```
MODULE $crosslink2$
EXTENDS $TLC, Naturals, Sequences, utils$

CONSTANTS $BcNodes, BftNodes, CrossLink2Nodes$
CONSTANTS $Sigma, L$

VARIABLES $bc\_chains, bft\_chains, crosslink2\_chains$

INSTANCE $definitions$

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

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

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

Type checking

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

Lemma: Linear Prefix

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

```
$BcLinearPrefix \triangleq$
    $\forall\, i \in 1 \,..\, BcNodes :$
        $\forall\, k \in 2 \,..\, Len(bc\_chains[i]) : bc\_chains[i][k].hash \geq bc\_chains[i][k-1].hash$
```

```
$BftLinearPrefix \triangleq$
    $\forall\, i \in 1 \,..\, BftNodes :$
        $\forall\, k \in 2 \,..\, Len(bft\_chains[i]) : bft\_chains[i][k].hash \geq bft\_chains[i][k-1].hash$
```

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

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

```
$BftViewAgreement \triangleq$
    $\forall\, i, j \in 1 \,..\, BftNodes :$
        $\lor\ IsPrefix(bft\_chains[i],\ bft\_chains[j])$
        $\lor\ IsPrefix(bft\_chains[j],\ bft\_chains[i])$
```

Definition: Computable efficiently function

$\star bftlastfinal : \star bftblock \rightarrow \star bftblock \cup \{\bot\}$

```
$BftLastFinal(n) \triangleq bft\_chains[n]$
```

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

```
$BftFinalAgreement \triangleq$
    $\forall\, i, j \in 1 \,..\, BftNodes :$
        $\lor\ IsPrefix(BftLastFinal(i),\ BftLastFinal(j))$
        $\lor\ IsPrefix(BftLastFinal(j),\ BftLastFinal(i))$
```

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

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

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 ≜
    ∀ i ∈ 1 .. BcNodes :
        IsPrefix(PruneFirsts(bc_chains[i], Sigma), bc_chains[i])
```

Definition: *-linear

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

```
BcLinear(T, U) ≜ 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 ≜ □[
    ∀ i ∈ 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 ≜
    ∀ i ∈ 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 $fin_i^t \preceq\!\!\!\!\succeq_{bc} fin_j^u$.

```
AssuredFinality ≜
    ∀ i, j ∈ 1 .. CrossLink2Nodes :
        ∨ IsPrefix(crosslink2_chains[i].fin, crosslink2_chains[j].fin)
        ∨ IsPrefix(crosslink2_chains[j].fin, crosslink2_chains[i].fin)
```