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*

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

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

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

$ChooseKey(k) \triangleq \text{CHOOSE } e \in KEY : e \neq k$

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

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