MODULE *BitcoinTransactionsSpec*

This *Spec* is used to run a model against the *BitcoinTransactions* module.

By moving the model and the runner here, we allow other modules like *LNContracts* to freely use *BitcoinTransactions* and run their own models.

EXTENDS *BitcoinTransactions*

$vars \triangleq \langle chain\_height,\ transactions,\ mempool,\ published \rangle$

$Init \triangleq$
- $\land\ transactions = [id \in TXID \mapsto [inputs \mapsto \langle\rangle,\ outputs \mapsto \langle\rangle]]$
- $\land\ chain\_height = 0$
- $\land\ mempool = \{\}$
- $\land\ published = [id \in TXID \mapsto NoSpendHeight]$

$TypeOK \triangleq$
- $\land\ transactions \in [TXID \to [inputs : Seq(Input),\ outputs : Seq(Output)]]$
- $\land\ mempool \in \text{SUBSET } TXID$
- $\land\ published \in [TXID \to Int]$

$Next \triangleq$
- $\lor \exists\, k \in Keys,\ id \in TXID,\ a \in AMOUNT :$
  - $\lor\ AddP2WKHCoinbaseToMempool(id, \langle k \rangle, a)$
- $\lor \exists\, keys \in Keys \times Keys,\ id \in TXID,\ amount \in AMOUNT :$
  - $\lor\ AddMultisigCoinbaseToMempool(id, keys, amount)$
- $\lor \exists\, id \in TXID,\ a \in AMOUNT,\ input\_type \in OutputTypes,\ output\_type \in OutputTypes :$
  $AddSpendTxToMempool(id, a, input\_type, output\_type)$
- $\lor\ \exists\, id \in TXID : ConfirmMempoolTx(id)$

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