MODULE *BitSnark*

This module specifies the transaction flow in the *bitSNARK* protocol.

EXTENDS *Naturals*

VARIABLES

All published transactions.

blockchain,

Balances of the participants.

balances

$$
\begin{aligned}
&\mathit{Transactions} \triangleq \{ \\
&\quad \text{“Proof”},\ \text{“Uncontested Proof”},\ \text{“Challenge”},\ \text{“Uncontested Challenge”}, \\
&\quad \text{“State”},\ \text{“Uncontested State”},\ \text{“Select”},\ \text{“Uncontested Select”}, \\
&\quad \text{“Argument”},\ \text{“Uncontested Argument”},\ \text{“Proof Refuted”} \\
&\}
\end{aligned}
$$

$$\mathit{StartingBalances} \triangleq [\mathit{prover} \mapsto 2,\ \mathit{verifier} \mapsto 1,\ \mathit{locked} \mapsto 0]$$

$$\mathit{IsProofValid} \triangleq \text{CHOOSE } v \in \{\text{TRUE, FALSE}\} : \text{TRUE}$$

Invariants.

$$
\begin{aligned}
&\mathit{TypeOK} \triangleq \\
&\quad \land \quad \mathit{blockchain} \subseteq \mathit{Transactions} \\
&\quad \land \quad \text{DOMAIN } \mathit{balances} = \{\text{“prover”},\ \text{“verifier”},\ \text{“locked”}\}
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Sum}(bs) &\triangleq bs[\text{“prover”}] + bs[\text{“verifier”}] + bs[\text{“locked”}] \\
\mathit{ValueOK} &\triangleq \mathit{Sum}(\mathit{balances}) = \mathit{Sum}(\mathit{StartingBalances})
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{IncentiveOK} \triangleq \\
&\quad \land \text{“Proof Refuted”} \in \mathit{blockchain} \Rightarrow \\
&\qquad \mathit{balances}[\text{“verifier”}] \geq \mathit{StartingBalances}[\text{“verifier”}] \\
&\quad \land \text{“Uncontested Argument”} \in \mathit{blockchain} \Rightarrow \\
&\qquad \mathit{balances}[\text{“prover”}] \geq \mathit{StartingBalances}[\text{“prover”}]
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{AllOK} \triangleq \\
&\quad \land \mathit{TypeOK} \\
&\quad \land \mathit{ValueOK} \\
&\quad \land \mathit{IncentiveOK}
\end{aligned}
$$

Transaction Functions.

$$
\begin{aligned}
&\mathit{Proof} \triangleq \\
&\quad \land \mathit{blockchain} = \{\} \\
&\quad \land \mathit{blockchain}' = \mathit{blockchain} \cup \{\text{“Proof”}\} \\
&\quad \land \mathit{balances}' = [\mathit{balances} \text{ EXCEPT } ![\text{“prover”}] = @ - 2,\ ![\text{“locked”}] = @ + 2]
\end{aligned}
$$

$UncontestedProof \triangleq$
$\land$ "Proof" $\in blockchain$
$\land \{$"Uncontested Proof", "Challenge", "State"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Uncontested Proof"$\}$
$\land balances' = [balances \text{ EXCEPT } ![$"locked"$] = @ - 2, ![$"prover"$] = @ + 2]$

$Challenge \triangleq$
$\land$ "Proof" $\in blockchain$
$\land \{$"Uncontested Proof", "Challenge", "State"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Challenge"$\}$
$\land balances' = [balances \text{ EXCEPT } ![$"verifier"$] = @ - 1, ![$"locked"$] = @ + 1]$

$UncontestedChallenge \triangleq$
$\land$ "Challenge" $\in blockchain$
$\land \{$"State", "Uncontested Challenge"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Uncontested Challenge"$\}$
$\land balances' = [balances \text{ EXCEPT } ![$"locked"$] = @ - 3, ![$"verifier"$] = @ + 3]$

$State \triangleq$
$\land$ "Proof" $\in blockchain$
$\land \{$"Uncontested Proof", "Challenge", "State"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"State"$\}$
$\land$ UNCHANGED $balances$

$UncontestedState \triangleq$
$\land$ "State" $\in blockchain$
$\land \{$"Select", "Uncontested State"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Uncontested State"$\}$
$\land balances' = [balances \text{ EXCEPT } ![$"locked"$] = @ - 3, ![$"prover"$] = @ + 3]$

$Select \triangleq$
$\land$ "State" $\in blockchain$
$\land \{$"Uncontested State", "Select"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Select"$\}$
$\land$ UNCHANGED $balances$

$UncontestedSelect \triangleq$
$\land$ "Select" $\in blockchain$
$\land \{$"Argument", "Uncontested Select"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Uncontested Select"$\}$
$\land balances' = [balances \text{ EXCEPT } ![$"locked"$] = @ - 3, ![$"verifier"$] = @ + 3]$

$Argument \triangleq$
$\land$ "Select" $\in blockchain$
$\land \{$"Uncontested Select", "Argument"$\} \cap blockchain = \{\}$
$\land blockchain' = blockchain \cup \{$"Argument"$\}$
$\land$ UNCHANGED $balances$

$UncontestedArgument \triangleq$
$\land$ "Argument" $\in$ $blockchain$
$\land$ {"Uncontested Argument", "Proof Refuted"} $\cap$ $blockchain = \{\}$
$\land$ $blockchain' = blockchain \cup$ {"Uncontested Argument"}
$\land$ $balances' = [balances$ EXCEPT ![“locked”] $= @ - 3$, ![“prover”] $= @ + 3]$

$ProofRefuted \triangleq$
$\land$ "Argument" $\in$ $blockchain$
$\land$ {"Uncontested Argument", "Proof Refuted"} $\cap$ $blockchain = \{\}$
$\land$ $IsProofValid =$ FALSE
$\land$ $blockchain' = blockchain \cup$ {"Proof Refuted"}
$\land$ $balances' = [balances$ EXCEPT ![“locked”] $= @ - 3$, ![“verifier”] $= @ + 3]$

Flow.

$Init \triangleq$
$\land$ $blockchain = \{\}$
$\land$ $balances = StartingBalances$

$Next \triangleq$
$\lor$ $Proof$
$\lor$ $UncontestedProof$
$\lor$ $Challenge$
$\lor$ $UncontestedChallenge$
$\lor$ $State$
$\lor$ $UncontestedState$
$\lor$ $Select$
$\lor$ $UncontestedSelect$
$\lor$ $Argument$
$\lor$ $UncontestedArgument$
$\lor$ $ProofRefuted$