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

$Ss = \{\} \rightarrow \{\}$

$\Box$ $\exists S \in Ss : Ss = \{S\} \rightarrow \text{CHOOSE } S \in Ss : Ss = \{S\}$

$\Box$ OTHER $\rightarrow$

LET $S \triangleq (\text{CHOOSE } S \in Ss : \text{TRUE})$

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)

$$
\begin{array}{l}
Max(X,\ Leq(\_,\ \_)) \ \triangleq \\
\quad \textsc{choose}\ m \in X : \forall\, x \in X : Leq(x,\ m)
\end{array}
$$

$$
\begin{array}{l}
\textsc{recursive}\ \ ConsistentChain(\_) \\
ConsistentChain(M) \ \triangleq \\
\quad \textsc{if}\ M = \{\} \\
\quad\ \ \textsc{then}\ \textsc{false} \\
\quad\ \ \textsc{else}\ \ \textsc{let}\ r \ \triangleq\ Max(\{m.round : m \in M\},\ \leq)\ \textsc{in} \\
\qquad\quad \lor\ \ r = 0 \\
\qquad\quad \lor\ \ \textsc{let}\ Tip \ \triangleq\ \{m \in M : m.round = r\} \\
\qquad\qquad\qquad\quad Pred \ \triangleq\ \{m \in M : m.round = r - 1\} \\
\qquad\qquad\quad \textsc{in}\quad \land\ \ \forall\, m \in Tip : \\
\qquad\qquad\qquad\qquad \land\ \ Pred \subseteq m.pred \\
\qquad\qquad\qquad\qquad \land\ \ 2 * Cardinality(Pred) > Cardinality(m.pred) \\
\qquad\qquad\qquad\quad\ \ \land\ \ ConsistentChain(M \setminus Tip)
\end{array}
$$

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

$$
\begin{array}{l}
HeaviestConsistentChain(M) \ \triangleq \\
\quad \textsc{let}\ r \ \triangleq\ Max(\{m.round : m \in M\},\ \leq) \\
\qquad\quad Cs \ \triangleq\ \{C \in \textsc{subset}\ M : ConsistentChain(C)\} \\
\quad \textsc{in} \\
\qquad \textsc{if}\ Cs = \{\}\ \textsc{then}\ \{\} \\
\qquad\ \ \textsc{else}\ \ Max(Cs,\ \textsc{lambda}\ \ C1,\ C2 : Cardinality(C1) \leq Cardinality(C2))
\end{array}
$$