```
──────────────────── 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 ≜
    ∧ bc_chains = [i ∈ 1 . . BcNodes ↦ ⟨BcGenesisBlock⟩]
    ∧ bft_chains = [i ∈ 1 . . BftNodes ↦ ⟨BftGenesisBlock⟩]
    ∧ crosslink2_chains = [i ∈ 1 . . CrossLink2Nodes ↦ CrossLink2GenesisBlock]

HonestBc ≜
   ∃ n ∈ 1 . . BcNodes :
      LET
          base  ≜ bc_chains[BestBcChainIdx]
          bft   ≜ bft_chains[BestBftChainIdx]
          tip   ≜ base[Len(base)].hash
          next  ≜ tip + 1IN
       ∧ bc_chains′ = [bc_chains EXCEPT ![n] = Append(base, [
           context_bft ↦ bft[Len(bft)].hash,
           hash ↦ next])]
       ∧ UNCHANGED ⟨bft_chains, crosslink2_chains⟩

HonestBft ≜
   ∃ n ∈ 1 . . BftNodes :
      LET
          base  ≜ bft_chains[BestBftChainIdx]
          bc    ≜ bc_chains[BestBcChainIdx]
          tip   ≜ base[Len(base)].hash
          next  ≜ tip + 1
          hdrs  ≜ PruneLasts(bc, Sigma)IN
       ∧ bft_chains′ = [bft_chains EXCEPT ![n] = Append(base, [
               headers_bc ↦ hdrs,
               hash ↦ next])]
       ∧ UNCHANGED ⟨bc_chains, crosslink2_chains⟩

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

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

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

Assumptions

```
ASSUME $BftThresholdOK$
```

Lemma: Linear Prefix

If $A \preceq_\star C$ and $B \preceq_\star C$ then $A \mathrel{\preceq\!\!\!\!\succeq}_\star B$.

```
$BcLinearPrefix \triangleq$
    $\forall\, a,\, b,\, c \in 1 \mathrel{..} BcNodes :$
        LET $A \triangleq bc\_chains[a]$
            $B \triangleq bc\_chains[b]$
            $C \triangleq bc\_chains[c]$
        IN  $IsPrefix(A,\, C) \land IsPrefix(B,\, C) \Rightarrow$
             $IsPrefix(A,\, B) \lor IsPrefix(B,\, A)$
```

```
$BftLinearPrefix \triangleq$
    $\forall\, a,\, b,\, c \in 1 \mathrel{..} BftNodes :$
        LET $A \triangleq bft\_chains[a]$
            $B \triangleq bft\_chains[b]$
            $C \triangleq bft\_chains[c]$
        IN  $IsPrefix(A,\, C) \land IsPrefix(B,\, C) \Rightarrow$
             $IsPrefix(A,\, B) \lor IsPrefix(B,\, A)$
```

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 $V_i^t \ \mathrel{\preceq\!\!\!\succeq}_{\star}\ V_j^u$.

```
$BcViewAgreement \triangleq$
    $\forall\, i,\, j \in 1 \mathrel{..} BcNodes :$
        $\lor\ IsPrefix(bc\_chains[i],\, bc\_chains[j])$
        $\lor\ IsPrefix(bc\_chains[j],\, bc\_chains[i])$
```

```
$BftViewAgreement \triangleq$
    $\forall\, i,\, j \in HonestBftNodes :$
        $\lor\ IsPrefix(bft\_chains[i],\, bft\_chains[j])$
        $\lor\ IsPrefix(bft\_chains[j],\, bft\_chains[i])$
```

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 $bftlastfinal(C) \mathrel{\preceq\!\!\!\succeq}_{bft} \star bftlastfinal(C\prime)$.

```
$BftFinalAgreement \triangleq$
    $\forall\, i,\, j \in HonestBftNodes :$
        $\lor\ IsPrefix(BftLastFinal(i),\, BftLastFinal(j))$
        $\lor\ IsPrefix(BftLastFinal(j),\, BftLastFinal(i))$
```

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

```
$BcPrefixConsistency \triangleq$
    $\forall\, i,\, j \in 1 \mathrel{..} BcNodes :$
        $Len(bc\_chains[i]) \leq Len(bc\_chains[j]) \Rightarrow$
```

$$\mathit{IsPrefix}(\mathit{PruneFirsts}(\mathit{bc\_chains}[i],\ \mathit{Sigma}),\ \mathit{bc\_chains}[j])$$

Definition: Prefix Agreement

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

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

Definition: *-linear

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

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

Definition: Local finalization linearity

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

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

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 $\mathit{fin}_i \preceq ch_i^r \lceil^{\sigma}_{\star bc}$

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

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 $\mathit{fin}_i^t \mathrel{\preceq\mkern-14mu\succeq}_{bc} \mathit{fin}_j^u$.

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

Theorem: Ledger prefix property

For any node i that is honest at time t, and any confirmation depth μ, $\mathsf{fin}_i^t \preceq (\mathsf{ba}_{\mu})_i^t$

$$\begin{array}{l}
\mathit{LedgerPrefixProperty} \triangleq \\
\quad \forall\, i \in 1 \mathrel{..} \mathit{CrossLink2Nodes} : \\
\quad\quad \mathit{IsPrefix}(\mathit{crosslink2\_chains}[i].\mathit{fin},\ \mathit{crosslink2\_chains}[i].\mathit{ba})
\end{array}$$