MODULE *crosslink2*

EXTENDS *TLC*, *Naturals*, *Sequences*, *utils*

CONSTANTS *BcNodes*, *BftNodes*, *CrossLink2Nodes*
CONSTANTS *Sigma*, *L*

VARIABLES *bc_chains*, *bft_chains*, *crosslink2_chains*

INSTANCE *definitions*

$$
\begin{aligned}
&Init \triangleq \\
&\quad \land\ bc\_chains = [i \in 1 \,..\, BcNodes \mapsto \langle BcGenesisBlock \rangle] \\
&\quad \land\ bft\_chains = [i \in 1 \,..\, BftNodes \mapsto \langle BftGenesisBlock \rangle] \\
&\quad \land\ crosslink2\_chains = [i \in 1 \,..\, CrossLink2Nodes \mapsto CrossLink2GenesisBlock]
\end{aligned}
$$

$$
\begin{aligned}
&Next \triangleq \\
&\quad \lor \exists\, n \in 1 \,..\, BcNodes : \\
&\qquad \land\ bc\_chains' = [bc\_chains \text{ EXCEPT } ![n] = Append(\\
&\qquad\quad bc\_chains[ChooseBestBcChain], [\\
&\qquad\qquad context\_bft \mapsto ChooseContextBft, \\
&\qquad\qquad hash \mapsto ChooseBestBcTip + 1])] \\
&\qquad \land\ \text{UNCHANGED } \langle bft\_chains, crosslink2\_chains \rangle \\
&\quad \lor \exists\, m \in 1 \,..\, BftNodes : \\
&\qquad \land\ bft\_chains' = [bft\_chains \text{ EXCEPT } ![m] = Append(\\
&\qquad\quad bft\_chains[ChooseBestBftChain], [\\
&\qquad\qquad headers\_bc \mapsto PruneLasts(ChooseBcView, Sigma), \\
&\qquad\qquad hash \mapsto ChooseBestBftTip + 1])] \\
&\qquad \land\ \text{UNCHANGED } \langle bc\_chains, crosslink2\_chains \rangle \\
&\quad \lor \exists\, c \in 1 \,..\, CrossLink2Nodes : \\
&\qquad \land\ crosslink2\_chains' = [crosslink2\_chains \text{ EXCEPT } ![c] = [\\
&\qquad\quad fin \mapsto PruneFirsts(bc\_chains[ChooseBestBcChain], Sigma)]] \\
&\qquad \land\ \text{UNCHANGED } \langle bc\_chains, bft\_chains \rangle
\end{aligned}
$$

$$
Spec \triangleq Init \land \Box[Next]_{\langle bc\_chains,\, bft\_chains,\, crosslink2\_chains \rangle}
$$

Type checking

$$
\begin{aligned}
&BcChainsTypeCheck \triangleq bc\_chains \in Seq(Seq([context\_bft : Nat, hash : Nat])) \\
&BftChainsTypeCheck \triangleq bft\_chains \in \\
&\quad Seq(Seq([headers\_bc : Seq([context\_bft : Nat, hash : Nat]), hash : Nat])) \\
&CrossLink2ChainsTypeCheck \triangleq crosslink2\_chains \in \\
&\quad Seq([fin : Seq([context\_bft : Nat, hash : Nat])])
\end{aligned}
$$

Lemma: Linear Prefix

If $A \preceq_\star C$ and $B \preceq_\star C$ then $A \mathrel{\dot{\asymp}_\star} B$.

$$
\begin{array}{l}
\mathit{BcLinearPrefix} \triangleq \\
\quad \forall\, a,\, b,\, c \in 1\,..\,\mathit{BcNodes} : \\
\qquad \text{LET } A \triangleq \mathit{bc\_chains}[a] \\
\qquad\qquad\; B \triangleq \mathit{bc\_chains}[b] \\
\qquad\qquad\; C \triangleq \mathit{bc\_chains}[c] \\
\qquad \text{IN } \mathit{IsPrefix}(A,\, C) \wedge \mathit{IsPrefix}(B,\, C) \Rightarrow \\
\qquad\qquad \mathit{IsPrefix}(A,\, B) \vee \mathit{IsPrefix}(B,\, A)
\end{array}
$$

$$
\begin{array}{l}
\mathit{BftLinearPrefix} \triangleq \\
\quad \forall\, a,\, b,\, c \in 1\,..\,\mathit{BftNodes} : \\
\qquad \text{LET } A \triangleq \mathit{bft\_chains}[a] \\
\qquad\qquad\; B \triangleq \mathit{bft\_chains}[b] \\
\qquad\qquad\; C \triangleq \mathit{bft\_chains}[c] \\
\qquad \text{IN } \mathit{IsPrefix}(A,\, C) \wedge \mathit{IsPrefix}(B,\, C) \Rightarrow \\
\qquad\qquad \mathit{IsPrefix}(A,\, B) \vee \mathit{IsPrefix}(B,\, A)
\end{array}
$$

Definition: Agreement on a view

An execution of Π has Agreement on the view $V : \mathit{Node} \times \mathit{Time} \to \star\mathit{chain}$ iff for all times t, u and all Π nodes i, j (potentially the same) such that i is honest at time t and j is honest at time u, we have $V_i^t \mathrel{\dot{\asymp}_\star} V_j^u$.

$$
\begin{array}{l}
\mathit{BcViewAgreement} \triangleq \\
\quad \forall\, i,\, j \in 1\,..\,\mathit{BcNodes} : \\
\qquad \vee\, \mathit{IsPrefix}(\mathit{bc\_chains}[i],\, \mathit{bc\_chains}[j]) \\
\qquad \vee\, \mathit{IsPrefix}(\mathit{bc\_chains}[j],\, \mathit{bc\_chains}[i])
\end{array}
$$

$$
\begin{array}{l}
\mathit{BftViewAgreement} \triangleq \\
\quad \forall\, i,\, j \in 1\,..\,\mathit{BftNodes} : \\
\qquad \vee\, \mathit{IsPrefix}(\mathit{bft\_chains}[i],\, \mathit{bft\_chains}[j]) \\
\qquad \vee\, \mathit{IsPrefix}(\mathit{bft\_chains}[j],\, \mathit{bft\_chains}[i])
\end{array}
$$

Definition: Final agreement

An execution of $\Pi_{\star bft}$ has Final Agreement iff for all *bftvalid* blocks C in honest view at time t and $C\prime$ in honest view at time $t\prime$, we have $\mathit{bftlastfinal}(C) \mathrel{\dot{\asymp}_{bft}} \star\mathit{bftlastfinal}(C\prime)$.

$$
\begin{array}{l}
\mathit{BftFinalAgreement} \triangleq \\
\quad \forall\, i,\, j \in 1\,..\,\mathit{BftNodes} : \\
\qquad \vee\, \mathit{IsPrefix}(\mathit{BftLastFinal}(i),\, \mathit{BftLastFinal}(j)) \\
\qquad \vee\, \mathit{IsPrefix}(\mathit{BftLastFinal}(j),\, \mathit{BftLastFinal}(i))
\end{array}
$$

Definition: Prefix Consistency

An execution of $\Pi_{\star bc}$ has Prefix Consistency at confirmation depth σ, iff for all times $t \leq u$ and all nodes i, j (potentially the same) such that i is honest at time t and j is honest at time u, we have that $ch_i^t \lceil^\sigma_{\star bc} \preceq_{\star bc} ch_j^u$.

$BcPrefixConsistency \triangleq$
$\forall\, i,\, j \in 1\,..\,BcNodes :$
$Len(bc\_chains[i]) \leq Len(bc\_chains[j]) \Rightarrow$
$IsPrefix(PruneFirsts(bc\_chains[i],\, Sigma),\, bc\_chains[j])$

Definition: Prefix Agreement

An execution of $\Pi_{\star bc}$ has Prefix Agreement at confirmation depth σ iff it has Agreement on the view $(i, t) \mapsto ch_i^t\lceil^{\sigma}_{\star bc}$.

$BcPrefixAgreement \triangleq$
$\forall\, i \in 1\,..\,BcNodes :$
$IsPrefix(PruneFirsts(bc\_chains[i],\, Sigma),\, bc\_chains[i])$

Definition: *-linear

A function $S : I \to \star block$ is *-linear iff for every $t, u \in I$ where $t \leq u$ we have $S(t) \preceq_\star S(u)$

$BcLinear(T,\, U) \triangleq IsPrefix(T,\, U)$

Definition: Local finalization linearity

Node i has Local finalization linearity up to time t iff the time series of $\star bc$-blocks $fin_i^{r \leq t}$ is $\star bc$-linear.

$LocalFinalizationLinearity \triangleq \Box[$
$\forall\, i \in 1\,..\,CrossLink2Nodes :$
$BcLinear(crosslink2\_chains[i].fin,\, crosslink2\_chains'[i].fin)]_{crosslink2\_chains}$

Lemma: Local fin-depth

In any execution of Crosslink 2, for any node i that is honest at time t, there exists a time $r \leq t$ such that $fin_i \preceq ch_i^r\lceil^{\sigma}_{\star bc}$

$LocalFinDepth \triangleq$
$\forall\, i \in 1\,..\,CrossLink2Nodes :$
$IsPrefix(crosslink2\_chains[i].fin,\, bc\_chains[ChooseBestBcChain])$

Definition: Assured Finality

An execution of Crosslink 2 has Assured Finality iff for all times t, u and all nodes i, j (potentially the same) such that i is honest at time t and j is honest at time u, we have $fin_i^t \preceq_{bc} fin_j^u$.

$AssuredFinality \triangleq$
$\forall\, i,\, j \in 1\,..\,CrossLink2Nodes :$
$\lor\, IsPrefix(crosslink2\_chains[i].fin,\, crosslink2\_chains[j].fin)$
$\lor\, IsPrefix(crosslink2\_chains[j].fin,\, crosslink2\_chains[i].fin)$