MODULE *BitSnark*

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

EXTENDS *Naturals*

CONSTANTS

The size of the verification program.

PROGRAM_SIZE,

Size of the prover stake.

PROVER_STAKE,

Size of the verifier payment.

VERIFIER_PAYMENT

VARIABLES

All published transactions, with counters for transactions that can appear more than once.

blockchain,

statesCounter,

selectsCounter,

The number of *contentioned* instructions.

contentioned,

Balances of the protocol – "prover", "verifier" and "locked".

balances

The set of all allowed transactions
(remember that *State* and *Select* can be published more than once - hence the counters).

$Transactions \triangleq \{$
"Proof", "Uncontested Proof", "Challenge", "Uncontested Challenge",
"State", "Uncontested State", "Select", "Uncontested Select",
"Argument", "Uncontested Argument", "Proof Refuted"$\}$

$StartingBalances \triangleq [prover \mapsto PROVER\_STAKE,\ verifier \mapsto VERIFIER\_PAYMENT,\ locked \mapsto 0]$

$Init \triangleq$
$\land\ blockchain = \{\}$
$\land\ statesCounter = 0$
$\land\ selectsCounter = 0$
$\land\ contentioned = PROGRAM\_SIZE$
$\land\ balances = StartingBalances$

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

Invariants.

$TypeOK \triangleq$
$\land\quad blockchain \subseteq Transactions$
$\land\quad$ DOMAIN $balances = \{$"prover", "verifier", "locked"$\}$

$Sum(bs) \triangleq bs[$"prover"$] + bs[$"verifier"$] + bs[$"locked"$]$

$ValueOK \triangleq Sum(balances) = Sum(StartingBalances)$

$IncentiveOK \triangleq$
$\quad \land$ "Proof Refuted" $\in blockchain \Rightarrow$
$\quad\quad balances[\text{"verifier"}] \geq StartingBalances[\text{"verifier"}]$
$\quad \land$ "Uncontested Argument" $\in blockchain \Rightarrow$
$\quad\quad balances[\text{"prover"}] \geq StartingBalances[\text{"prover"}]$

$AllOK \triangleq$
$\quad \land TypeOK$
$\quad \land ValueOK$
$\quad \land IncentiveOK$

Transaction Functions.

$Proof \triangleq$
$\quad \land blockchain = \{\}$
$\quad \land blockchain' = blockchain \cup \{\text{"Proof"}\}$
$\quad \land balances' = [balances \text{ EXCEPT } ![\text{"prover"}] = @ - 2,\ ![\text{"locked"}] = @ + 2]$
$\quad \land \text{UNCHANGED } statesCounter$
$\quad \land \text{UNCHANGED } selectsCounter$
$\quad \land \text{UNCHANGED } contentioned$

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

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

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

$\land$ UNCHANGED $statesCounter$
$\land$ UNCHANGED $selectsCounter$
$\land$ UNCHANGED $contentioned$

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

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

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

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

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

$\land$ UNCHANGED $selectsCounter$
$\land$ UNCHANGED $contentioned$

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

$ProofRefuted \triangleq$
$\land$ "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"$] = @ + 3]$
$\land$ UNCHANGED $statesCounter$
$\land$ UNCHANGED $selectsCounter$
$\land$ UNCHANGED $contentioned$

Flow.

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