MODULE *Bitcoin*

Specifies the behaviour of the bitcoin blockchain and transactions

EXTENDS *Sequences*, *Naturals*, *FiniteSets*

CONSTANTS *TXID*,
InputSeqNo,
Amount,
ScriptPubKey, Script for outputs
ScriptSig Script for inputs

VARIABLES
transactions, Set of all transactions
spent Function of output to input it spends

Input for a transaction has an id, sequence number and a *scriptPubKey*

$Input \triangleq [txid : TXID,\ seqno : InputSeqNo,\ scriptPubKey : ScriptPubKey]$

Output for a transaction has a *scriptSig* and an amount

$Output \triangleq [scriptSig : ScriptSig,\ amount : Amount]$

Transaction is a set of inputs and outputs.

It is a coinbase transaction if inputs are empty.

$Transaction \triangleq [inputs : Input,\ outputs : Output]$

$vars \triangleq \langle transactions,\ spent \rangle$

$NoInputVal \triangleq \text{CHOOSE } v : v \notin Input$

$Init \triangleq$
$\quad \land\ spent = [output \in Output \mapsto NoInputVal]$

$TypeInvariant \triangleq$
$\quad \land\ spent \in [Output \to Input]$

An output is spendable if it is not market spent.

$IsSpendableOutput(output) \triangleq$
$\quad \land\ spent[output] = NoInputVal$

Does the output *scriptSig* match the input *scriptPubKey* For now, we are working with strings being equal. There is no scripting support.

$ScriptMatch(output,\ input) \triangleq$
$\quad \land\quad output.scriptSig = input.scriptPubKey$

Create a new transaction and add it immediately to the set of transactions.

Mark output as spent by the given input

We don't spec block creation, broadcast of txs and blocks or coinbase txs

$$
\begin{aligned}
&GenerateTransaction(output,\ input) \triangleq \\
&\quad \land\ output \notin \text{UNION } \{tx.outputs : tx \in transactions\} \\
&\quad \land\ input \notin \text{UNION } \{tx.inputs : tx \in transactions\} \\
&\quad \land\ IsSpendableOutput(output) \\
&\quad \land\ ScriptMatch(output,\ input) \\
&\quad \land\ spent' = [spent \text{ EXCEPT } ![output] = input] \\
&\quad \land\ transactions' = Append(transactions, \\
&\qquad\qquad\qquad\qquad [inputs : \{input\},\ outputs : \{output\}])
\end{aligned}
$$

$$
\begin{aligned}
&Next \triangleq \\
&\quad \exists\, output \in Output,\ input \in Input : \\
&\qquad \lor\ SpendOutput(output,\ input) \\
&\qquad \lor\ GenerateTransaction(output,\ input)
\end{aligned}
$$

$$Spec \triangleq Init \land \Box[Next]_{vars}$$

Safety

$AllOutputsAreSpent$
$AllSpendScriptsMatch$

Liveness
$AllInputsWithMatchingOutputAreSpent$
