MODULE *htlc*

Specifications for the *HTLC* sending and forwarding. The protocol is composed of a number of actions like initiate, update, expire. These actions collectively specify how the state of each node and the balance on each channel can change.

EXTENDS *Integers*

CONSTANTS *Node*, *InitialBalance*

Channels are unidirectional in the spec. This helps us track states and balances for the purposes of the specifications.

$$\textsc{variables}\ \ \begin{array}{l} channel\_states, \\ channel\_balances \end{array}$$

$$vars \triangleq \langle channel\_states,\ channel\_balances \rangle$$

$$update\_states \triangleq \{\text{“ready”},\ \text{“pending”},\ \text{“in\_latest\_commit\_tx”},\ \text{“prev\_commit\_tx\_revoked”}\}$$

Initialise with any given initial balance and ready state

$$\begin{array}{l} Init \triangleq \\ \quad \land \forall \langle m,\ n \rangle \in Node \times Node : \\ \qquad \land\ channel\_balances[\langle m,\ n \rangle] = \textsc{choose}\ b : b \in InitialBalance \\ \qquad \land\ channel\_states[\langle m,\ n \rangle] = \text{“ready”} \end{array}$$

$$\begin{array}{ll} TypeInvariant \triangleq & \\ \quad \land\ channel\_balances \in [Node \times Node \rightarrow InitialBalance] & \text{channel balance} \\ \quad \land\ channel\_states \in [Node \times Node \rightarrow channel\_states] & \text{channels } htlc \text{ state} \end{array}$$

When invoked on channel $\langle a,\ b \rangle$. The commit transaction of b is affected.

$$\begin{array}{l} update\_add\_htlc(channel,\ amount) \triangleq \\ \quad \land\ commit\_txs[channel] = \text{“ready”} \\ \quad \land\ commit\_txs' = [commit\_txs\ \ \textsc{except}\ ![channel] = \text{“pending”}] \end{array}$$