MODULE $TLCVDFConsensus$

EXTENDS $Integers$, $FiniteSets$

CONSTANTS

$p1,\ p2,\ p3$

$P \triangleq \{p1,\ p2,\ p3\}$
$B \triangleq \{p1\}$
$tAdv \triangleq 2$
$tWB \triangleq 3$ the adversary has a $1.5x$ advantage

We use the following definition to bound the state-space for the model-checker
$MaxTick \triangleq 9$
$MCTick \triangleq 0\,..\,MaxTick$
$MCRound \triangleq 0\,..\,(MaxTick \% tWB)$
$MCMessageID \triangleq 0\,..\,(MCRound * Cardinality(P))$

VARIABLES $messages,\ messageCount,\ pendingMessage,\ tick,\ doneTick$, pc

INSTANCE $VDFConsensus$

$TickConstraint \triangleq tick \leq MaxTick$

$Canary1 \triangleq \neg($
$\quad \forall\, p \in P : doneTick[p] > 5$
$)$

Check that the adversary can indeed outpace the round number of well-behaved nodes:
$Canary2 \triangleq \neg($
$\quad tick = 6 \land \exists\, m \in messages : m.sender = p1 \land m.round = 2$
$)$

The TLC model-checker confirms all the assumptions below.

ASSUME $Intersection(\{\{1,\ 2\},\ \{2,\ 3\}\}) = \{2\}$
ASSUME $Intersection(\{\}) = \{\}$
ASSUME $Intersection(\{\{1,\ 2\},\ \{3,\ 4\}\}) = \{\}$

$m1 \triangleq [id \mapsto 1,\ round \mapsto 0,\ coffer \mapsto \{\}]$ well-behaved message
$m2 \triangleq [id \mapsto 2,\ round \mapsto 0,\ coffer \mapsto \{\}]$ well-behaved message
$m3 \triangleq [id \mapsto 3,\ round \mapsto 0,\ coffer \mapsto \{\}]$ malicious message
$m4 \triangleq [id \mapsto 4,\ round \mapsto 1,\ coffer \mapsto \{m1,\ m2\}]$ well-behaved message
$m5 \triangleq [id \mapsto 5,\ round \mapsto 1,\ coffer \mapsto \{m1,\ m2,\ m3\}]$ well-behaved message
$m6 \triangleq [id \mapsto 6,\ round \mapsto 1,\ coffer \mapsto \{m1,\ m3\}]$ malicious message

ASSUME $\neg ConsistentSet(\{m1,\ m2,\ m3\})$
ASSUME $ConsistentSet(\{m4,\ m5\})$
ASSUME $\neg ConsistentSet(\{m4,\ m5,\ m6\})$

ASSUME $ConsistentChain(\{m1,\ m2,\ m3\})$
ASSUME $ConsistentChain(\{m1,\ m2,\ m4,\ m5\})$
ASSUME $\neg ConsistentChain(\{m1,\ m2,\ m3,\ m4,\ m5\})$ $m3$ is not a predecessor of $m4$
ASSUME $\neg ConsistentChain(\{m1,\ m2,\ m3,\ m4,\ m5,\ m6\})$ $\{m4,\ m5,\ m6\}$ is not even consistent

ASSUME $HeaviestConsistentChain(\{m1,\ m2,\ m3\}) = \{m1,\ m2,\ m3\}$

Now we have a problem: the heaviest consistent chain in $\{m1,\ m2,\ m3,\ m4,\ m5\}$ does not have all the well-behaved messages. That's because both $\{m1,\ m2,\ m3,\ m5\}$ and $\{m1,\ m2,\ m4,\ m5\}$ are consistent chains, and we break ties arbitrarily. Should we make more recent messages heavier?

ASSUME $HeaviestConsistentChain(\{m1,\ m2,\ m3,\ m4,\ m5\}) = \{m1,\ m2,\ m3,\ m5\}$ oops