MODULE *BossWorker*

EXTENDS *Naturals*, *FiniteSets*

Specification of the *BossWorker* smart contract

CONSTANT *possibleWorkers*, *possibleClaims*
VARIABLES *rollupsPhase*, *workerStatus*, *correctClaim*, *claimStatus*, *bossStatus*

Useful global definitions

RollupsPhase $\triangleq$
$\{$"InputAccumulation", receiving inputs (correct claim may change)
"ClaimSuggestion", workers can suggest claims and the boss can remove them
"ClaimSubmission"$\}$ anyone can submit suggested claims

WorkerStatus $\triangleq$
$\{$"Unemployed", worker does nothing
"Employed"$\}$ worker can suggest claims

ClaimStatus $\triangleq$
$\{$"NotSuggested", no worker has suggested such claim
"Suggested"$\}$ some worker has suggested this claim

BossStatus $\triangleq$
$\{$"Idle", boss is not prompted to do anything
"Prompted", boss is prompted to validate suggested claims
"NotHappy", boss is not happy with claim
"Happy"$\}$ boss is happy with claim (final state until new epoch)

EmployedWorkers $\triangleq$
$\{worker \in possibleWorkers : workerStatus[worker] = \text{"Employed"}\}$

UnemployedWorkers $\triangleq$
$\{worker \in possibleWorkers : workerStatus[worker] = \text{"Unemployed"}\}$

SuggestedClaims $\triangleq$
$\{claim \in possibleClaims : claimStatus[claim] = \text{"Suggested"}\}$

EmptyClaimStatus $\triangleq$

$[claim \in possibleClaims \mapsto$ "NotSuggested"$]$

Invariants

$TypeOK \triangleq$
- $\land \quad workerStatus \in [possibleWorkers \to WorkerStatus]$
- $\land \quad claimStatus \in [possibleClaims \to ClaimStatus]$
- $\land \quad bossStatus \in BossStatus$
- $\land \quad rollupsPhase \in RollupsPhase$
- $\land \quad correctClaim \in possibleClaims$
- $\land \quad Cardinality(SuggestedClaims) \quad \in \{0, 1\}$
- $\land \quad Cardinality(EmployedWorkers) \in \{0, 1\}$

$CorrectSubmittableClaim \triangleq$
- $rollupsPhase =$ "ClaimSubmission" $\Rightarrow$
  - $\forall\, claim \quad \in SuggestedClaims : claim = correctClaim$

Initial state

$Init \triangleq$
- $\land\, workerStatus = [worker \in possibleWorkers \mapsto$ "Unemployed"$]$
- $\land\, claimStatus = EmptyClaimStatus$
- $\land\, rollupsPhase \in RollupsPhase$
- $\land\, correctClaim \in possibleClaims$
- $\land\, bossStatus =$ "Idle"

Worker behaviour

$WorkerSuggestsClaim \triangleq$
- $\exists\, worker \in EmployedWorkers :$
  - $\exists\, newClaim \in possibleClaims :$
    - $\land\, rollupsPhase =$ "ClaimSuggestion"
    - $\land\, SuggestedClaims = \{\}$ (cannot suggest twice)
    - $\land\, claimStatus' = [EmptyClaimStatus$ EXCEPT $![newClaim] =$ "Suggested"$]$
    - $\land$ UNCHANGED $\langle rollupsPhase, workerStatus, correctClaim, bossStatus\rangle$

Boss behaviour

$BossHiresWorker \triangleq$
- $\exists\, worker \in UnemployedWorkers :$

  The boss should not hire a worker while prompted because then a malicious worker might be able to suggest a bad claim leaving the boss with too little time to fire him and to remove the claim

  - $\land\, bossStatus =$ "Idle"
  - $\land\, EmployedWorkers = \{\}$ (cannot have multiple workers at the same time)
  - $\land\, workerStatus' = [workerStatus$ EXCEPT $![worker] =$ "Employed"$]$
  - $\land$ UNCHANGED $\langle rollupsPhase, correctClaim, claimStatus, bossStatus\rangle$

$BossFiresWorkerAndRemovesClaim \triangleq$
$\exists\, worker \in EmployedWorkers :$
$\land\ claimStatus' = EmptyClaimStatus$
$\land\ workerStatus' = [workerStatus \text{ EXCEPT } ![worker] = \text{“Unemployed”}]$
$\land$ UNCHANGED $\langle rollupsPhase, correctClaim, bossStatus\rangle$

$BossIsPrompted \triangleq$
$\land\ rollupsPhase = \text{“ClaimSuggestion”}$
$\land\ bossStatus = \text{“Idle”}$
$\land\ bossStatus' = \text{“Prompted”}$
$\land$ UNCHANGED $\langle rollupsPhase, correctClaim, claimStatus, workerStatus\rangle$

$BossValidatesClaim \triangleq$
$\land\ rollupsPhase = \text{“ClaimSuggestion”}$
$\land\ bossStatus = \text{“Prompted”}$
$\land$ IF $correctClaim \in SuggestedClaims$
THEN $bossStatus' = \text{“Happy”}$
ELSE $bossStatus' = \text{“NotHappy”}$
$\land$ UNCHANGED $\langle rollupsPhase, correctClaim, claimStatus, workerStatus\rangle$

$BossGetsHappy \triangleq$
$\land\ rollupsPhase = \text{“ClaimSuggestion”}$
$\land\ bossStatus = \text{“NotHappy”}$
$\land\ EmployedWorkers = \{\}$ worker was fired
$\land\ SuggestedClaims = \{\}$ claim was removed
$\land\ bossStatus' = \text{“Happy”}$
$\land$ UNCHANGED $\langle rollupsPhase, correctClaim, claimStatus, workerStatus\rangle$

User behaviour

$UserSendsInput \triangleq$
$\land\ rollupsPhase = \text{“InputAccumulation”}$
$\land\ correctClaim' \in possibleClaims$ (machine hash changes)
$\land$ UNCHANGED $\langle rollupsPhase, workerStatus, claimStatus, bossStatus\rangle$

$UserSubmitsClaim \triangleq$
$\exists\, claim \in SuggestedClaims :$
$\land\ rollupsPhase = \text{“ClaimSubmission”}$
$\land\ claimStatus' = EmptyClaimStatus$ (new epoch, new claims)
$\land$ UNCHANGED $\langle rollupsPhase, workerStatus, correctClaim, bossStatus\rangle$

Rollups behaviour

$NextPhase \triangleq$
$\lor\ \land\ rollupsPhase = \text{“InputAccumulation”}$
$\land\ rollupsPhase' = \text{“ClaimSuggestion”}$
$\land$ UNCHANGED $\langle workerStatus, correctClaim, claimStatus, bossStatus\rangle$

$\lor \land rollupsPhase = \text{“ClaimSuggestion”}$
$\quad \land bossStatus = \text{“Happy”}$ (we assume the boss has enough time)
$\quad \land rollupsPhase' = \text{“ClaimSubmission”}$
$\quad \land \text{UNCHANGED } \langle workerStatus, correctClaim, claimStatus, bossStatus \rangle$
$\lor \land rollupsPhase = \text{“ClaimSubmission”}$
$\quad \land rollupsPhase' = \text{“InputAccumulation”}$
$\quad \land bossStatus' = \text{“Idle”}$
$\quad \land \text{UNCHANGED } \langle workerStatus, correctClaim, claimStatus \rangle$

Next state

$Next \triangleq$
$\quad \lor BossHiresWorker$
$\quad \lor BossFiresWorkerAndRemovesClaim$
$\quad \lor BossIsPrompted$
$\quad \lor BossValidatesClaim$
$\quad \lor BossGetsHappy$
$\quad \lor UserSendsInput$
$\quad \lor WorkerSuggestsClaim$
$\quad \lor UserSubmitsClaim$
$\quad \lor NextPhase$

* Modification History
* Last modified *Wed Jun* 01 00:26:15 *BRT* 2022 by *guilherme*
* Created *Mon* May 30 11:40:33 *BRT* 2022 by *guilherme*