```
──────────────────── MODULE TransactionV2 ────────────────────

EXTENDS Integers, Sequences

CONSTANT accounts, initialBalances

VARIABLE balances, msgs

Init ≜ balances = initialBalances
    ∧  msgs = {}

DbUpdate ≜ msgs ≠ {}
           ∧ LET msg ≜ CHOOSE msg ∈ msgs : TRUE
             IN  msgs′ = msgs \ {msg}
              ∧  balances′ = [[balances EXCEPT ![msg.from] = msg.amount_from]
                                        EXCEPT ![msg.to] = msg.amount_to]

TransferMoney(from, to, amount) ≜ balances[from] − amount ≥ 0  Account needs to have enough balance, from pro
                               ∧  msgs′ = msgs ∪ {[from ↦ from
                                                 , to ↦ to
                                                 , amount_from ↦ balances[from] − amount
                                                 , amount_to ↦ balances[to] + amount
                                                 ]}
                               ∧  UNCHANGED ⟨balances⟩

Next ≜ DbUpdate
    ∨  ∧ ∃ from, to ∈ accounts :
           from ≠ to ∧ ∃ amount ∈ 1 . . balances[from] :  Send only positive integers, from property testing
             TransferMoney(from, to, amount)
       ∧ ∀ acc ∈ accounts : balances[acc] > 0

INVARIANTS

TypeOK ≜ msgs ⊆ [from : accounts, to : accounts, amount_from : Int, amount_to : Int]

BalancesAlwaysPositive ≜ ∀ acc ∈ accounts : balances[acc] ≥ 0

RECURSIVE SumBalance(_, _, _)

SumBalance(accs, bal, total) ≜ IF accs = {}
                                 THEN total
                                 ELSE LET acc ≜ CHOOSE acc ∈ accs : TRUE
                                      IN  SumBalance(accs \ {acc}, bal, total + bal[acc])

TotalMoneyStable ≜ SumBalance(accounts, initialBalances, 0) = SumBalance(accounts, balances, 0)

──────────────────────────────────────────────────────────────
```

* Modification History

* Last modified Sun *Aug* 08 22:59:55 *CEST* 2021 by *rchaves*

\ * Created Sun *Aug* 08 21:06:07 *CEST* 2021 by *rchaves*