
MODULE *Contracts*

EXTENDS *Integers*,
TLC,
Sequences

CONSTANTS

CSV, The csv value to use in contracts
Height The height up to which we run the spec

Channel contracts only ever have two parties

$Party \triangleq \{\text{"alice"}, \text{"bob"}\}$

For the first revocation we only need two keys per party

$NumKey \triangleq 2$

Set of all keys

$Key \triangleq \forall p \in Party, k \in 0 \dots NumKey - 1 : \langle p, k \rangle$

Value to capture missing *CSV* in output

$NoCSV \triangleq \text{CHOOSE } c : c \notin 0 \dots CSV$

Multisig outputs without *CSV* encumbrance

$MultiSigOutput \triangleq \forall a, b \in Party \times Party : \langle a, b, NoCSV \rangle$

Multisig outputs with *CSV* encumbrance

$MultiSigWithCSVOutput \triangleq \forall a, b \in Party \times Party : \langle a, b, CSV \rangle$

P2PKH outputs, without encumbrance

$P2PKH \triangleq Key$

$AllOutput \triangleq MultiSigOutput \cup MultiSigWithCSVOutput \cup P2PKH$

$NoOutput \triangleq \text{CHOOSE } o : o \notin AllOutput$

Set of all signatures for all commit txs. The signature in real world is related to the commit transaction, however, leave out this complication of how the signature is generated. If there is a signature by a key on a tx, it is assumed it is correctly signed as per bitcoin's requirements

$Sig \triangleq \forall p \in Party, k \in 0 \dots NumKey - 1 : \langle p, k \rangle$

Value to capture unsigned transactions

$NoSig \triangleq \text{CHOOSE } s : s \notin Sig$

Define the commitment tx type. We don't have *HTLCs* yet. We also don't filter outputs to the party here. We leave that for actions, or we'll add the filter when needed.

$CommitmentTx \triangleq [$
 $party \mapsto Party,$

$$\begin{aligned}
& outputs \mapsto Seq(AllOutput), \\
& local_sig \mapsto Sig \cup NoSig, \\
& remote_sig \mapsto Sig \cup NoSig
\end{aligned}$$

]

VARIABLES

$commitment_txs$ The set of all commiment transactions for both parties

$vars \triangleq \langle commitment_txs \rangle$

$Init \triangleq$
 $\wedge commitment_txs = \forall p \in Party : [p \rightarrow \langle \rangle]$

$TypeInvariant \triangleq$
 $\wedge commitment_txs \in CommitmentTx$
