MODULE *formal*

EXTENDS *Integers*, *Sequences*

CONSTANT *accounts*, *initialBalances*

VARIABLE *balances*, *msgs*

$$
\begin{aligned}
&\mathit{Init} \triangleq \mathit{balances} = \mathit{initialBalances} \\
&\quad \land \quad \mathit{msgs} = \{\}
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{DbUpdate} \triangleq \mathit{msgs} \neq \{\} \\
&\qquad \land \text{LET } \mathit{msg} \triangleq \text{CHOOSE } \mathit{msg} \in \mathit{msgs} : \text{TRUE} \\
&\qquad\quad \text{IN} \quad \mathit{msgs}' = \mathit{msgs} \setminus \{\mathit{msg}\} \\
&\qquad\quad \land \quad \mathit{balances}' = [\mathit{balances} \text{ EXCEPT } ![\mathit{msg}.\mathit{account}] = \mathit{msg}.\mathit{amount}]
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{TransferMoney}(\mathit{from}, \mathit{to}, \mathit{amount}) \triangleq \mathit{balances}[\mathit{from}] - \mathit{amount} \geq 0 \text{ Account needs to have enough balance, from pr} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \land \quad \mathit{msgs}' = \mathit{msgs} \cup \{[\mathit{account} \mapsto \mathit{from}, \mathit{amount} \mapsto \mathit{balances}[\mathit{from}] - \mathit{amount} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad [\mathit{account} \mapsto \mathit{to}, \mathit{amount} \mapsto \mathit{balances}[\mathit{to}] + \mathit{amount}]\} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \land \quad \text{UNCHANGED } \langle \mathit{balances} \rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{Next} \triangleq \mathit{DbUpdate} \\
&\quad \lor \quad \land \exists\, \mathit{from}, \mathit{to} \in \mathit{accounts} : \\
&\qquad\quad \exists\, \mathit{amount} \in 1 \,..\, \mathit{balances}[\mathit{from}] : \text{ Send only positive integers, from property testing} \\
&\qquad\qquad\quad \mathit{TransferMoney}(\mathit{from}, \mathit{to}, \mathit{amount}) \\
&\qquad\quad \land \forall\, \mathit{acc} \in \mathit{accounts} : \mathit{balances}[\mathit{acc}] > 0
\end{aligned}
$$

INVARIANTS

$$
\mathit{TypeOK} \triangleq \mathit{msgs} \subseteq [\mathit{account} : \mathit{accounts}, \mathit{amount} : \mathit{Int}] \text{ Amount has to be an integer, from static typing}
$$

$$
\mathit{BalancesAlwaysPositive} \triangleq \forall\, \mathit{acc} \in \mathit{accounts} : \mathit{balances}[\mathit{acc}] \geq 0
$$

$$
\begin{aligned}
&\mathit{TotalMoneyStable} \triangleq \text{LET } \mathit{Sum}(\mathit{balance}) \triangleq [x, y \in \mathit{accounts} \mapsto \mathit{balance}[x] + \mathit{balance}[y]] \\
&\qquad\qquad\qquad\qquad\qquad\quad \text{IN} \quad \mathit{Sum}(\mathit{initialBalances}) = \mathit{Sum}(\mathit{balances})
\end{aligned}
$$

* Modification History
* Last modified Sun *Aug* 08 20:56:01 *CEST* 2021 by *rchaves*
* Created Sat *Aug* 07 23:59:18 *CEST* 2021 by *rchaves*