MODULE *crosslink2*

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

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

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

INSTANCE *definitions*

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

$$
\begin{aligned}
&\mathit{HonestBc} \triangleq \\
&\quad \exists\, n \in 1 \,..\, \mathit{BcNodes} : \\
&\qquad \text{LET} \\
&\qquad\quad \mathit{base} \triangleq \mathit{bc\_chains}[\mathit{BestBcChainIdx}] \\
&\qquad\quad \mathit{bft} \triangleq \mathit{bft\_chains}[\mathit{BestBftChainIdx}] \\
&\qquad\quad \mathit{tip} \triangleq \text{IF } \mathit{Len}(\mathit{base}) = 0 \text{ THEN } 0 \text{ ELSE } \mathit{base}[\mathit{Len}(\mathit{base})].\mathit{hash} \\
&\qquad\quad \mathit{next} \triangleq \mathit{tip} + 1 \text{IN} \\
&\qquad \land\ \mathit{bc\_chains}' = [\mathit{bc\_chains} \text{ EXCEPT } ![n] = \mathit{Append}(\mathit{base}, [\\
&\qquad\quad \mathit{context\_bft} \mapsto \mathit{bft}[\mathit{Len}(\mathit{bft})].\mathit{hash}, \\
&\qquad\quad \mathit{hash} \mapsto \mathit{next}])] \\
&\qquad \land\ \text{UNCHANGED } \langle \mathit{bft\_chains}, \mathit{crosslink2\_chains} \rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{HonestBft} \triangleq \\
&\quad \exists\, n \in 1 \,..\, \mathit{BftNodes} : \\
&\qquad \text{LET} \\
&\qquad\quad \mathit{base} \triangleq \mathit{bft\_chains}[\mathit{BestBftChainIdx}] \\
&\qquad\quad \mathit{bc} \triangleq \mathit{bc\_chains}[\mathit{BestBcChainIdx}] \\
&\qquad\quad \mathit{tip} \triangleq \text{IF } \mathit{Len}(\mathit{base}) = 0 \text{ THEN } 0 \text{ ELSE } \mathit{base}[\mathit{Len}(\mathit{base})].\mathit{hash} \\
&\qquad\quad \mathit{next} \triangleq \mathit{tip} + 1 \\
&\qquad\quad \mathit{hdrs} \triangleq \mathit{PruneLasts}(\mathit{bc}, \mathit{Sigma}) \text{IN} \\
&\qquad \land\ \mathit{bft\_chains}' = [\mathit{bft\_chains} \text{ EXCEPT } ![n] = \mathit{Append}(\mathit{base}, [\\
&\qquad\qquad \mathit{headers\_bc} \mapsto \mathit{hdrs}, \\
&\qquad\qquad \mathit{hash} \mapsto \mathit{next}])] \\
&\qquad \land\ \text{UNCHANGED } \langle \mathit{bc\_chains}, \mathit{crosslink2\_chains} \rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{ByzantineBft} \triangleq \\
&\quad \exists\, n \in \mathit{ByzBft} : \\
&\qquad \text{LET} \\
&\qquad\quad \mathit{base} \triangleq \mathit{bft\_chains}[\mathit{BestBftChainIdx}]
\end{aligned}
$$

$bc \triangleq bc\_chains[BestBcChainIdx]$
$tip \triangleq \text{IF } Len(base) = 0 \text{ THEN } 0 \text{ ELSE } base[Len(base)].hash$

Byzantine node can create an arbitrary faulty block within a range

$byz \triangleq tip + (\text{CHOOSE } inc \in 2 \,..\, 10 : \text{TRUE})$
$hdrs \triangleq PruneLasts(bc, Sigma)\text{IN}$
$\land\ bft\_chains' = [bft\_chains \text{ EXCEPT } ![n] = Append(base, [$
$headers\_bc \mapsto hdrs,$
$hash \mapsto byz])]$
$\land \text{UNCHANGED } \langle bc\_chains, crosslink2\_chains\rangle$

$HonestCrosslink \triangleq$
$\exists\, n \in 1 \,..\, CrossLink2Nodes :$
LET
$fin \triangleq PruneFirsts(bc\_chains[BestBcChainIdx], Sigma)\text{IN}$
$\land\ crosslink2\_chains' = [crosslink2\_chains \text{ EXCEPT } ![n] = [fin \mapsto fin]]$
$\land \text{UNCHANGED } \langle bc\_chains, bft\_chains\rangle$
$\lor \text{UNCHANGED } \langle bc\_chains, bft\_chains, crosslink2\_chains\rangle$

$Next \triangleq$
$\lor HonestBc$
$\lor HonestBft$
$\lor HonestCrosslink$
$\lor ByzantineBft$

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

Type checking

$BcChainsTypeCheck \triangleq bc\_chains \in Seq(Seq([context\_bft : Nat, hash : Nat]))$
$BftChainsTypeCheck \triangleq bft\_chains \in$
$Seq(Seq([headers\_bc : Seq([context\_bft : Nat, hash : Nat]), hash : Nat]))$
$CrossLink2ChainsTypeCheck \triangleq crosslink2\_chains \in$
$Seq([fin : Seq([context\_bft : Nat, hash : Nat])])$

Assumptions

ASSUME $BftThresholdOK$

Lemma: Linear Prefix

If $A \preceq_\star C$ and $B \preceq_\star C$ then $A \asymp_\star B$.

$BcLinearPrefix \triangleq$
$\forall\, a, b, c \in 1 \,..\, BcNodes :$
LET $A \triangleq bc\_chains[a]$
$B \triangleq bc\_chains[b]$

$$
\begin{array}{l}
\quad\quad C \triangleq bc\_chains[c] \\
\quad \text{IN} \quad IsPrefix(A,\ C) \land IsPrefix(B,\ C) \Rightarrow \\
\quad\quad\quad IsPrefix(A,\ B) \lor IsPrefix(B,\ A)
\end{array}
$$

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

Definition: Agreement on a view

An execution of Π has Agreement on the view $V : Node \times Time \to \star chain$ 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 $V_i^t \preceq_\star V_j^u$.

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

$$
\begin{array}{l}
BftViewAgreement \triangleq \\
\quad \forall\, i,\ j \in HonestBftNodes : \\
\quad\quad \lor IsPrefix(bft\_chains[i],\ bft\_chains[j]) \\
\quad\quad \lor IsPrefix(bft\_chains[j],\ bft\_chains[i])
\end{array}
$$

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 $bftlastfinal(C) \preceq_{bft} \star bftlastfinal(C\prime)$.

$$
\begin{array}{l}
BftFinalAgreement \triangleq \\
\quad \forall\, i,\ j \in HonestBftNodes : \\
\quad\quad \lor IsPrefix(BftLastFinal(i),\ BftLastFinal(j)) \\
\quad\quad \lor IsPrefix(BftLastFinal(j),\ BftLastFinal(i))
\end{array}
$$

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 $ch_i^t \lceil^\sigma_{\star bc} \preceq_{\star bc} ch_j^u$.

$$
\begin{array}{l}
BcPrefixConsistency \triangleq \\
\quad \forall\, i,\ j \in 1\,..\,BcNodes : \\
\quad\quad Len(bc\_chains[i]) \leq Len(bc\_chains[j]) \Rightarrow \\
\quad\quad\quad\quad IsPrefix(PruneFirsts(bc\_chains[i],\ Sigma),\ bc\_chains[j])
\end{array}
$$

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 $fin_i \preceq ch_i^r\lceil^{\sigma}_{\star bc}$

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

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 $fin_i^t \preceq_{bc} fin_j^u$.

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