MODULE *BossWorker*

Copyright 2022 *Cartesi Pte.* Ltd.

Licensed under the *Apache* License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://*www.apache.org*/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

EXTENDS *Naturals*, *FiniteSets*

Specification of the *BossWorker* smart contract

CONSTANT

noWorker,	*address*(0)
validWorkers,	valid addresses
noClaim,	*bytes*32(0)
validClaims	valid *byte*32 values

ASSUME

$\land\ noWorker \notin validWorkers$
$\land\ noClaim \notin validClaims$

VARIABLES

rollupsEpoch,	rollups epoch index
rollupsEpochHash,	correct rollups epoch hash
bwPhase,	boss worker view of rollups phases
bwWorker,	worker
bwSuggestedClaim,	last suggested claim
bwEpoch,	epoch of last suggested claim
bwClaimer,	worker that made last suggested claim
bwIsClaimValidated	whether the boss (off-chain) is ok with suggested claim

Useful global definitions

$BossWorkerPhase \triangleq$

{“InputAccumulation”,	receiving inputs (epoch hash may change)
“ClaimSuggestion”,	workers can suggest claims and the boss is idle
“ClaimValidation”,	workers can suggest claims and the boss is active
“ClaimSubmission”}	anyone can submit suggested claims

Invariants

$TypeOK \triangleq$

$\land\ bwPhase \in BossWorkerPhase$
$\land\ rollupsEpoch \in Nat$

$\land \quad \mathit{rollupsEpochHash} \in \mathit{validClaims}$
$\land \quad \mathit{bwWorker} \in \mathit{validWorkers} \cup \{\mathit{noWorker}\}$
$\land \quad \mathit{bwSuggestedClaim} \in \mathit{validClaims} \cup \{\mathit{noClaim}\}$
$\land \quad \mathit{bwEpoch} \in \mathit{Nat}$
$\land \quad \mathit{bwClaimer} \in \mathit{validWorkers} \cup \{\mathit{noWorker}\}$
$\land \quad \mathit{bwIsClaimValidated} \in \textsc{boolean}$

$\mathit{CanUserSubmitClaim} \triangleq$
$\quad \land \mathit{bwPhase} = \text{“ClaimSubmission”}$
$\quad \land \mathit{bwClaimer} = \mathit{bwWorker}$
$\quad \land \mathit{bwEpoch} = \mathit{rollupsEpoch}$
$\quad \land \mathit{bwSuggestedClaim} \in \mathit{validClaims}$

$\mathit{SuggestedClaimIsCorrect} \triangleq$
$\quad \mathit{bwSuggestedClaim} = \mathit{rollupsEpochHash}$

$\mathit{SubmittableClaimIsCorrect} \triangleq$
$\quad \mathit{CanUserSubmitClaim} \Rightarrow \mathit{SuggestedClaimIsCorrect}$

Initial state

$\mathit{Init} \triangleq$
$\quad \land \mathit{rollupsEpoch} = 0$
$\quad \land \mathit{rollupsEpochHash} \in \mathit{validClaims}$ could be in any machine state
$\quad \land \mathit{bwPhase} \in \mathit{BossWorkerPhase}$ could be in any boss worker phase
$\quad \land \mathit{bwWorker} = \mathit{noWorker}$
$\quad \land \mathit{bwSuggestedClaim} = \mathit{noClaim}$
$\quad \land \mathit{bwEpoch} = 0$
$\quad \land \mathit{bwClaimer} = \mathit{noWorker}$
$\quad \land \mathit{bwIsClaimValidated} = \textsc{false}$

Worker behaviour

$\mathit{SuggestClaim} \triangleq$
$\quad \land \mathit{bwWorker} \in \mathit{validWorkers}$ (there must be a valid worker)

Workers cannot suggest a claim if they have already done so, since this would allow workers to submit bad claims right on the end of the *ClaimSuggestion* phase, leaving the boss with no reaction time.

$\quad \land \lnot(\mathit{bwClaimer} = \mathit{bwWorker} \land \mathit{bwEpoch} = \mathit{rollupsEpoch})$
$\quad \land \mathit{bwPhase} \in \{\text{“ClaimSuggestion”}, \text{“ClaimValidation”}\}$
$\quad \land \mathit{bwSuggestedClaim}' \in \mathit{validClaims}$
$\quad \land \mathit{bwEpoch}' = \mathit{rollupsEpoch}$
$\quad \land \mathit{bwClaimer}' = \mathit{bwWorker}$
$\quad \land \textsc{unchanged} \ \langle \mathit{rollupsEpoch},$
$\qquad\qquad\qquad \mathit{rollupsEpochHash},$
$\qquad\qquad\qquad \mathit{bwPhase},$
$\qquad\qquad\qquad \mathit{bwWorker},$

$$\qquad\qquad\qquad bwIsClaimValidated\rangle$$

Boss behaviour

$$\begin{aligned}
&SetWorker \triangleq \\
&\quad \land\ bwWorker' \in validWorkers \cup \{noWorker\} \\
&\quad \land\ bwIsClaimValidated = \text{FALSE} \quad \text{(boss has no reason to change worker if claim is validated)} \\
&\quad \land\ \text{UNCHANGED}\ \langle rollupsEpoch, \\
&\qquad\qquad\qquad rollupsEpochHash, \\
&\qquad\qquad\qquad bwPhase, \\
&\qquad\qquad\qquad bwSuggestedClaim, \\
&\qquad\qquad\qquad bwEpoch, \\
&\qquad\qquad\qquad bwClaimer, \\
&\qquad\qquad\qquad bwIsClaimValidated\rangle
\end{aligned}$$

$$\begin{aligned}
&ValidateClaim \triangleq \\
&\quad \land\ bwPhase = \text{“ClaimValidation”} \\
&\quad \land\ bwIsClaimValidated = \text{FALSE} \\
&\quad \land\ bwSuggestedClaim = rollupsEpochHash \\
&\quad \land\ bwClaimer = bwWorker \\
&\quad \land\ bwEpoch = rollupsEpoch \\
&\quad \land\ bwIsClaimValidated' = \text{TRUE} \\
&\quad \land\ \text{UNCHANGED}\ \langle rollupsEpoch, \\
&\qquad\qquad\qquad rollupsEpochHash, \\
&\qquad\qquad\qquad bwPhase, \\
&\qquad\qquad\qquad bwWorker, \\
&\qquad\qquad\qquad bwSuggestedClaim, \\
&\qquad\qquad\qquad bwEpoch, \\
&\qquad\qquad\qquad bwClaimer\rangle
\end{aligned}$$

User behaviour

$$\begin{aligned}
&AddInput \triangleq \\
&\quad \land\ bwPhase = \text{“InputAccumulation”} \\
&\quad \land\ rollupsEpochHash' \in validClaims \quad \text{(machine hash changes)} \\
&\quad \land\ \text{UNCHANGED}\ \langle rollupsEpoch, \\
&\qquad\qquad\qquad bwPhase, \\
&\qquad\qquad\qquad bwWorker, \\
&\qquad\qquad\qquad bwSuggestedClaim, \\
&\qquad\qquad\qquad bwEpoch, \\
&\qquad\qquad\qquad bwClaimer, \\
&\qquad\qquad\qquad bwIsClaimValidated\rangle
\end{aligned}$$

Rollups behaviour

$$NextPhase \triangleq$$

```
$\lor \land bwPhase = \text{“InputAccumulation”}$
   $\land bwPhase' = \text{“ClaimSuggestion”}$
   $\land$ UNCHANGED $\langle rollupsEpoch,$
                     $rollupsEpochHash,$
                     $bwWorker,$
                     $bwSuggestedClaim,$
                     $bwEpoch,$
                     $bwClaimer,$
                     $bwIsClaimValidated\rangle$
$\lor \land bwPhase = \text{“ClaimSuggestion”}$
   $\land bwPhase' = \text{“ClaimValidation”}$
   $\land$ UNCHANGED $\langle rollupsEpoch,$
                     $rollupsEpochHash,$
                     $bwWorker,$
                     $bwSuggestedClaim,$
                     $bwEpoch,$
                     $bwClaimer,$
                     $bwIsClaimValidated\rangle$
$\lor$  we assume the boss has enough time to make the claim valid
   $\land bwPhase = \text{“ClaimValidation”}$
   $\land bwIsClaimValidated = \text{TRUE}$
   $\land bwPhase' = \text{“ClaimSubmission”}$
   $\land$ UNCHANGED $\langle rollupsEpoch,$
                     $rollupsEpochHash,$
                     $bwWorker,$
                     $bwSuggestedClaim,$
                     $bwEpoch,$
                     $bwClaimer,$
                     $bwIsClaimValidated\rangle$
$\lor \land bwPhase = \text{“ClaimSubmission”}$
   $\land bwPhase' = \text{“InputAccumulation”}$
   $\land bwIsClaimValidated' = \text{FALSE}$
   $\land rollupsEpoch' = rollupsEpoch + 1$
   $\land$ UNCHANGED $\langle rollupsEpochHash,$
                     $bwWorker,$
                     $bwSuggestedClaim,$
                     $bwEpoch,$
                     $bwClaimer\rangle$
```

Next state

```
$Next \triangleq$
    $\lor SetWorker$
    $\lor AddInput$
    $\lor SuggestClaim$
```

$\lor \mathit{ValidateClaim}$
$\lor \mathit{NextPhase}$

* Modification History
* Last modified *Tue Jun* 21 23:27:05 *BRT* 2022 by *guilherme*
* Created *Mon* May 30 11:40:33 *BRT* 2022 by *guilherme*