

EXTENDS *Naturals*

CONSTANT

indexApprovedSet, approved indices
timestampSet, timestamps
ancillaryDataSet, miscellaneous data
currencySet, currencies for rewards
rewardSet, possible rewards
proposerBond, proposer bond as a function of index
disputerBond, disputer bond as a function of index
livenessPeriod, window for disputes after proposal
accounts, Ethereum accounts
answerSet, possible answers to all requests
storeContractID, *UMA*'s Address
escrowAddress dummy address for conservation of money

ASSUME *escrowAddress* \in *accounts*

ASSUME *storeContractID* \in *accounts*

ASSUME *proposerBond* \in [*indexApprovedSet* \rightarrow *Nat*]

ASSUME *disputerBond* \in [*indexApprovedSet* \rightarrow *Nat*]

ASSUME *livenessPeriod* \in *Nat*

ASSUME *rewardSet* \subseteq *Nat*

VARIABLE

requestSet, outstanding requests
proposeSet, outstanding proposals
disputeSet, outstanding disputes
acceptSet, expired proposals and resolved disputes
balanceOf, *ETH* balance as a function of address
time time ticks

requests \triangleq

[*identifier* : *indexApprovedSet*,
timestamp : *timestampSet*,
ancillaryData : *ancillaryDataSet*,
currency : *currencySet*,
reward : *rewardSet*,
requestAddress : *accounts*]

proposals \triangleq

[*requestItem* : *requests*,
timestamp : *timestampSet*,
answer : *answerSet*,
proposeAddress : *accounts*]

$$\begin{aligned}
disputes &\triangleq \\
&[proposeItem : proposals, \\
×tamp : timestampSet, \\
&disputeAddress : accounts] \\
accepts &\triangleq \\
&[proposeOrDisputeItem : proposals \cup disputes, \\
&answer : answerSet, \\
&identifier : indexApprovedSet, \\
×tamp : timestampSet] \\
requestAction(requestItem, currentTime) &\triangleq \\
&\wedge requestItem.timestamp = currentTime \\
&\wedge balanceOf[requestItem.requestAddress] \geq requestItem.reward \\
&\wedge requestSet' = requestSet \cup \{requestItem\} \\
&\wedge balanceOf' = [balanceOf \text{ EXCEPT } !.requestItem.requestAddress = @ - requestItem.reward, \\
&\hspace{15em} !.escrowAddress = @ + requestItem.reward] \\
&\wedge time' = time + 1 \\
&\wedge \text{UNCHANGED } \langle disputeSet, acceptSet, proposeSet \rangle \\
requestActionExists &\triangleq \\
&\exists requestItem \in requests : requestAction(requestItem, time) \\
proposeAction(proposeItem, currentTime) &\triangleq \\
\text{LET } index &\triangleq proposeItem.requestItem.identifier \\
proposerAddress &\triangleq proposeItem.proposeAddressIN \\
&\wedge proposeItem.requestItem \in requestSet \\
&\wedge proposeItem.timestamp = currentTime \\
&\wedge balanceOf[proposeItem.proposeAddress] \geq proposerBond[index] \\
&\wedge proposeSet' = proposeSet \cup \{proposeItem\} \\
&\wedge requestSet' = requestSet \setminus \{proposeItem.requestItem\} \\
&\wedge balanceOf' = [balanceOf \text{ EXCEPT } !.proposerAddress = @ - \\
&\hspace{15em} proposerBond[index] + \\
&\hspace{15em} proposeItem.requestItem.reward, \\
&\hspace{15em} !.escrowAddress = @ + \\
&\hspace{15em} proposerBond[index] - \\
&\hspace{15em} proposeItem.requestItem.reward] \\
&\wedge time' = time + 1 \\
&\wedge \text{UNCHANGED } \langle acceptSet, disputeSet \rangle \\
proposeActionExists &\triangleq \\
&\exists proposeItem \in proposals : proposeAction(proposeItem, time)
\end{aligned}$$

$$\begin{aligned}
& \wedge \text{acceptSet}' = \text{acceptSet} \cup \{\text{acceptItem}\} \\
& \wedge \text{time}' = \text{time} + 1 \\
& \wedge \text{UNCHANGED } \langle \text{requestSet}, \text{proposeSet} \rangle \\
\text{dvmActionExists} & \triangleq \\
& \exists \text{acceptItem} \in \text{accepts}, \\
& \text{dvmResult} \in \text{BOOLEAN}, \\
& \text{dvmAnswer} \in \text{answerSet} : \text{dvmAction}(\text{acceptItem}, \text{dvmResult}, \text{dvmAnswer}, \text{time}) \\
\text{proposeExpire}(\text{acceptItem}, \text{currentTime}) & \triangleq \\
& \wedge \text{acceptItem.proposeOrDisputeItem} \in \text{proposeSet} \\
& \wedge \text{acceptItem.identifier} = \text{acceptItem.proposeOrDisputeItem.requestItem.identifier} \\
& \wedge \text{acceptItem.answer} = \text{acceptItem.proposeOrDisputeItem.answer} \\
& \wedge \text{acceptItem.timestamp} = \text{currentTime} \\
& \wedge \text{currentTime} \geq \text{acceptItem.proposeOrDisputeItem.proposeTimeStamp} + \text{livenessPeriod} \\
& \wedge \text{proposeSet}' = \text{proposeSet} \setminus \{\text{acceptItem.proposeOrDisputeItem}\} \\
& \wedge \text{acceptSet}' = \text{acceptSet} \cup \{\text{acceptItem}\} \\
& \wedge \text{time}' = \text{time} + 1 \\
& \wedge \text{UNCHANGED } \langle \text{requestSet}, \text{disputeSet}, \text{balanceOf} \rangle \\
\text{proposeExpireExists} & \triangleq \\
& \exists \text{acceptItem} \in \text{accepts} : \text{proposeExpire}(\text{acceptItem}, \text{time}) \\
\text{timeAdvance} & \triangleq \\
& \wedge \text{time}' = \text{time} + 1 \\
& \wedge \text{UNCHANGED } \langle \text{acceptSet}, \text{requestSet}, \text{proposeSet}, \text{disputeSet}, \text{balanceOf} \rangle \\
\text{Init} & \triangleq \\
& \wedge \text{acceptSet} = \{\} \\
& \wedge \text{requestSet} = \{\} \\
& \wedge \text{proposeSet} = \{\} \\
& \wedge \text{disputeSet} = \{\} \\
& \wedge \text{balanceOf} \in [\text{accounts} \rightarrow \text{Nat}] \\
& \wedge \text{time} = 0 \\
\text{Next} & \triangleq \\
& \vee \text{requestActionExists} \\
& \vee \text{proposeActionExists} \\
& \vee \text{disputeActionExists} \\
& \vee \text{dvmActionExists} \\
& \vee \text{proposeExpireExists} \\
& \vee \text{timeAdvance} \\
\text{vars} & \triangleq \langle \text{acceptSet}, \text{requestSet}, \text{proposeSet}, \text{disputeSet}, \text{balanceOf}, \text{time} \rangle \\
\text{Spec} & \triangleq \text{Init} \wedge \Box[\text{Next}]_{\text{vars}}
\end{aligned}$$
