
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

$\wedge bc_chains = [i \in 1 \dots BcNodes \mapsto \langle BcGenesisBlock \rangle]$

$\wedge bft_chains = [i \in 1 \dots BftNodes \mapsto \langle BftGenesisBlock \rangle]$

$\wedge crosslink2_chains = [i \in 1 \dots CrossLink2Nodes \mapsto CrossLink2GenesisBlock]$

HonestBc \triangleq

$\exists n \in 1 \dots BcNodes :$

LET

$base \triangleq bc_chains[BestBcChainIdx]$

$bft \triangleq bft_chains[BestBftChainIdx]$

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

$next \triangleq tip + 1$ IN

$\wedge bc_chains' = [bc_chains \text{ EXCEPT } ![n] = Append(base, [$
 $context_bft \mapsto bft[Len(bft)].hash,$
 $hash \mapsto next])]$

$\wedge \text{UNCHANGED } \langle bft_chains, crosslink2_chains \rangle$

HonestBft \triangleq

$\exists n \in 1 \dots BftNodes :$

LET

$base \triangleq bft_chains[BestBftChainIdx]$

$bc \triangleq bc_chains[BestBcChainIdx]$

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

$next \triangleq tip + 1$

$hdrs \triangleq PruneLasts(bc, Sigma)$ IN

$\wedge bft_chains' = [bft_chains \text{ EXCEPT } ![n] = Append(base, [$
 $headers_bc \mapsto hdrs,$
 $hash \mapsto next])]$

$\wedge \text{UNCHANGED } \langle bc_chains, crosslink2_chains \rangle$

ByzantineBft \triangleq

$\exists n \in ByzBft :$

LET

$base \triangleq bft_chains[BestBftChainIdx]$

$$\begin{aligned}
bc &\triangleq bc_chains[BestBcChainIdx] \\
tip &\triangleq base[Len(base)].hash \\
&\text{Byzantine node can create an arbitrary faulty block within a range} \\
byz &\triangleq tip + (\text{CHOOSE } inc \in 2 \dots 10 : \text{TRUE}) \\
hdrs &\triangleq PruneLasts(bc, Sigma)IN \\
\wedge bft_chains' &= [bft_chains \text{ EXCEPT } ![n] = Append(base, [\\
&\quad headers_bc \mapsto hdrs, \\
&\quad hash \mapsto byz])] \\
&\wedge \text{UNCHANGED } \langle bc_chains, crosslink2_chains \rangle \\
HonestCrosslink &\triangleq \\
&\exists n \in 1 \dots CrossLink2Nodes : \\
&\quad \text{LET} \\
&\quad \quad fin \triangleq PruneFirsts(bc_chains[BestBcChainIdx], Sigma)IN \\
&\quad \quad \wedge crosslink2_chains' = [crosslink2_chains \text{ EXCEPT } ![n] = [fin \mapsto fin]] \\
&\quad \quad \wedge \text{UNCHANGED } \langle bc_chains, bft_chains \rangle \\
&\quad \vee \text{UNCHANGED } \langle bc_chains, bft_chains, crosslink2_chains \rangle \\
Next &\triangleq \\
&\vee HonestBc \\
&\vee HonestBft \\
&\vee HonestCrosslink \\
&\vee ByzantineBft \\
Spec &\triangleq Init \wedge \Box[Next]_{\langle bc_chains, bft_chains, crosslink2_chains \rangle}
\end{aligned}$$

Type checking

$$\begin{aligned}
BcChainsTypeCheck &\triangleq bc_chains \in Seq(Seq([context_bft : Nat, hash : Nat])) \\
BftChainsTypeCheck &\triangleq bft_chains \in \\
&\quad Seq(Seq([headers_bc : Seq([context_bft : Nat, hash : Nat]), hash : Nat])) \\
CrossLink2ChainsTypeCheck &\triangleq crosslink2_chains \in \\
&\quad Seq([fin : Seq([context_bft : Nat, hash : Nat])])
\end{aligned}$$

Assumptions

ASSUME *BftThresholdOK*

Lemma: Linear Prefix

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

$$\begin{aligned}
BcLinearPrefix &\triangleq \\
&\forall a, b, c \in 1 \dots BcNodes : \\
&\quad \text{LET } A \triangleq bc_chains[a] \\
&\quad \quad B \triangleq bc_chains[b]
\end{aligned}$$

$$\begin{aligned}
C &\triangleq bc_chains[c] \\
\text{IN } &IsPrefix(A, C) \wedge IsPrefix(B, C) \Rightarrow \\
&IsPrefix(A, B) \vee IsPrefix(B, A)
\end{aligned}$$

$$\begin{aligned}
BftLinearPrefix &\triangleq \\
&\forall a, b, c \in 1 \dots BftNodes : \\
&\text{LET } A \triangleq bft_chains[a] \\
&\quad B \triangleq bft_chains[b] \\
&\quad C \triangleq bft_chains[c] \\
\text{IN } &IsPrefix(A, C) \wedge IsPrefix(B, C) \Rightarrow \\
&IsPrefix(A, B) \vee IsPrefix(B, A)
\end{aligned}$$

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 $V_i^t \star V_j^u$.

$$\begin{aligned}
BcViewAgreement &\triangleq \\
&\forall i, j \in 1 \dots BcNodes : \\
&\quad \vee IsPrefix(bc_chains[i], bc_chains[j]) \\
&\quad \vee IsPrefix(bc_chains[j], bc_chains[i])
\end{aligned}$$

$$\begin{aligned}
BftViewAgreement &\triangleq \\
&\forall i, j \in HonestBftNodes : \\
&\quad \vee IsPrefix(bft_chains[i], bft_chains[j]) \\
&\quad \vee IsPrefix(bft_chains[j], bft_chains[i])
\end{aligned}$$

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' in honest view at time t' , we have $bftlastfinal(C) \star_{bft} bftlastfinal(C')$.

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

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

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

Definition: Prefix Agreement

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

$BcPrefixAgreement \triangleq$
 $\forall i \in 1 \dots BcNodes :$
 $IsPrefix(PruneFirsts(bc_chains[i], Sigma), bc_chains[i])$

Definition: \star -linear

A function $S : I \rightarrow \star block$ is \star -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.

$LocalFinalizationLinearity \triangleq \Box[$
 $\forall i \in 1 \dots CrossLink2Nodes :$
 $BcLinear(crosslink2_chains[i].fin, crosslink2_chains'[i].fin)]_{crosslink2_chains}$

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

$LocalFinDepth \triangleq$
 $\forall i \in 1 \dots CrossLink2Nodes :$
 $IsPrefix(crosslink2_chains[i].fin, bc_chains[BestBcChainIdx])$

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 $fin_i^t \not\preceq_{bc}^u fin_j^u$.

$AssuredFinality \triangleq$
 $\forall i, j \in 1 \dots CrossLink2Nodes :$
 $\vee IsPrefix(crosslink2_chains[i].fin, crosslink2_chains[j].fin)$
 $\vee IsPrefix(crosslink2_chains[j].fin, crosslink2_chains[i].fin)$