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 $definitions$

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

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

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

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

$bc \triangleq bc\_chains[BestBcChainIdx]$
$tip \triangleq base[Len(base)].hash$

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 $A \asymp_\star B$.

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

$C \triangleq bc\_chains[c]$
IN $IsPrefix(A, C) \land IsPrefix(B, C) \Rightarrow$
$IsPrefix(A, B) \lor IsPrefix(B, A)$

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

Definition: Agreement on a view

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

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

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

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

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

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 $ch_i^t \lceil_{\star bc}^{\sigma} \preceq_{\star bc} ch_j^u$.

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

Definition: Prefix Agreement

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

$$
\begin{aligned}
&\mathit{BcPrefixAgreement} \triangleq \\
&\quad \forall\, i \in 1 \,..\, \mathit{BcNodes} : \\
&\qquad \mathit{IsPrefix}(\mathit{PruneFirsts}(\mathit{bc\_chains}[i],\ \mathit{Sigma}),\ \mathit{bc\_chains}[i])
\end{aligned}
$$

Definition: *-linear

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

$$
\mathit{BcLinear}(T,\ U) \triangleq \mathit{IsPrefix}(T,\ U)
$$

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.

$$
\begin{aligned}
&\mathit{LocalFinalizationLinearity} \triangleq \Box[\\
&\quad \forall\, i \in 1 \,..\, \mathit{CrossLink2Nodes} : \\
&\qquad \mathit{BcLinear}(\mathit{crosslink2\_chains}[i].\mathit{fin},\ \mathit{crosslink2\_chains}'[i].\mathit{fin})]_{\mathit{crosslink2\_chains}}
\end{aligned}
$$

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

$$
\begin{aligned}
&\mathit{LocalFinDepth} \triangleq \\
&\quad \forall\, i \in 1 \,..\, \mathit{CrossLink2Nodes} : \\
&\qquad \mathit{IsPrefix}(\mathit{crosslink2\_chains}[i].\mathit{fin},\ \mathit{bc\_chains}[\mathit{BestBcChainIdx}])
\end{aligned}
$$

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 $fin_i^t \preceq\succeq_{bc} fin_j^u$.

$$
\begin{aligned}
&\mathit{AssuredFinality} \triangleq \\
&\quad \forall\, i,\ j \in 1 \,..\, \mathit{CrossLink2Nodes} : \\
&\qquad \lor\ \mathit{IsPrefix}(\mathit{crosslink2\_chains}[i].\mathit{fin},\ \mathit{crosslink2\_chains}[j].\mathit{fin}) \\
&\qquad \lor\ \mathit{IsPrefix}(\mathit{crosslink2\_chains}[j].\mathit{fin},\ \mathit{crosslink2\_chains}[i].\mathit{fin})
\end{aligned}
$$