Chain Transition Helper Functions

$$\mathsf{getGKeys} \in \mathsf{NewEpochState} \to \mathbb{P}\,\mathsf{KeyHash_G}$$

$$\mathsf{getGKeys}\ nes = \mathrm{dom}\ genDelegs$$

$$\textbf{where} \qquad \begin{aligned} (\_,\ \_,\ \_,\ es,\ \_,\ \_) &=\ nes \\ (\_,\ \_,\ ls,\ \_,\ \_) &=\ es \\ (\_,\ ((\_,\ \_,\ \_,\ \_,\ genDelegs,\ \_),\ \_)) &=\ ls \end{aligned}$$

$$\mathsf{updateNES} \in \mathsf{NewEpochState} \to \mathsf{BlocksMade} \to \mathsf{LState} \to \mathsf{NewEpochState}$$

$$\mathsf{updateNES}\ (e_\ell,\ b_{prev},\ \_,\ (acnt,\ ss,\ \_,\ prevPp,\ pp),\ ru,\ pd)\ b_{cur}\ ls =$$
$$\quad (e_\ell,\ b_{prev},\ b_{cur},\ (acnt,\ ss,\ ls,\ prevPp,\ pp),\ ru,\ pd)$$

$$\mathsf{chainChecks} \in \mathbb{N} \to (\mathbb{N}, \mathbb{N}, \mathsf{ProtVer}) \to \mathsf{BHeader} \to \mathsf{Bool}$$

$$\mathsf{chainChecks}\ maxpv\ (maxBHSize,\ maxBBSize,\ protocolVersion)\ bh =$$
$$\quad m \le maxpv$$
$$\quad \wedge\ \mathsf{bHeaderSize}\ bh \le maxBHSize$$
$$\quad \wedge\ \mathsf{hBbsize}\ (\mathsf{bhbody}\ bh) \le maxBBSize$$
$$\quad \textbf{where}\ (m,\ \_) := protocolVersion$$

$$\mathsf{lastAppliedHash} \in \mathsf{LastAppliedBlock}^? \to \mathsf{HashHeader}^?$$

$$\mathsf{lastAppliedHash}\ lab = \begin{cases} \diamond & lab = \diamond \\ h & lab = (\_,\ \_,\ h) \end{cases}$$

$$\mathsf{prtlSeqChecks} \to \mathsf{LastAppliedBlock}^? \to \mathsf{BHeader} \to \mathsf{Bool}$$

$$\mathsf{prtlSeqChecks}\ lab\ bh = \begin{cases} \mathsf{True} & lab = \diamond \\ s_\ell < slot \wedge b_\ell + 1 = bn \wedge ph = \mathsf{bprev}\ bhb & lab = (b_\ell,\ s_\ell,\ \_) \end{cases}$$

$$\textbf{where}$$
$$\quad bhb := \mathsf{bhbody}\ bh$$
$$\quad bn := \mathsf{bblockno}\ bhb$$
$$\quad slot := \mathsf{bslot}\ bhb$$
$$\quad ph := \mathsf{lastAppliedHash}\ lab$$

Figure 74: Helper Functions used in the CHAIN transition

$$bh := \text{bheader } block \qquad bhb := \text{bhbody } bh \qquad s := \text{bslot } bhb$$

$$\text{prtlSeqChecks } lab\ bh$$

$$\vdash nes \xrightarrow[\text{TICK}]{s} nes'$$

$$(e_1, \_, \_, \_, \_, \_) := nes$$
$$(e_2, \_, b_{cur}, es, \_, pd) := nes'$$
$$(acnt, \_, ls, \_, pp) := es$$
$$(\_, ((\_, \_, \_, \_, genDelegs, \_), (\_, \_, \_))) := ls$$
$$ne := e_1 \neq e_2$$
$$\eta_{ph} := \text{prevHashToNonce } (\text{lastAppliedHash } lab)$$

$$\text{chainChecks MaxMajorPV } (\text{maxHeaderSize } pp, \text{maxBlockSize } pp, \text{pv } pp)\ bh$$

$$\begin{matrix} pp \\ \eta_c \\ \eta_{ph} \end{matrix} \vdash \begin{pmatrix} \eta_0 \\ \eta_h \end{pmatrix} \xrightarrow[\text{TICKN}]{ne} \begin{pmatrix} \eta_0' \\ \eta_h' \end{pmatrix}$$

$$\begin{matrix} (\text{d } pp) \\ pd \\ genDelegs \\ \eta_0' \end{matrix} \vdash \begin{pmatrix} cs \\ \eta_v \\ \eta_c \end{pmatrix} \xrightarrow[\text{PRTCL}]{bh} \begin{pmatrix} cs' \\ \eta_v' \\ \eta_c' \end{pmatrix}$$

$$\begin{matrix} pp \\ acnt \end{matrix} \vdash \begin{pmatrix} ls \\ b_{cur} \end{pmatrix} \xrightarrow[\text{BBODY}]{block} \begin{pmatrix} ls' \\ b_{cur}' \end{pmatrix}$$

$$nes'' := \text{updateNES } nes'\ b_{cur}',\ ls'$$
$$lab' := (\text{bblockno } bhb,\ s,\ \text{bhash } bh)$$

$$\text{Chain} \rule{}{} \qquad (43)$$

$$\vdash \begin{pmatrix} nes \\ cs \\ \eta_0 \\ \eta_v \\ \eta_c \\ \eta_h \\ lab \end{pmatrix} \xrightarrow[\text{CHAIN}]{block} \begin{pmatrix} nes'' \\ cs' \\ \eta_0' \\ \eta_v' \\ \eta_c' \\ \eta_h' \\ lab' \end{pmatrix}$$

Figure 75: Chain rules

12.14 Byron to Shelley Transition

This section defines the valid initial Shelley ledger states and describes how to transition the state held by the Byron ledger to Shelley. The Byron ledger state CEState is defined in [BC-D1]. The valid initial Shelley ledger states are exactly the range of the function initialShelleyState defined in Figure 76. Figure 77 defines the transition function from Byron. Note that we use the hash of the final Byron header as the first evolving and candidate nonces for Shelley.

Shelley Initial States

$$\text{initialShelleyState} \in \text{LastAppliedBlock}^? \to \text{Epoch} \to \text{UTxO} \to \text{Coin} \to \text{GenesisDelegation}$$
$$\to (\text{Slot} \mapsto \text{KeyHash}_{\mathsf{G}}^?) \to \text{PParams} \to \text{Seed} \to \text{ChainState}$$

$$
\text{initialShelleyState}
\begin{pmatrix}
lab \\
e \\
utxo \\
reserves \\
genDelegs \\
pp \\
initNonce
\end{pmatrix}
=
\begin{pmatrix}
\begin{pmatrix}
\begin{pmatrix}
e \\
\varnothing \\
\varnothing \\
\begin{pmatrix} 0 \\ reserves \end{pmatrix} \\
(\varnothing, \varnothing) \\
(\varnothing, \varnothing) \\
(\varnothing, \varnothing) \\
\varnothing \\
\varnothing \\
0
\end{pmatrix} \\
\begin{pmatrix}
\begin{pmatrix} utxo \\ 0 \\ 0 \\ (\varnothing, \varnothing) \end{pmatrix} \\
\begin{pmatrix}
\begin{pmatrix} \varnothing \\ \varnothing \\ \varnothing \\ \varnothing \\ genDelegs \\ \varnothing \end{pmatrix} \\
\begin{pmatrix} \varnothing \\ \varnothing \\ \varnothing \end{pmatrix}
\end{pmatrix} \\
pp \\
pp
\end{pmatrix} \\
\diamond \\
\varnothing \\
cs \\
initNonce \\
initNonce \\
initNonce \\
0_{seed} \\
lab
\end{pmatrix}
$$

where $cs = \{hk \mapsto 0 \mid (hk, \_) \in \text{range}\, genDelegs\}$

Figure 76: Initial Shelley States

Byron to Shelley Transition

$\mathsf{toShelley} \in \mathsf{CEState} \to \mathsf{GenesisDelegation} \to \mathsf{BlockNo} \to \mathsf{ChainState}$

$$
\mathsf{toShelley} \begin{pmatrix} s_{last} \\ \overline{h} \\ (utxo,\ reserves) \\ \overline{us} \end{pmatrix} gd\ bn = \mathsf{initialShelleyState} \begin{pmatrix} (s_{last}\ bn,\ \mathsf{prevHashToNonce}\ h) \\ e \\ \mathsf{hash}\ h \\ utxo \\ reserves \\ gd \\ \mathsf{overlaySchedule}\ e\ (\mathsf{dom}\ gd)\ pp \\ pp \\ \mathsf{prevHashToNonce}\ h \end{pmatrix}
$$

where

$e = \mathsf{epoch}\ s_{last}$

$pp = \mathsf{pps}\ us$

Figure 77: Byron to Shelley State Transtition