peersS1 \cap peersS2) > n - nh$
 355 $\langle 3 \rangle$ $(2 * threshold - n) > n - nh$
 356 BY *ThresholdOK*, *PeersOK* DEF *ThresholdOK*, *PeersOK*
 357 $\langle 3 \rangle$ $\text{Cardinality}(peersS1 \cap peersS2) \in \text{Nat}$ BY *FS_CardinalityType*, $\langle 2 \rangle$ 2
 358 $\langle 3 \rangle$ $threshold \in \text{Nat} \wedge n \in \text{Nat} \wedge nh \in \text{Nat}$ BY *ThresholdOK*, *PeersOK* DEF *ThresholdOK*, *PeersOK*
 359 $\langle 3 \rangle$ f QED BY $\langle 2 \rangle$ 1
 360 $\langle 2 \rangle$ 4. $(peersS1 \cap peersS2) \cap peersH \neq \{\}$
 361 $\langle 3 \rangle$ 0 $(peersS1 \cap peersS2) \subseteq peers \wedge peersH \subseteq peers$ BY *PeersOK*, *ThresholdOK* DEF *peers*, *PeersOK*, *T*
 362 $\langle 3 \rangle$ 1 $\text{Cardinality}(peers) = n \wedge \text{Cardinality}(peersH) = nh$ BY *PeersOK* DEF *PeersOK*
 363 $\langle 3 \rangle$ 2 $\text{Cardinality}(peersS1 \cap peersS2) \in \text{Nat} \wedge \text{Cardinality}(peersH) \in \text{Nat} \wedge \text{Cardinality}(peers) \in \text{Nat}$ BY
 364 $\langle 3 \rangle$ 3 $\text{Cardinality}(peersS1 \cap peersS2) + \text{Cardinality}(peersH) > \text{Cardinality}(peers)$ BY $\langle 3 \rangle$ 1, $\langle 2 \rangle$ 3, $\langle 3 \rangle$ 2
 365 $\langle 3 \rangle$ f QED
 366 BY $\langle 3 \rangle$ 0, $\langle 2 \rangle$ 0, $\langle 3 \rangle$ 3, $\langle 3 \rangle$ 1, *FS_MajoritiesIntersect*, *CardPeers*
 367 $\langle 2 \rangle$ f. QED

368 BY $\langle 2 \rangle 2, \langle 2 \rangle 4, FS_EmptySet$
 369 $\langle 1 \rangle$ f. QED
 370 BY $\langle 1 \rangle$ a, $\langle 1 \rangle$ b, $\langle 1 \rangle 2$ DEF *Cardinality*
 372 **Peers locally enforce FC**
 373 LEMMA $TPeersLocalFC \triangleq Protocol \Rightarrow \Box PeersLocalFC$
 374 $\langle 1 \rangle$ USE DEF *PeersLocalFC*, *Inv1*, *TypeOK*
 375 $\langle 1 \rangle$ b. $Init \wedge TypeOK \Rightarrow PeersLocalFC$
 376 $\langle 2 \rangle$ SUFFICES ASSUME $Init \wedge TypeOK$,
 377 NEW $P \in peersH$
 378 PROVE $\wedge \forall B \in signed[P] : extends(B, Pv[P])$
 379 $\wedge \forall B \in FRP(P) : B = Pv[P]$
 380 BY DEF *PeersLocalFC*
 381 $\langle 2 \rangle P \in peers$ BY DEF *peers*
 382 $\langle 2 \rangle signed[P] = \{\} \wedge (FRP(P) \cap FinalW) = \{\}$
 383 $\langle 3 \rangle 1. signed[P] = \{\}$
 384 BY DEF *Init*
 385 $\langle 3 \rangle 2. FRP(P) = \{\}$
 386 $\langle 4 \rangle 1 (signed[P] \cup \{Pv[P]\}) = \{B0\}$ BY DEF *Init*
 387 $\langle 4 \rangle$ qed QED BY $\langle 4 \rangle 1, PhasesOK, WOK$ DEF *Init, FinalW, FRP, PhasesOK, WOK, NFRP, phase*
 388 $\langle 3 \rangle 3.$ QED
 389 BY $\langle 3 \rangle 1, \langle 3 \rangle 2$
 390 $\langle 2 \rangle 1. \forall B \in signed[P] : extends(B, Pv[P])$
 391 BY *ExtendsRefl* DEF *Init, FRP, NFRP, FinalW*
 392 $\langle 2 \rangle 2. \forall B \in FRP(P) : B = Pv[P]$
 393 BY *ExtendsRefl* DEF *Init, FRP, NFRP, FinalW*
 394 $\langle 2 \rangle 3.$ QED
 395 BY $\langle 2 \rangle 1, \langle 2 \rangle 2$
 396 $\langle 1 \rangle$ i. $TypeOK \wedge PeersLocalFC \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle} \Rightarrow PeersLocalFC'$
 397 $\langle 2 \rangle$ USE DEF *PeersLocalFC*
 398 $\langle 2 \rangle$ qed QED
 399 $\langle 3 \rangle$ SUFFICES ASSUME $TypeOK \wedge PeersLocalFC \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle}$,
 400 NEW $P \in peersH'$
 401 PROVE $(\wedge \forall B \in signed[P] : extends(B, Pv[P])$
 402 $\wedge \forall B \in FRP(P) : B = Pv[P])'$
 403 BY DEF *PeersLocalFC*
 404 $\langle 3 \rangle P \in peersH \wedge P \in peers$ BY DEF *peers*
 405 $\langle 3 \rangle$ QED
 406 $\langle 4 \rangle 1.$ ASSUME NEW $P_1 \in peersH$,
 407 NEW $bu \in W$,
 408 $\wedge extends(Pv[P_1], bu)$
 409 $\wedge phase(Pv[P_1]) \neq pf$
 410 $\wedge Pv' = [Pv \text{ EXCEPT } ![P_1] = bu]$
 411 $\wedge \text{UNCHANGED } \langle fr, nfr, signed \rangle$
 412 PROVE $(\wedge \forall B \in signed[P] : extends(B, Pv[P]))$

413 $\wedge \forall B \in FRP(P) : B = Pv[P]]'$
 414 $\langle 5 \rangle P_1 \in peers$ BY DEF *peers*
 415 $\langle 5 \rangle$ CASE $P_1 = P$
 416 $\langle 6 \rangle$ CASE $FRP(P) = \{\}$
 417 $\langle 7 \rangle$ CASE $phase(bu) = pf$
 418 $\langle 8 \rangle FRP(P)' = \{bu\}$ BY $\langle 4 \rangle 1$ DEF *FRP*, *FinalW*, *NFRP*
 419 $\langle 8 \rangle$ qed QED
 420 $\langle 9 \rangle 1. (\forall B \in signed[P] : extends(B, Pv[P]))'$
 421 BY $\langle 4 \rangle 1$, *ExtendsTrans* DEF *FRP*, *FinalW*, *NFRP*
 422 $\langle 9 \rangle 2. (\forall B \in FRP(P) : B = Pv[P])'$
 423 BY $\langle 4 \rangle 1$ DEF *FRP*, *FinalW*, *NFRP*
 424 $\langle 9 \rangle 3.$ QED
 425 BY $\langle 9 \rangle 1$, $\langle 9 \rangle 2$
 426 $\langle 7 \rangle$ CASE $phase(bu) \neq pf$
 427 $\langle 8 \rangle FRP(P)' = \{\}$ BY $\langle 4 \rangle 1$ DEF *FRP*, *FinalW*, *NFRP*
 428 $\langle 8 \rangle$ qed QED
 429 $\langle 9 \rangle 1. (\forall B \in signed[P] : extends(B, Pv[P]))'$
 430 BY $\langle 4 \rangle 1$, *ExtendsTrans* DEF *FRP*, *FinalW*, *NFRP*
 431 $\langle 9 \rangle 2. (\forall B \in FRP(P) : B = Pv[P])'$
 432 BY $\langle 4 \rangle 1$ DEF *FRP*, *FinalW*, *NFRP*
 433 $\langle 9 \rangle 3.$ QED
 434 BY $\langle 9 \rangle 1$, $\langle 9 \rangle 2$
 435 $\langle 7 \rangle$ qed QED OBVIOUS
 436 $\langle 6 \rangle$ CASE $FRP(P) \neq \{\}$
 437 $\langle 7 \rangle \exists B \in FRP(P) : TRUE$ OBVIOUS
 438 $\langle 7 \rangle \exists B \in FRP(P) : B = Pv[P] \wedge phase(Pv[P]) = pf$ BY DEF *FRP*, *FinalW*
 439 $\langle 7 \rangle$ qed QED BY $\langle 4 \rangle 1$
 440 $\langle 6 \rangle$ qed QED BY DEF *FRP*, *NFRP*, *FinalW*
 441 $\langle 5 \rangle$ qed QED BY $\langle 4 \rangle 1$ DEF *FRP*, *NFRP*, *FinalW*
 442 $\langle 4 \rangle 2.$ ASSUME NEW $P_1 \in peersH$,
 443 NEW $bs \in W$,
 444 $\wedge extends(bs, Pv[P_1]) \wedge phase(bs) = phase(Pv[P_1])$
 445 $\wedge (phase(Pv[P_1]) = pf \Rightarrow bs = Pv[P_1])$
 446 $\wedge signed' = [signed \text{ EXCEPT } ![P_1] = signed[P_1] \cup \{bs\}]$
 447 $\wedge UNCHANGED \langle fr, nfr, Pv \rangle$
 448 PROVE $(\wedge \forall B \in signed[P] : extends(B, Pv[P]))$
 449 $\wedge \forall B \in FRP(P) : B = Pv[P]]'$
 450 $\langle 5 \rangle P_1 \in peers$ BY DEF *peers*
 451 $\langle 5 \rangle$ CASE $P_1 \neq P$
 452 $\langle 6 \rangle 1 signed[P] = signed[P]'$ BY $\langle 4 \rangle 2$ DEF *FRP*, *FinalW*, *NFRP*
 453 $\langle 6 \rangle FRP(P) = FRP(P)' \wedge signed[P] = signed[P]' \wedge Pv[P] = Pv[P]'$ BY $\langle 4 \rangle 2$, $\langle 6 \rangle 1$ DEF *FRP*, *FinalW*
 454 $\langle 6 \rangle$ QED BY $\langle 4 \rangle 2$
 455 $\langle 5 \rangle$ CASE $P_1 = P$
 456 $\langle 6 \rangle$ CASE $FRP(P) = \{\}$
 457 $\langle 7 \rangle$ CASE $phase(Pv[P_1]) = pf$

458 $\langle 8 \rangle \text{ phase}(bs) = pf$ BY $\langle 4 \rangle 2$
 459 $\langle 8 \rangle bs = Pv[P_1]$ BY $\langle 4 \rangle 2$
 460 $\langle 8 \rangle FRP(P)' = \{bs\}$ BY $\langle 4 \rangle 1$ DEF $FRP, FinalW, NFRP$
 461 $\langle 8 \rangle$ qed QED
 462 $\langle 9 \rangle 1. (\forall B \in signed[P] : extends(B, Pv[P]))'$
 463 BY $\langle 4 \rangle 2, ExtendsTrans$ DEF $FRP, FinalW, NFRP$
 464 $\langle 9 \rangle 2. (\forall B \in FRP(P) : B = Pv[P])'$
 465 BY $\langle 4 \rangle 2$ DEF $FRP, FinalW, NFRP$
 466 $\langle 9 \rangle 3.$ QED
 467 BY $\langle 9 \rangle 2, \langle 4 \rangle 2$
 468 $\langle 7 \rangle$ CASE $phase(Pv[P_1]) \neq pf$
 469 $\langle 8 \rangle \text{ phase}(bs) \neq pf$ BY $\langle 4 \rangle 2$
 470 $\langle 8 \rangle FRP(P)' = \{\}$ BY $\langle 4 \rangle 2$ DEF $FRP, FinalW, NFRP$
 471 $\langle 8 \rangle$ qed QED
 472 $\langle 9 \rangle 1. (\forall B \in signed[P] : extends(B, Pv[P]))'$
 473 BY $\langle 4 \rangle 2, ExtendsTrans$ DEF $FRP, FinalW, NFRP$
 474 $\langle 9 \rangle 2. (\forall B \in FRP(P) : B = Pv[P])'$
 475 BY $\langle 4 \rangle 2$ DEF $FRP, FinalW, NFRP$
 476 $\langle 9 \rangle 3.$ QED
 477 BY $\langle 9 \rangle 1, \langle 4 \rangle 2$
 478 $\langle 7 \rangle$ qed QED OBVIOUS
 479 $\langle 6 \rangle$ CASE $FRP(P) \neq \{\}$
 480 $\langle 7 \rangle Pv[P] = Pv[P]'$ BY $\langle 4 \rangle 2$
 481 $\langle 7 \rangle \exists B \in FRP(P) : \forall Bf \in FRP(P) : B = Bf \wedge B = Pv[P] \wedge phase(Pv[P]) = pf \wedge phase(bs) = pf$
 482 $\langle 7 \rangle extends(bs, Pv[P])'$ BY $\langle 4 \rangle 2$
 483 $\langle 7 \rangle signed[P]' = signed[P] \cup \{bs\}$ BY $\langle 4 \rangle 2$
 484 $\langle 7 \rangle$ qed QED
 485 $\langle 8 \rangle 1. (\forall B \in signed[P] : extends(B, Pv[P]))'$
 486 $\langle 9 \rangle$ SUFFICES ASSUME NEW $B \in (signed[P])'$
 487 PROVE $extends(B, Pv[P])'$
 488 OBVIOUS
 489 $\langle 9 \rangle$ QED
 490 BY $\langle 4 \rangle 2$
 491 $\langle 8 \rangle 2. (\forall B \in FRP(P) : B = Pv[P])'$
 492 $\langle 9 \rangle$ SUFFICES ASSUME NEW $B \in FRP(P)'$
 493 PROVE $(B = Pv[P])'$
 494 OBVIOUS
 495 $\langle 9 \rangle B = Pv[P]$ BY $\langle 4 \rangle 2$ DEF $FRP, FinalW, NFRP$
 496 $\langle 9 \rangle$ QED
 497 BY $\langle 4 \rangle 2$
 498 $\langle 8 \rangle 3.$ QED
 499 BY $\langle 8 \rangle 1, \langle 8 \rangle 2$
 500 $\langle 6 \rangle$ qed QED BY DEF $FRP, NFRP, FinalW$
 501 $\langle 5 \rangle$ qed QED BY $\langle 4 \rangle 2$ DEF $FRP, NFRP, FinalW$
 502 $\langle 4 \rangle 3.$ ASSUME NEW $P_1 \in peersD,$

503 NEW $bs \in W$,
 504 $\wedge signed' = [signed \text{ EXCEPT } ![P_1] = signed[P_1] \cup \{bs\}]$
 505 $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$
 506 PROVE $(\wedge \forall B \in signed[P] : extends(B, Pv[P]))$
 507 $\wedge \forall B \in FRP(P) : B = Pv[P])'$
 508 $\langle 5 \rangle P_1 \notin peersH \text{ BY } PeersOK \text{ DEF } PeersOK$
 509 $\langle 5 \rangle \text{qed QED BY } \langle 4 \rangle 3 \text{ DEF } FRP, NFRP, FinalW$
 510 $\langle 4 \rangle 4$. ASSUME NEW $bu \in W$,
 511 NEW $R \in readers$,
 512 $\wedge GuR(bu)$
 513 $\wedge nfr' = [nfr \text{ EXCEPT } ![R] = nfr[R] \cup \{bu\}]$
 514 $\wedge \text{UNCHANGED } \langle fr, Pv, signed \rangle$
 515 PROVE $(\wedge \forall B \in signed[P] : extends(B, Pv[P]))$
 516 $\wedge \forall B \in FRP(P) : B = Pv[P])'$
 517 BY $\langle 4 \rangle 4 \text{ DEF } FRP, NFRP, FinalW$
 518 $\langle 4 \rangle 5$. ASSUME NEW $bu \in W$,
 519 NEW $R \in readers$,
 520 $\wedge GuR(bu) \wedge phase(bu) = pf$
 521 $\wedge fr' = [fr \text{ EXCEPT } ![R] = fr[R] \cup \{bu\}]$
 522 $\wedge \text{UNCHANGED } \langle nfr, Pv, signed \rangle$
 523 PROVE $(\wedge \forall B \in signed[P] : extends(B, Pv[P]))$
 524 $\wedge \forall B \in FRP(P) : B = Pv[P])'$
 525 BY $\langle 4 \rangle 5 \text{ DEF } FRP, NFRP, FinalW$
 526 $\langle 4 \rangle 6$. CASE UNCHANGED $\langle fr, nfr, Pv, signed \rangle$
 527 BY $\langle 4 \rangle 6 \text{ DEF } FRP, NFRP, FinalW$
 528 $\langle 4 \rangle 7$. QED
 529 BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 4 \rangle 3, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 6 \text{ DEF } Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdateP$
 530 $\langle 1 \rangle \text{qed QED BY } \langle 1 \rangle b, \langle 1 \rangle i, Invariance1, PTL \text{ DEF } Protocol, Inv1, TypeOK$

 532 Peers locally enforce FA
 533 LEMMA $TPeersLocalFA \triangleq Protocol \Rightarrow \Box PeersLocalFA$
 534 $\langle 1 \rangle \text{ USE DEF } PeersLocalFA, Inv1, TypeOK$
 535 $\langle 1 \rangle b$. $Init \wedge TypeOK \Rightarrow PeersLocalFA$
 536 $\langle 2 \rangle \text{ SUFFICES ASSUME } Init \wedge TypeOK$,
 537 NEW $P \in peersH$
 538 PROVE $FA_param(FRP(P),$
 539 $NFRP(P))$
 540 BY DEF $PeersLocalFA$
 541 $\langle 2 \rangle \text{ USE DEF } FRP, NFRP$
 542 $\langle 2 \rangle P \in peers \text{ BY } PeersOK \text{ DEF } PeersOK, peers$
 543 $\langle 2 \rangle signed[P] = \{\}$ BY DEF $Init$
 544 $\langle 2 \rangle signed[P] \cap \{B \in W : phase(B) = pf\} = \{\}$ BY DEF $Init$
 545 $\langle 2 \rangle 1$. $(signed[P] \cap \{B \in W : phase(B) = pf\}) = \{\} \vee \exists Bf \in (signed[P] \cap \{B \in W : phase(B) = pf\}) : (si$
 546 $\langle 3 \rangle \text{ QED BY DEF } Init, FA_param$
 547 $\langle 2 \rangle 2$. $\forall Bf \in (signed[P] \cap \{B \in W : phase(B) = pf\}) : \forall B \in (signed[P]) : extends(B, Bf)$

548 $\langle 3 \rangle$ QED BY DEF *Init*, *FA_param*
549 $\langle 2 \rangle 11$. $FRP(P) = \{\}$ $\vee \exists Bf \in FRP(P) : FRP(P) = \{Bf\}$
550 BY DEF *FA_param*
551 $\langle 2 \rangle 21$. $\forall Bf \in FRP(P) : \forall B \in NFRP(P) : extends(B, Bf)$
552 BY *ExtendsRefl* DEF *FA_param*, *ExtendsRefl*
553 $\langle 2 \rangle 3$. QED
554 BY $\langle 2 \rangle 11$, $\langle 2 \rangle 21$ DEF *FA_param*
555 $\langle 1 \rangle i$. $TypeOK \wedge PeersLocalFA \wedge PeersLocalFC \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle} \Rightarrow PeersLocalFA'$
556 $\langle 2 \rangle$ SUFFICES ASSUME $TypeOK \wedge PeersLocalFA \wedge PeersLocalFC \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle}$,
557 NEW $P \in peersH'$
558 PROVE $FA_param(FRP(P),$
559 $NFRP(P))'$
560 BY DEF *PeersLocalFA*
561 $\langle 2 \rangle$ $P \in peersH \wedge P \in peers$ BY DEF *peers*
562 $\langle 2 \rangle$ USE DEF *PeersLocalFC*
563 $\langle 2 \rangle$ qed. QED
564 $\langle 3 \rangle 1$. ASSUME NEW $P_1 \in peersH$,
565 NEW $bu \in W$,
566 $\wedge extends(Pv[P_1], bu)$
567 $\wedge phase(Pv[P_1]) \neq pf$
568 $\wedge Pv' = [Pv \text{ EXCEPT } ![P_1] = bu]$
569 $\wedge \text{UNCHANGED } \langle fr, nfr, signed \rangle$
570 PROVE $FA_param(FRP(P),$
571 $NFRP(P))'$
572 $\langle 5 \rangle$ $P_1 \in peers$ BY DEF *peers*
573 $\langle 5 \rangle$ CASE $P_1 = P$
574 $\langle 6 \rangle$ CASE $FRP(P) = \{\}$
575 $\langle 7 \rangle$ CASE $phase(bu) = pf$
576 $\langle 8 \rangle$ $FRP(P)' = \{bu\}$ BY $\langle 3 \rangle 1$ DEF *FRP*, *FinalW*, *NFRP*
577 $\langle 8 \rangle$ qed QED
578 $\langle 9 \rangle 1$. $(\forall B \in signed[P] : extends(B, Pv[P]))'$
579 BY $\langle 3 \rangle 1$, *ExtendsTrans* DEF *FRP*, *FinalW*, *NFRP*
580 $\langle 9 \rangle 2$. $(\forall B \in FRP(P) : B = Pv[P])'$
581 BY $\langle 3 \rangle 1$ DEF *FRP*, *FinalW*, *NFRP*
582 $\langle 9 \rangle$ $FRP(P)' = \{bu\}$ BY $\langle 9 \rangle 1$, $\langle 9 \rangle 2$, $\langle 3 \rangle 1$
583 $\langle 9 \rangle \forall B \in NFRP(P)' : extends(B, bu)$
584 $\langle 10 \rangle$ $NFRP(P)' \subseteq NFRP(P) \cup \{bu\}$ BY $\langle 3 \rangle 1$ DEF *NFRP*, *FRP*, *FinalW*
585 $\langle 10 \rangle \forall B \in NFRP(P) : extends(B, bu)$
586 $\langle 11 \rangle$ SUFFICES ASSUME NEW $B \in NFRP(P)$
587 PROVE $extends(B, bu)$
588 OBVIOUS
589 $\langle 11 \rangle$ $B \in W \wedge Pv[P] \in W$ BY DEF *NFRP*
590 $\langle 11 \rangle$ $extends(B, Pv[P])$
591 $\langle 12 \rangle$ CASE $B = Pv[P]$ BY *ExtendsRefl*
592 $\langle 12 \rangle$ CASE $B \in NFRP(P)$ BY DEF *NFRP*

```

593         ⟨12⟩ QED BY DEF PeersLocalFA, ExtendsTrans, FA_param
594         ⟨11⟩ QED BY ExtendsTrans, ⟨3⟩1
595         ⟨10⟩ extends(bu, bu) BY ExtendsRefl
596         ⟨10⟩qed QED BY ⟨9⟩1, ⟨9⟩2, ⟨3⟩1 DEF PeersLocalFC
597         ⟨9⟩3. QED
598         BY ⟨9⟩1, ⟨9⟩2 DEF FA_param
599         ⟨7⟩CASE phase(bu) ≠ pf
600         ⟨8⟩ FRP(P)' = {} BY ⟨3⟩1 DEF FRP, FinalW, NFRP
601         ⟨8⟩qed QED
602         ⟨9⟩1. (∀ B ∈ signed[P] : extends(B, Pv[P]))'
603         BY ⟨3⟩1, ExtendsTrans DEF FRP, FinalW, NFRP
604         ⟨9⟩2. (∀ B ∈ FRP(P) : B = Pv[P])'
605         BY ⟨3⟩1 DEF FRP, FinalW, NFRP
606         ⟨9⟩3. QED
607         BY ⟨9⟩1, ⟨9⟩2 DEF FA_param
608         ⟨7⟩qed QED OBVIOUS
609         ⟨6⟩CASE FRP(P) ≠ {}
610         ⟨7⟩ ∃ B ∈ FRP(P) : TRUEOBVIOUS
611         ⟨7⟩ ∃ B ∈ FRP(P) : B = Pv[P] ∧ phase(Pv[P]) = pf BY DEF FRP, FinalW
612         ⟨7⟩qed QED BY ⟨3⟩1
613         ⟨6⟩qed QED BY DEF FRP, NFRP, FinalW
614         ⟨5⟩qed QED BY ⟨3⟩1 DEF FRP, NFRP, FinalW
615         ⟨3⟩2. ASSUME NEW P_1 ∈ peersH,
616             NEW bs ∈ W,
617             ∧ extends(bs, Pv[P_1]) ∧ phase(bs) = phase(Pv[P_1])
618             ∧ (phase(Pv[P_1]) = pf ⇒ bs = Pv[P_1])
619             ∧ signed' = [signed EXCEPT ![P_1] = signed[P_1] ∪ {bs}]
620             ∧ UNCHANGED ⟨fr, nfr, Pv⟩
621         PROVE FA_param(FRP(P),
622             NFRP(P))'
623         BY ⟨3⟩2 DEF FRP, NFRP, FinalW, FA_param
624         ⟨3⟩3. ASSUME NEW P_1 ∈ peersD,
625             NEW bs ∈ W,
626             ∧ signed' = [signed EXCEPT ![P_1] = signed[P_1] ∪ {bs}]
627             ∧ UNCHANGED ⟨fr, nfr, Pv⟩
628         PROVE FA_param(FRP(P),
629             NFRP(P))'
630         ⟨4⟩ P_1 ∉ peersH BY PeersOK DEF PeersOK
631         ⟨4⟩qed QED BY ⟨3⟩3 DEF FRP, NFRP, FinalW
632         ⟨3⟩4. ASSUME NEW bu ∈ W,
633             NEW R ∈ readers,
634             ∧ GuR(bu)
635             ∧ nfr' = [nfr EXCEPT ![R] = nfr[R] ∪ {bu}]
636             ∧ UNCHANGED ⟨fr, Pv, signed⟩
637         PROVE FA_param(FRP(P),

```

638 $NFRP(P))'$
 639 BY $\langle 3 \rangle 4$ DEF $FRP, NFRP, FinalW, FA_param$
 640 $\langle 3 \rangle 5$. ASSUME NEW $bu \in W$,
 641 NEW $R \in readers$,
 642 $\wedge GuR(bu) \wedge phase(bu) = pf$
 643 $\wedge fr' = [fr \text{ EXCEPT } ![R] = fr[R] \cup \{bu\}]$
 644 $\wedge \text{UNCHANGED } \langle nfr, Pv, signed \rangle$
 645 PROVE $FA_param(FRP(P),$
 646 $NFRP(P))'$
 647 BY $\langle 3 \rangle 5$ DEF $FRP, NFRP, FinalW, FA_param$
 648 $\langle 3 \rangle 6$. CASE UNCHANGED $\langle fr, nfr, Pv, signed \rangle$
 649 BY $\langle 3 \rangle 6$ DEF $FRP, NFRP, FinalW, FA_param$
 650 $\langle 3 \rangle 7$. QED
 651 BY $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, \langle 3 \rangle 4, \langle 3 \rangle 5, \langle 3 \rangle 6$ DEF $Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH$
 652 $\langle 1 \rangle f$. QED BY $\langle 1 \rangle b, \langle 1 \rangle i, Invariance1, PTL, TPearsLocalFC$ DEF $Protocol, Inv1, TypeOK$

654 **Preservation of Gu for all read contents and final contents have phase pf**
 655 LEMMA $TReadersLocalGu \triangleq Protocol \Rightarrow \Box ReadersLocalGu$
 656 $\langle 1 \rangle$ USE DEF $ReadersLocalGu, Inv1, TypeOK$
 657 $\langle 1 \rangle b$. $Init \wedge TypeOK \Rightarrow ReadersLocalGu$ BY DEF $Init$
 658 $\langle 1 \rangle i$. $TypeOK \wedge ReadersLocalGu \wedge [Next]_{\langle fr, nfr, Pv, signed \rangle} \Rightarrow ReadersLocalGu'$
 659 $\langle 2 \rangle$ SUFFICES ASSUME $TypeOK$,
 660 $ReadersLocalGu$,
 661 NEW $R \in readers'$,
 662 $[Next]_{\langle fr, nfr, Pv, signed \rangle}$
 663 PROVE $(\wedge \forall B \in nfr[R] : GuR(B)$
 664 $\wedge \forall B \in fr[R] : GuR(B) \wedge phase(B) = pf)'$
 665 BY DEF $ReadersLocalGu$
 666 $\langle 2 \rangle 1$. ASSUME NEW $P \in peersH$,
 667 $\exists bu \in W$:
 668 $\wedge extends(Pv[P], bu)$
 669 $\wedge phase(Pv[P]) \neq pf$
 670 $\wedge Pv' = [Pv \text{ EXCEPT } ![P] = bu]$
 671 $\wedge \text{UNCHANGED } \langle fr, nfr, signed \rangle$
 672 PROVE $(\wedge \forall B \in nfr[R] : GuR(B)$
 673 $\wedge \forall B \in fr[R] : GuR(B) \wedge phase(B) = pf)'$
 674 BY $\langle 2 \rangle 1$ DEF GuR
 675 $\langle 2 \rangle 2$. ASSUME NEW $P \in peersH$,
 676 $\exists bs \in W$:
 677 $\wedge extends(bs, Pv[P]) \wedge phase(bs) = phase(Pv[P])$
 678 $\wedge (phase(Pv[P]) = pf \Rightarrow bs = Pv[P])$
 679 $\wedge signed' = [signed \text{ EXCEPT } ![P] = signed[P] \cup \{bs\}]$
 680 $\wedge \text{UNCHANGED } \langle fr, nfr, Pv \rangle$
 681 PROVE $(\wedge \forall B \in nfr[R] : GuR(B)$
 682 $\wedge \forall B \in fr[R] : GuR(B) \wedge phase(B) = pf)'$

```

683   BY ⟨2⟩2 DEF GuR
684   ⟨2⟩3. ASSUME NEW P ∈ peersD,
685           ∃ bs ∈ W :
686           ∧ signed' = [signed EXCEPT ![P] = signed[P] ∪ {bs}]
687           ∧ UNCHANGED ⟨fr, nfr, Pv⟩
688   PROVE ( ∧ ∀ B ∈ nfr[R] : GuR(B)
689           ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf)'
690   BY ⟨2⟩3 DEF GuR
691   ⟨2⟩4. ASSUME NEW bu ∈ W,
692           NEW R_1 ∈ readers,
693           ∧ GuR(bu)
694           ∧ nfr' = [nfr EXCEPT ![R_1] = nfr[R_1] ∪ {bu}]
695           ∧ UNCHANGED ⟨fr, Pv, signed⟩
696   PROVE ( ∧ ∀ B ∈ nfr[R] : GuR(B)
697           ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf)'
698   BY ⟨2⟩4 DEF GuR
699   ⟨2⟩5. ASSUME NEW bu ∈ W,
700           NEW R_1 ∈ readers,
701           ∧ GuR(bu) ∧ phase(bu) = pf
702           ∧ fr' = [fr EXCEPT ![R_1] = fr[R_1] ∪ {bu}]
703           ∧ UNCHANGED ⟨nfr, Pv, signed⟩
704   PROVE ( ∧ ∀ B ∈ nfr[R] : GuR(B)
705           ∧ ∀ B ∈ fr[R] : GuR(B) ∧ phase(B) = pf)'
706   BY ⟨2⟩5 DEF GuR
707   ⟨2⟩6. CASE UNCHANGED ⟨fr, nfr, Pv, signed⟩
708   BY ⟨2⟩6 DEF GuR
709   ⟨2⟩7. QED
710   BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6 DEF Next, ReadFinal, ReadNonFinal, SignPD, SignPH, UpdatePH
711   ⟨1⟩f. QED BY ⟨1⟩b, ⟨1⟩i, Invariance1, PTL, TPeersLocalFC DEF Protocol, Inv1, TypeOK

713   The previous properties imply ReaderAgreement that boils down to FA applied between two readers
714   LEMMA soundReaderAgreement  $\triangleq$  TypeOK ∧ ReadersLocalGu ∧ PeersLocalFC ∧ PeersLocalFA  $\Rightarrow$  ReaderAgreement
715   ⟨1⟩ USE DEF ReaderAgreement, TypeOK, BSfr, BSnfr
716   ⟨1⟩qed QED
717   ⟨2⟩ SUFFICES ASSUME TypeOK ∧ ReadersLocalGu ∧ PeersLocalFC ∧ PeersLocalFA,
718           NEW R1 ∈ readers, NEW R2 ∈ readers,
719           NEW B1 ∈ BSfr ∪ BSnfr,
720           NEW B2 ∈ BSfr
721   PROVE extends(B1, B2)
722   BY DEF ReaderAgreement
723   ⟨2⟩1 GuR(B1) ∧ GuR(B2) BY DEF ReadersLocalGu
724   ⟨2⟩2 (B1 ∈ fr[R1]  $\Rightarrow$  phase(B1) = pf) ∧ (B2 ∈ fr[R2]  $\Rightarrow$  phase(B2) = pf) BY DEF ReadersLocalGu
725   ⟨2⟩ B1 ∈ W ∧ B2 ∈ W BY DEF TypeOK
726   ⟨2⟩ QED
727   ⟨3⟩ SUFFICES ASSUME NEW PS1 ∈ SUBSET peers,

```


728 $\wedge \text{Cardinality}(PS1) \geq \text{threshold}$
729 $\wedge \forall P1 \in PS1 : B1 \in \text{signed}[P1],$
730 NEW $PS2 \in \text{SUBSET } \text{peers},$
731 $\wedge \text{Cardinality}(PS2) \geq \text{threshold}$
732 $\wedge \forall P2 \in PS2 : B2 \in \text{signed}[P2]$
733 PROVE $\text{extends}(B1, B2)$
734 BY $\langle 2 \rangle 1$ DEF GuR
735 $\langle 3 \rangle \exists Ph \in \text{peers}H : Ph \in PS1 \wedge Ph \in PS2$ BY $TIntersecPeers$ DEF $IntersecPeers$
736 $\langle 3 \rangle$ qed QED
737 $\langle 4 \rangle$ SUFFICES ASSUME NEW $Ph \in \text{peers}H,$
738 $Ph \in PS1 \wedge Ph \in PS2$
739 PROVE $\text{extends}(B1, B2)$
740 OBVIOUS
741 $\langle 4 \rangle Ph \in \text{peers}$ BY DEF $peers$
742 $\langle 4 \rangle B1 \in \text{signed}[Ph] \wedge B2 \in \text{signed}[Ph]$ OBVIOUS
743 $\langle 4 \rangle \text{phase}(B2) = pf$ BY DEF $ReadersLocalGu$
744 $\langle 4 \rangle$ QED BY DEF $PeersLocalFA, FA_param, FRP, NFRP, FinalW$

746 Therefore, *ReaderAgreement* is an invariant of *Protocol*.
747 LEMMA $TReaderAgreement \triangleq \text{Protocol} \Rightarrow \Box \text{ReaderAgreement}$
748 BY *Invariance1, PTL, TPeersLocalFC, TPeersLocalFA, TReadersLocalGu, soundReaderAgreement* DEF *Proto*

750 *ReaderAgreement* and some previous invariants imply *FA*.
751 LEMMA $\text{soundFA} \triangleq \text{ReaderAgreement} \wedge \text{ReadersLocalGu} \wedge \text{TypeOK} \Rightarrow \text{FA}$
752 $\langle 1 \rangle$ USE DEF $BSfr, BSnfr$
753 $\langle 1 \rangle$ SUFFICES ASSUME $\text{ReaderAgreement} \wedge \text{ReadersLocalGu} \wedge \text{TypeOK}$
754 PROVE FA
755 OBVIOUS
756 $\langle 1 \rangle 1$ UNION $\{fr[R] : R \in \text{readers}\} = \{\} \vee \text{UNION } \{fr[R] : R \in \text{readers}\} \neq \{\}$ OBVIOUS
757 $\langle 1 \rangle 2$ CASE UNION $\{fr[R] : R \in \text{readers}\} = \{\}$
758 $\langle 2 \rangle 1. BSfr = \{\} \vee \exists Bf \in BSfr : BSfr = \{Bf\}$
759 BY $\langle 1 \rangle 2$ DEF FA
760 $\langle 2 \rangle 2. \forall Bf \in BSfr : \forall B \in BSnfr : \text{extends}(B, Bf)$
761 BY $\langle 1 \rangle 2$ DEF FA
762 $\langle 2 \rangle 3.$ QED
763 BY $\langle 2 \rangle 1, \langle 2 \rangle 2$ DEF FA
764 $\langle 1 \rangle 3$ CASE UNION $\{fr[R] : R \in \text{readers}\} \neq \{\}$
765 $\langle 2 \rangle 1 \exists Bf \in \text{UNION } \{fr[R] : R \in \text{readers}\} :$
766 $\wedge \forall B \in \text{UNION } \{nfr[R] : R \in \text{readers}\} : \text{extends}(B, Bf)$ FA (ii)
767 $\wedge \text{UNION } \{fr[R] : R \in \text{readers}\} = \{Bf\}$
768 $\langle 3 \rangle 1$ ASSUME NEW $Bf \in \text{UNION } \{fr[R] : R \in \text{readers}\}$
769 PROVE $\wedge \forall B \in \text{UNION } \{nfr[R] : R \in \text{readers}\} : \text{extends}(B, Bf)$ FA (ii)
770 $\wedge \text{UNION } \{fr[R] : R \in \text{readers}\} = \{Bf\}$ FA (i)
771 $\langle 4 \rangle$ qed QED
772 $\langle 5 \rangle 1. \forall B \in \text{UNION } \{nfr[R] : R \in \text{readers}\} : \text{extends}(B, Bf)$

```

773      BY <1>3 DEF ReaderAgreement, FA, TypeOK, ReadersLocalGu
774 <5>2. UNION {fr[R] : R ∈ readers} = {Bf}
775 <6> ∃ R ∈ readers : Bf ∈ fr[R] OBVIOUS
776 <6> ASSUME NEW B ∈ UNION {fr[R] : R ∈ readers} PROVE B = Bf
777 <7> ∃ R2 ∈ readers : B ∈ fr[R2] OBVIOUS
778 <7>qed QED
779 <8> SUFFICES ASSUME NEW R2 ∈ readers,
780      B ∈ fr[R2],
781      NEW R ∈ readers,
782      Bf ∈ fr[R]
783      PROVE B = Bf
784      OBVIOUS
785 <8> phase(Bf) = pf BY DEF ReadersLocalGu
786 <8> phase(B) = pf BY DEF ReadersLocalGu
787 <8> extends(B, Bf) ∧ extends(Bf, B)
788      BY antiSymEx DEF ReaderAgreement
789 <8> QED BY antiSymEx DEF TypeOK
790 <6> QED
791 BY <1>3 DEF FA, TypeOK
792 <5>3. QED
793 BY <5>1, <5>2
794 <3>2 ∃ Bf ∈ UNION {fr[R] : R ∈ readers} : TRUE BY <1>3
795 <3>qed QED BY <1>3, <3>1, <3>2 DEF FA, TypeOK
796 <2>f QED BY <2>1, <1>3 DEF FA
797 <1> QED
798 BY <1>1, <1>2, <1>3

800 ** Final theorem: final-agreement (FA) is an invariant of our protocol, specified as Spec.
801 THEOREM TFA ≜ Protocol ⇒ □FA
802 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

```