## MODULE *VDFConsensus*

EXTENDS *FiniteSets*, *Naturals*

CONSTANTS
    $P$ the set of processes
, $B$ the set of malicious processes
, $tAdv$ the time it takes for a malicious process to produce a message
, $tWB$ the time it takes for a well-behaved process to produce a message

ASSUME $B \subseteq P$ malicious processes are a subset of all processes
$W \triangleq P \setminus B$ the set of well-behaved processes

$Tick \triangleq Nat$ a tick is a real-time clock tick
$Round \triangleq Nat$ a round is just a tag on a message

Processes build a *DAG* of messages. The message-production rate of well-behaved processes is of 1 message per *tWB* ticks, and that of malicious processes is of 1 message per *tAdv* ticks. We require that, collectively, well-behaved processes produce messages at a rate strictly higher than that of malicious processes.

ASSUME $Cardinality(W) * tAdv > Cardinality(B) * tWB$

$MessageID \triangleq Nat$

A message consists of a unique *ID*, a round number, and a pointer to a set of previous messages:

$Message \triangleq [id : MessageID,\ round : Round,\ pred : \text{SUBSET}\ MessageID]$

We will need the intersection of a set of sets:

```
RECURSIVE $Intersection(\_)$
$Intersection(Ss) \triangleq$
    CASE
        $Ss = \{\} \rightarrow \{\}$
    □   $\exists S \in Ss : Ss = \{S\} \rightarrow$ CHOOSE $S \in Ss : Ss = \{S\}$
    □   OTHER $\rightarrow$
            LET $S \triangleq$ (CHOOSE $S \in Ss$ : TRUE)
            IN  $S \cap Intersection(Ss \setminus \{S\})$
```

A set of messages is consistent when the intersection of the sets of predecessors of each message is a strict majority of the predecessors of each message.

```
$ConsistentSet(M) \triangleq$
    LET $I \triangleq Intersection(\{m.pred : m \in M\})$
    IN  $\forall m \in M : 2 * Cardinality(I) > Cardinality(m.pred)$
```

A consistent chain is a subset of the messages in the *DAG* that potentially has some dangling pointers (*i.e.* messages that have predecessors not in the chain) and that satisfies the following recursive predicate:

* Any set of messages which all have a round of 0 is a consistent chain.

* A set of messages $C$ with some non-zero rounds and maximal round $r$ is a consistent chain when, with *Tip* being the set of messages in the chain that have round $r$ and *Pred* being the set of messages in the chain with round $r - 1$, *Pred* is a strict majority of the set of predecessors of each message in *Tip* and $C \setminus Tip$ is a consistent chain. (Note that this implies that *Tip* is a consistent set)

```
Max(X, Leq(_, _)) ≜
     CHOOSE m ∈ X : ∀ x ∈ X : Leq(x, m)

RECURSIVE ConsistentChain(_)
ConsistentChain(M) ≜
   IF M = {}
    THEN FALSE
    ELSE LET r ≜ Max({m.round : m ∈ M}, ≤ )IN
      ∨ r = 0
      ∨ LET Tip ≜ {m ∈ M : m.round = r}
             Pred ≜ {m ∈ M : m.round = r − 1}
         IN     ∧ ∀ m ∈ Tip :
                   ∧ Pred ⊆ m.pred
                   ∧ 2 ∗ Cardinality(Pred) > Cardinality(m.pred)
                ∧ ConsistentChain(M \ Tip)
```

Given a message *DAG*, the heaviest consistent chain is a consistent chain in the *DAG* that has a maximal number of messages.

```
HeaviestConsistentChain(M) ≜
   LET r ≜ Max({m.round : m ∈ M}, ≤ )
        Cs ≜ {C ∈ SUBSET M : ConsistentChain(C)}
   IN
       IF Cs = {} THEN {}
        ELSE Max(Cs, LAMBDA C1, C2 : Cardinality(C1) ≤ Cardinality(C2))

VARIABLES
   messages \∗ the messages produced so far
 , wellBehavedMessages \∗ the set of message IDs produced by well-behaved processes
 , pendingCoffer \∗ coffer on which the VDF is being computed
 , tick \∗ number of elapsed ticks

\∗ TODO: PlusCal?

TypeOK ≜
   ∧ messages ∈ SUBSET Message
   ∧ wellBehavedMessages ∈ SUBSET MessageID

Init ≜
   ∧ messages = {}
   ∧ wellBehavedMessages = {}
   ∧ tick = 0
```

```
Next $\triangleq$
    $\land$ CASE
            tick % $tWB = 0 \rightarrow$
                LET $r$ $\triangleq$ tick $\div tWB$IN
                    $\exists\, M \in$ SUBSET messages :
                        $\land$ $wellBehavedMessages \subseteq M$
                        $\land$ $pendingCoffer$' $= \{m \in HeaviestConsistentChain(M) : m.round = r\}$
        $\Box$ tick % $tWB = tWB - 1 \rightarrow$
                messages' = messages $\cup \{[id \mapsto tick,\ round \mapsto tick \div tWB,\ pred \mapsto pendingCoffer]\}$

        ELSE TRUE
    $\land$ tick' = tick + 1
```