MODULE *IscpBatchTimestamp*

Let's assume the transaction currently being built is t_i and the previous one is t_{i-1}. The following requirements apply to the timestamp $t_i.ts$ of the transaction t_i:

1. Transaction timestamps are non-decreasing function in a chain, i.e.
$$t_i.ts \geq t_{i-1}.ts.$$
2. A transaction timestamp is not smaller than the timestamps of request transactions taken as inputs in t_i, i.e.
$$\forall r \in t_i.req : t_i.ts \geq t_i.req[r].tx.ts,$$
where $t_i.req$ is a list of requests processed as inputs in the transaction t_i, $t_i.req[r]$ is a particular request and $t_i.req[r].tx$ is a transaction the request belongs to.

The initial attempt was to use the timestamp $t_i.ts$ as a median of timestamps proposed by the committee nodes accepted to participate in the transaction t_i by the ACS procedure. This approach conflicts with the rules of selecting requests for the batch (take requests that are mentioned in at least $F+1$ proposals). In this way it is possible that the median is smaller than some request transaction timestamp .
In this document we model the case, when we take maximal of the proposed timestamps excluding the F highest values. This value is close to the 66th percentile (while median is the 50th percentile). In this case all the requests selected to the batch will have timestamp lower than the batch timestamp IF THE BATCH PROPOSALS MEET THE CONDITION

$$\forall p \in batchProposals : \forall r \in p.req : p.req[r].tx.ts \leq p.ts.$$

It is possible that it can be not the case, because of the byzantine nodes. The specification bellow shows, that property (2) can be violated, in the case of byzantine node sending timestamp lower than the requests in the proposal.
The receiving node thus needs to check, if the proposals are correct. For this check it must have all the transactions received before deciding the final batch. The detected invalid batch proposals must be excluded from the following procedure. But that can decrease number of requests included into the final batch (because requests are included if mentioned in $F+1$ proposals). It is safe on the receiver side to "fix" such proposals by setting their timestamp to the maximal transaction timestamp of the requests in the proposal.

EXTENDS *Naturals*, *FiniteSets*, *TLAPS*, *FiniteSetTheorems*, *NaturalsInduction*, *FunctionTheorems*

CONSTANT *Time* — A set of timestamps, represented as natural numbers to have $\leq$.

CONSTANT *Nodes* — A set of node identifiers.

CONSTANT *Byzantine* — A set of byzantine node identifiers.

ASSUME $ConstantAssms \triangleq$

$\quad \land IsFiniteSet(Time) \land Time \neq \{\} \land Time \subseteq Nat$

$\quad \land IsFiniteSet(Nodes) \land Nodes \neq \{\}$

$\quad \land Byzantine \subseteq Nodes$

$Requests \triangleq Time$ — Assume requests are identified by timestamps of their *TX* only.

VARIABLE *acsNodes* — Nodes decided to be part of the round by the *ACS*.

VARIABLE *npRq* — Node proposal: A set of requests.

VARIABLE *npTS* — Node proposal: Timestamp.

$vars \triangleq \langle acsNodes, npRq, npTS \rangle$

$N \triangleq Cardinality(Nodes)$

$F \triangleq$ CHOOSE $F \in 0 \,..\, N :$

$\qquad \land N \geq 3 * F + 1$ — *Byzantine* quorum assumption.

```
          ∧ ∀ f ∈ 0 .. N : N ≥ 3 * f + 1 ⇒ F ≥ f    Consider maximal possible F.
ASSUME ByzantineAssms ≜ F ∈ Nat ∧ N ≥ 3 * F + 1 ∧ (N ≥ 4 ⇒ F ≥ 1)

FQuorums   ≜ {q ∈ SUBSET Nodes : Cardinality(q) = F}
F1Quorums  ≜ {q ∈ SUBSET Nodes : Cardinality(q) = F + 1}
NFQuorums  ≜ {q ∈ SUBSET Nodes : Cardinality(q) = N − F}
TSQuorums  ≜ {q ∈ SUBSET Nodes : q ⊆ acsNodes ∧ Cardinality(q) = Cardinality(acsNodes) − F}
```

BatchRqs is a set of requests selected to the batch. Requests are selected to a batch, if they are mentioned at least in $F + 1$ proposals.

```
BatchRq(rq) ≜ ∃ q ∈ F1Quorums :
                    ∧ q ⊆ acsNodes
                    ∧ ∀ n ∈ q : rq ∈ npRq[n]
BatchRqs    ≜ {rq ∈ Requests : BatchRq(rq)}
```

BatchTS(*ts*) is a predicate, that is true for the timestamp that should be considered as a batch timestamp. It must be maximal of the batch proposals, excluding F greatest ones.

```
SubsetTS(s) ≜ {npTS[n] : n ∈ s}
BatchTSx(ts) ≜ ∀ q ∈ TSQuorums :    TODO: Remove
                    ∧ ts ∈ SubsetTS(q)
                    ∧ ∀ x ∈ SubsetTS(q) : ts ≥ x
                    ∧ ∀ x ∈ SubsetTS(acsNodes \ q) : ts ≤ x
BatchTS(ts) ≜
  ∀ q ∈ FQuorums : (
     ∧ q ⊆ acsNodes
     ∧ ∀ x ∈ q, y ∈ acsNodes \ q : npTS[x] ≥ npTS[y]
  ) ⇒ (
    ∧  ts ∈ SubsetTS(acsNodes \ q)
    ∧  ∀ x ∈ SubsetTS(acsNodes \ q) : ts ≥ x
    ∧  ∀ x ∈ SubsetTS(q) : ts ≤ x
  )
```

A batch proposal is valid, if its timestamp is not less than timestamps of all the request transactions included to the proposal.

```
ProposalValid(n) ≜ ∀ rq ∈ npRq[n] : rq ≤ npTS[n]
├──────────────────────────────────────────────────────────────┤
Init ≜
   ∧ acsNodes ∈ SUBSET Nodes ∧ Cardinality(acsNodes) ≥ N − F
   ∧ npRq ∈ [acsNodes → (SUBSET Requests) \ {{}}]
   ∧ npTS ∈ [acsNodes → Time]
   ∧ ∀ n   ∈ (acsNodes \ Byzantine) : ProposalValid(n)   Fair node proposals are valid.
Next ≜ UNCHANGED vars   Only for model checking in TLC.
Spec ≜ Init ∧ □[Next]_vars

TypeOK ≜
   ∧ acsNodes ⊆ Nodes
```

$\land npRq \in [acsNodes \rightarrow \text{SUBSET } Requests]$

$\land npTS \in [acsNodes \rightarrow Time]$

$Invariant \triangleq$

$\forall ts \in Time, rq \in BatchRqs : BatchTS(ts) \Rightarrow rq \leq ts$

THEOREM $Spec \Rightarrow \Box TypeOK \land \Box Invariant$

PROOF OMITTED Checked with TLC, and check the proofs bellow.

LEMMA $SubsetsAllCardinalities \triangleq$

ASSUME NEW S, $IsFiniteSet(S)$

PROVE $\forall x \in 0 \,..\, Cardinality(S) : \exists q \in \text{SUBSET } S : Cardinality(q) = x$

PROOF

$\langle 1 \rangle$ DEFINE $P(x) \triangleq x \leq Cardinality(S) \Rightarrow \exists q \in \text{SUBSET } S : Cardinality(q) = x$

$\langle 1 \rangle 1.\ \forall x \in Nat : P(x)$

$\langle 2 \rangle 1.\ P(0)$BY $FS\_EmptySet$

$\langle 2 \rangle 2.\ \forall x \in Nat : P(x) \Rightarrow P(x+1)$

$\langle 3 \rangle 1.$ TAKE $x \in Nat$

$\langle 3 \rangle 2.$ HAVE $P(x)$

$\langle 3 \rangle 3.$ HAVE $x + 1 \leq Cardinality(S)$

$\langle 3 \rangle 4.$ PICK $qx \in \text{SUBSET } S : Cardinality(qx) = x$

BY $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $FS\_CardinalityType$

$\langle 3 \rangle 5.$ PICK $x1 \in S : x1 \notin qx$

BY $\langle 3 \rangle 3$, $\langle 3 \rangle 4$

$\langle 3 \rangle 6.$ WITNESS $qx \cup \{x1\} \in \text{SUBSET } S$

$\langle 3 \rangle 7.\ Cardinality(qx \cup \{x1\}) = x + 1$

BY $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $FS\_AddElement$, FS_Subset

$\langle 3 \rangle$ QED BY $\langle 3 \rangle 7$

$\langle 2 \rangle 3.$ QED BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $NatInduction$

$\langle 1 \rangle 2.$ QED BY $\langle 1 \rangle 1$

LEMMA $NatSubsetHasMax \triangleq$

ASSUME NEW S, $IsFiniteSet(S)$, $S \neq \{\}$, $S \in \text{SUBSET } Nat$

PROVE $\exists n \in S : \forall s \in S : s \leq n$

$\langle 1 \rangle$ DEFINE $P(x) \triangleq x \neq \{\} \land x \subseteq S \Rightarrow \exists n \in x : \forall s \in x : s \leq n$

$\langle 1 \rangle$ SUFFICES ASSUME TRUEPROVE $P(S)$OBVIOUS

$\langle 1 \rangle 0.\ IsFiniteSet(S)$OBVIOUS

$\langle 1 \rangle 1.\ P(\{\})$OBVIOUS

$\langle 1 \rangle 2.$ ASSUME NEW T, NEW x, $IsFiniteSet(T)$, $P(T)$, $x \notin T$PROVE $P(T \cup \{x\})$

$\langle 2 \rangle 1.$CASE $\forall t \in T : x \geq t$

$\langle 3 \rangle 0.$ HAVE $T \cup \{x\} \neq \{\} \land T \cup \{x\} \subseteq S$

$\langle 3 \rangle 1.$ WITNESS $x \in T \cup \{x\}$

$\langle 3 \rangle$ QED BY $\langle 2 \rangle 1$, $\langle 3 \rangle 0$

$\langle 2 \rangle 2.$CASE $\neg \forall t \in T : x \geq t$

$\langle 3 \rangle 4.$CASE $T = \{\} \lor \neg T \subseteq S$BY $\langle 3 \rangle 4$

$\langle 3 \rangle 5.$CASE $T \neq \{\} \land T \subseteq S$

```
      ⟨4⟩1. P(T) BY ⟨1⟩2
      ⟨4⟩2. ∃ n ∈ T : ∀ s ∈ T : s ≤ n BY ⟨4⟩1, ⟨3⟩5
      ⟨4⟩ QED BY ⟨4⟩2, ⟨3⟩5, ⟨2⟩2
    ⟨3⟩ QED BY ⟨3⟩4, ⟨3⟩5
  ⟨2⟩3. QED BY ⟨2⟩1, ⟨2⟩2
⟨1⟩ HIDE DEF P
⟨1⟩ QED BY ONLY ⟨1⟩0, ⟨1⟩1, ⟨1⟩2, FS_Induction

THEOREM SpecTypeOK ≜ Spec ⇒ □TypeOK
  ⟨1⟩1. Init ⇒ TypeOK BY DEF Init, TypeOK
  ⟨1⟩2. TypeOK ∧ [Next]_vars ⇒ TypeOK′ BY DEF vars, TypeOK, Next
  ⟨1⟩3. QED BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec

THEOREM SpecInvariant ≜ Byzantine = {} ∧ Spec ⇒ □Invariant
  ⟨1⟩ SUFFICES ASSUME Byzantine = {} PROVE Spec ⇒ □Invariant OBVIOUS
  ⟨1⟩1. TypeOK ∧ Init ⇒ Invariant
    ⟨2⟩ SUFFICES ASSUME TypeOK, Init PROVE Invariant OBVIOUS
    ⟨2⟩ USE DEF Invariant
    ⟨2⟩ TAKE ts ∈ Time, rq ∈ BatchRqs
    ⟨2⟩ HAVE BatchTS(ts) PROVE : rq ≤ ts
    ⟨2⟩1. ∀ q1 ∈ F1Quorums, q2 ∈ NFQuorums : q1 ∩ q2 ≠ {}
      ⟨3⟩ TAKE q1 ∈ F1Quorums, q2 ∈ NFQuorums
      ⟨3⟩1. N ∈ Nat ∧ F ∈ Nat BY ONLY ConstantAssms, ByzantineAssms, FS_CardinalityType DEF N, F
      ⟨3⟩2. Cardinality(q1) + Cardinality(q2) > Cardinality(Nodes) BY ONLY ⟨3⟩1 DEF N, F1Quorums, NFQ
      ⟨3⟩3. q1 ⊆ Nodes ∧ q2 ⊆ Nodes BY ONLY DEF F1Quorums, NFQuorums
      ⟨3⟩4. QED BY ONLY ⟨3⟩2, ⟨3⟩3, FS_MajoritiesIntersect, ConstantAssms
    ⟨2⟩2. ∀ rr ∈ BatchRqs : ∃ q ∈ F1Quorums : ∀ n ∈ q : rr ∈ npRq[n] BY DEF BatchRqs, BatchRq
    ⟨2⟩3. ∀ nn ∈ acsNodes : ProposalValid(nn) BY DEF Init
    ⟨2⟩4. acsNodes ⊆ Nodes BY DEF Init
    ⟨2⟩5. Cardinality(acsNodes) − F > 0
      ⟨3⟩1. Cardinality(acsNodes) ∈ Nat BY ⟨2⟩4, FS_CardinalityType, FS_Subset, ConstantAssms
      ⟨3⟩2. F ∈ Nat BY ByzantineAssms
      ⟨3⟩3. N ∈ Nat BY ConstantAssms, FS_CardinalityType DEF N
      ⟨3⟩4. Cardinality(acsNodes) ≥ N − F BY DEF Init
      ⟨3⟩5. N − F ≥ 2 ∗ F + 1 BY ByzantineAssms, ⟨3⟩2, ⟨3⟩3
      ⟨3⟩6. Cardinality(acsNodes) > F BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ByzantineAssms
      ⟨3⟩ QED BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩6
    ⟨2⟩6. Cardinality(acsNodes) − F ≥ 0 BY ⟨2⟩5
    ⟨2⟩7. ∀ fq ∈ FQuorums, f1q ∈ F1Quorums : ¬f1q ⊆ fq
      ⟨3⟩1. TAKE fq ∈ FQuorums, f1q ∈ F1Quorums
      ⟨3⟩2. SUFFICES ASSUME f1q ⊆ fq PROVE FALSE OBVIOUS
      ⟨3⟩3. IsFiniteSet(f1q) ∧ IsFiniteSet(fq) BY ConstantAssms, FS_Subset DEF FQuorums, F1Quorums
      ⟨3⟩4. Cardinality(f1q) ≤ Cardinality(fq) BY ⟨3⟩2, ⟨3⟩3, FS_Subset
      ⟨3⟩5. Cardinality(f1q) > Cardinality(fq) BY ByzantineAssms DEF F1Quorums, FQuorums
      ⟨3⟩q. QED BY ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, FS_CardinalityType
```

$\langle 2\rangle 8.\ F \in Nat \land F \geq 0 \land F \leq N \land F + 1 \leq N$

$\quad\langle 3\rangle 1.\ F \in Nat$ BY $ByzantineAssms$

$\quad\langle 3\rangle 2.\ F \geq 0$ BY $\langle 3\rangle 1$, $ConstantAssms$ DEF F

$\quad\langle 3\rangle 3.\ N \in Nat$ BY $ConstantAssms$, $FS\_CardinalityType$ DEF N

$\quad\langle 3\rangle 4.\ F \leq N$ BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 3$, $ConstantAssms$, $ByzantineAssms$ DEF F

$\quad\langle 3\rangle 5.\ F + 1 \leq N$ BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 3$, $ConstantAssms$, $ByzantineAssms$ DEF F

$\quad\langle 3\rangle$q. QED BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$, $\langle 3\rangle 5$

$\langle 2\rangle 9.\ FQuorums \neq \{\} \land F1Quorums \neq \{\} \land NFQuorums \neq \{\}$

$\qquad$ BY $\langle 2\rangle 8$, $FS\_CardinalityType$, $ConstantAssms$, $SubsetsAllCardinalities$

$\qquad$ DEF $FQuorums$, $F1Quorums$, $NFQuorums$, N

$\langle 2\rangle 10.$ PICK $fq \in FQuorums : fq \subseteq acsNodes \land \forall x \in fq, y \in acsNodes \setminus fq : npTS[x] \geq npTS[y]$

$\quad\langle 3\rangle 1.$ SUFFICES $\exists fq \in FQuorums : fq \subseteq acsNodes \land \forall x \in fq, y \in acsNodes \setminus fq : npTS[x] \geq npTS[y]$OBV

$\quad\langle 3\rangle 2.\ Cardinality(acsNodes) \geq N - F$ BY DEF $Init$

$\quad\langle 3\rangle 3.\ N - F \geq F$ BY $\langle 2\rangle 8$, $ByzantineAssms$, $ConstantAssms$, $FS\_CardinalityType$ DEF N

$\quad\langle 3\rangle 4.\ N - F > 0$ BY $\langle 2\rangle 8$, $ByzantineAssms$, $ConstantAssms$, $FS\_CardinalityType$ DEF N

$\quad\langle 3\rangle 5.\ N \in Nat$ BY $FS\_CardinalityType$, $ConstantAssms$ DEF N

$\quad\langle 3\rangle 6.\ acsNodes \subseteq Nodes$ BY DEF $Init$

$\quad\langle 3\rangle 7.\ acsNodes \neq \{\}$ BY ONLY $\langle 3\rangle 2$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 2\rangle 8$, $FS\_EmptySet$ DEF $Init$

$\quad\langle 3\rangle 8.\ IsFiniteSet(acsNodes)$ BY FS_Subset, $ConstantAssms$ DEF $Init$

$\quad\langle 3\rangle 9.$ PICK $card \in Nat : card = Cardinality(acsNodes)$ BY $\langle 3\rangle 8$, $FS\_CardinalityType$

$\quad\langle 3\rangle 10.\ card \geq 0 \land card \geq N - F \land card \geq F$ BY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 2\rangle 8$, $\langle 3\rangle 5$, $\langle 3\rangle 9$

$\quad\langle 3\rangle 11.$ PICK $q \in$ SUBSET $acsNodes : Cardinality(q) = F \land \forall x \in q, y \in acsNodes \setminus q : npTS[x] \geq npTS[y$

$\qquad\langle 4\rangle\ \forall q \in$ SUBSET $acsNodes : acsNodes \setminus q \subseteq Nodes$ BY DEF $Init$

$\qquad\langle 4\rangle\ \forall q \in$ SUBSET $acsNodes : acsNodes \setminus q \subseteq acsNodes$ BY DEF $Init$

$\qquad\langle 4\rangle\ \forall n \in acsNodes : npTS[n] \in Nat$ BY $ConstantAssms$ DEF $TypeOK$

$\qquad\langle 4\rangle\ \forall c \in 0 \,..\, card : \exists q \in$ SUBSET $acsNodes : Cardinality(q) = c \land \forall x \in q, y \in acsNodes \setminus q : npTS[x]$

$\qquad\quad\langle 5\rangle$ DEFINE $P(c) \triangleq c \leq card \Rightarrow \exists q \in$ SUBSET $acsNodes : Cardinality(q) = c \land \forall x \in q, y \in acsNode$

$\qquad\quad\langle 5\rangle 1.$ SUFFICES ASSUME TRUE PROVE $\forall c \in Nat : P(c)$ OBVIOUS

$\qquad\quad\langle 5\rangle 2.\ P(0)$ BY $\langle 3\rangle 9$, $FS\_EmptySet$

$\qquad\quad\langle 5\rangle 3.\ \forall c \in Nat : P(c) \Rightarrow P(c + 1)$

$\qquad\qquad\langle 6\rangle 1.$ TAKE $c \in Nat$

$\qquad\qquad\langle 6\rangle 2.$ HAVE $P(c)$

$\qquad\qquad\langle 6\rangle 3.$ HAVE $c + 1 \leq card$

$\qquad\qquad\langle 6\rangle 4.$ PICK $q \in$ SUBSET $acsNodes : Cardinality(q) = c \land (\forall x \in q, y \in acsNodes \setminus q : npTS[x] \geq np$

$\qquad\qquad\langle 6\rangle 5.$ PICK $x \in (acsNodes \setminus q) : \forall xx \in acsNodes \setminus q : npTS[x] \geq npTS[xx]$

$\qquad\qquad\quad\langle 7\rangle 1.\ Cardinality(acsNodes) \geq c + 1$ BY $\langle 6\rangle 3$, $\langle 3\rangle 9$

$\qquad\qquad\quad\langle 7\rangle 2.\ Cardinality(q) = c$ BY $\langle 6\rangle 4$

$\qquad\qquad\quad\langle 7\rangle$ DEFINE $Q \triangleq acsNodes \setminus q$

$\qquad\qquad\quad\langle 7\rangle 3.\ Q \neq \{\}$ BY $\langle 7\rangle 1$, $\langle 7\rangle 2$, FS_Subset

$\qquad\qquad\quad\langle 7\rangle 4.\ IsFiniteSet(Q)$ BY $\langle 3\rangle 8$, FS_Subset

$\qquad\qquad\quad\langle 7\rangle 5.\ Q \in$ SUBSET $acsNodes$ BY DEF $TypeOK$

$\qquad\qquad\quad\langle 7\rangle 6.$ PICK $tt \in \{npTS[xx] : xx \in Q\} : \forall ttt \in \{npTS[xx] : xx \in Q\} : ttt \leq tt$

$\qquad\qquad\qquad\langle 8\rangle$ DEFINE $QTS \triangleq \{npTS[xx] : xx \in Q\}$

$\qquad\qquad\qquad\langle 8\rangle$ HIDE DEF Q

$\qquad\qquad\qquad\langle 8\rangle 1.\ npTS \in [acsNodes \rightarrow Time]$ BY DEF $TypeOK$

$\langle 8\rangle 2.$ $QTS \neq \{\}$BY ONLY $\langle 7\rangle 3$, $\langle 7\rangle 5$, $\langle 8\rangle 1$
$\langle 8\rangle 3.$ $QTS \in$ SUBSET NatBY DEF $TypeOK$, Q
$\langle 8\rangle 4.$ $IsFiniteSet(QTS)$BY ONLY $\langle 7\rangle 4$, FS_Image
$\langle 8\rangle 5.$ $\exists\, tt \in QTS : \forall\, x \in QTS : tt \geq x$BY ONLY $\langle 8\rangle 2$, $\langle 8\rangle 3$, $\langle 8\rangle 4$, $NatSubsetHasMax$
$\langle 8\rangle 6.$ PICK $tt \in QTS : \forall\, x \in QTS : tt \geq x$BY $\langle 8\rangle 5$
$\langle 8\rangle 7.$ WITNESS $tt \in QTS$
$\langle 8\rangle 8.$ QED BY $\langle 8\rangle 6$
$\langle 7\rangle 7.$ $\exists\, nn \in Q : npTS[nn] = tt$BY ONLY $\langle 7\rangle 6$, $\langle 7\rangle 3$, $TypeOK$ DEF $TypeOK$
$\langle 7\rangle 8.$ PICK $nn \in Q : \; npTS[nn] = tt$BY $\langle 7\rangle 7$
$\langle 7\rangle 9.$ WITNESS $nn \in Q$
$\langle 7\rangle$ QED BY $\langle 7\rangle 6$, $\langle 7\rangle 8$
$\langle 6\rangle 6.$ $q \cup \{x\} \in$ SUBSET $acsNodes$BY $\langle 6\rangle 4$, $\langle 6\rangle 5$
$\langle 6\rangle 7.$ WITNESS $q \cup \{x\} \in$ SUBSET $acsNodes$
$\langle 6\rangle 8.$ $IsFiniteSet(q)$BY $\langle 3\rangle 8$, $\langle 6\rangle 4$, FS_Subset
$\langle 6\rangle 9.$ $Cardinality(q \cup \{x\}) = c + 1$BY $FS\_AddElement$, $\langle 6\rangle 5$, $\langle 6\rangle 4$, $\langle 6\rangle 8$
$\langle 6\rangle 10.$ $\forall\, xx \in q \cup \{x\},\ y \in acsNodes \setminus (q \cup \{x\}) : npTS[xx] \geq npTS[y]$
$\langle 7\rangle 1.$ TAKE $xx \in q \cup \{x\},\ y \in acsNodes \setminus (q \cup \{x\})$
$\langle 7\rangle 2.$CASE $xx \; = x$BY $\langle 7\rangle 2$, $\langle 6\rangle 5$
$\langle 7\rangle 3.$CASE $xx \; \in q$BY $\langle 7\rangle 3$, $\langle 6\rangle 4$
$\langle 7\rangle 4.$ QED BY $\langle 7\rangle 2$, $\langle 7\rangle 3$
$\langle 6\rangle 11.$ QED BY $\langle 6\rangle 9$, $\langle 6\rangle 10$
$\langle 5\rangle 4.$ HIDE DEF P
$\langle 5\rangle 5.$ QED BY $\langle 5\rangle 2$, $\langle 5\rangle 3$, $NatInduction$
$\langle 4\rangle$ QED BY $\langle 3\rangle 8$, $\langle 3\rangle 9$, $\langle 3\rangle 10$, $\langle 2\rangle 8$, FS_Subset, $FS\_CardinalityType$, $SubsetsAllCardinalities$
$\langle 3\rangle 12.$ $q \in FQuorums \wedge \forall\, x \in q,\ y \in acsNodes \setminus q : npTS[x] \geq npTS[y]$BY $\langle 3\rangle 11$, $\langle 3\rangle 6$ DEF $FQuorums$
$\langle 3\rangle 13.$ $q \in FQuorums$BY $\langle 3\rangle 11$, $\langle 3\rangle 6$ DEF $FQuorums$
$\langle 3\rangle 14.$ WITNESS $q \in FQuorums$
$\langle 3\rangle$ QED BY $\langle 3\rangle 12$, $\langle 3\rangle 14$
$\langle 2\rangle 11.$ $\forall\, x \in BatchRqs : x \leq ts$
$\langle 3\rangle 1.$ TAKE $x \in BatchRqs$
$\langle 3\rangle 2.$ $x \in Requests \wedge BatchRq(x)$BY $\langle 3\rangle 1$ DEF $BatchRqs$
$\langle 3\rangle 3.$ PICK $xf1q \in F1Quorums : xf1q \subseteq acsNodes \wedge \forall\, n \in xf1q : x \in npRq[n]$BY $\langle 3\rangle 2$ DEF $BatchRq$
$\langle 3\rangle 4.$ $xf1q \setminus fq \; \neq \{\}$
$\langle 4\rangle 1.$ $Cardinality(xf1q) = F + 1$BY $\langle 3\rangle 3$ DEF $F1Quorums$
$\langle 4\rangle 2.$ $Cardinality(fq) = F$BY $\langle 2\rangle 10$ DEF $FQuorums$
$\langle 4\rangle 3.$ $F \in Nat$BY $ByzantineAssms$
$\langle 4\rangle 4.$ $xf1q \subseteq Nodes \wedge fq \subseteq Nodes$BY $\langle 3\rangle 3$, $\langle 2\rangle 10$ DEF $F1Quorums$, $FQuorums$
$\langle 4\rangle 5.$ $IsFiniteSet(xf1q) \wedge IsFiniteSet(fq)$BY $\langle 4\rangle 4$, $ConstantAssms$, FS_Subset
$\langle 4\rangle 6.$ QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 5$, FS_Subset
$\langle 3\rangle 6.$ $\forall\, n \in (xf1q \setminus fq) : \forall\, r \in npRq[n] : r \leq ts$
$\langle 4\rangle 0.$ $xf1q \setminus fq \subseteq acsNodes$BY $\langle 2\rangle 10$, $\langle 3\rangle 3$
$\langle 4\rangle 10.$ TAKE $xn \in (xf1q \setminus fq)$
$\langle 4\rangle 11.$ TAKE $xr \in npRq[xn]$
$\langle 4\rangle 12.$ $xr \in Nat$BY $\langle 4\rangle 11$, $\langle 4\rangle 0$, $ConstantAssms$ DEF $TypeOK$, $Requests$
$\langle 4\rangle 13.$ $ts \in Nat$BY $ConstantAssms$

$\langle 4\rangle 14.\ npTS[xn] \in Nat$ BY $\langle 4\rangle 10$, $\langle 4\rangle 0$, $ConstantAssms$ DEF $TypeOK$
$\langle 4\rangle 1b.\ npTS[xn] \leq ts$
  $\langle 5\rangle 1.\ xn \in acsNodes$ BY $\langle 4\rangle 10$, $\langle 4\rangle 0$
  $\langle 5\rangle 2.\ xn \notin fq$ BY $\langle 4\rangle 10$
  $\langle 5\rangle 3.\ \land\ ts \in SubsetTS(acsNodes \setminus fq)$
    $\land\ \forall\, xx \in SubsetTS(acsNodes \setminus fq) : ts \geq xx$
    $\land\ \forall\, xx \in SubsetTS(fq) : ts \leq xx$
    BY $\langle 2\rangle 10$ DEF $BatchTS$
  $\langle 5\rangle q.$ QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEF $SubsetTS$
$\langle 4\rangle 2b.\ xr \leq npTS[xn]$
  $\langle 5\rangle$ $ProposalValid(xn)$ BY $\langle 4\rangle 0$ DEF $Init$
  $\langle 5\rangle$ QED BY DEF $ProposalValid$
$\langle 4\rangle$ QED BY ONLY $\langle 4\rangle 1b$, $\langle 4\rangle 2b$, $\langle 4\rangle 12$, $\langle 4\rangle 13$, $\langle 4\rangle 14$
$\langle 3\rangle 7.\ \exists\, n \in (xf1q \setminus fq) : x \in npRq[n]$ BY $\langle 3\rangle 4$, $\langle 3\rangle 3$
$\langle 3\rangle$ QED BY $\langle 3\rangle 6$, $\langle 3\rangle 7$
$\langle 2\rangle$ QED BY $\langle 2\rangle 11$
$\langle 1\rangle 2.\ Invariant \land [Next]_{vars} \Rightarrow Invariant'$
  $\langle 2\rangle 1.$ SUFFICES ASSUME $Invariant$ PROVE $[Next]_{vars} \Rightarrow Invariant'$
    OBVIOUS
  $\langle 2\rangle 2.$ UNCHANGED $vars \Rightarrow (Invariant')$
    BY $\langle 2\rangle 1$ DEF $vars$, $Invariant$, $BatchRq$, $BatchRqs$, $BatchTS$,
      $ProposalValid$, $SubsetTS$, $TSQuorums$
  $\langle 2\rangle 3.$ SUFFICES ASSUME $Next$ PROVE $Invariant'$
    BY $\langle 2\rangle 2$
  $\langle 2\rangle 4.$ QED BY $\langle 2\rangle 1$, $\langle 2\rangle 3$ DEF $vars$, $Next$, $Invariant$, $BatchRq$,
    $BatchRqs$, $BatchTS$, $ProposalValid$, $SubsetTS$, $TSQuorums$
$\langle 1\rangle q.$ QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, PTL, $SpecTypeOK$ DEF $Spec$, $vars$

Counter-example with $Nodes = 101 \,..\, 104$, $Byzantine = \{104\}$, $Time = 1 \,..\, 3$:
$PropposedRq$: (101 :> {1} @@ 102 :> {1} @@ 103 :> {2} @@ 104 :> {2}),
$PropposedTS$: (101 :> 1 @@ 102 :> 1 @@ 103 :> 2 @@ 104 :> 1),
$BatchRq$: {1, 2},
$BatchTS$: 1