MODULE *definitions*

LOCAL INSTANCE *Integers*
LOCAL INSTANCE *Sequences*
LOCAL INSTANCE *FiniteSets*
LOCAL INSTANCE *utils*

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

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

The genesis blocks for the chains.

$BcGenesisBlock \triangleq [context\_bft \mapsto 0,\ hash \mapsto 0]$
$BftGenesisBlock \triangleq [headers\_bc \mapsto \langle\rangle,\ hash \mapsto 0]$
$CrossLink2GenesisBlock \triangleq [fin \mapsto \langle BcGenesisBlock\rangle,\ ba \mapsto \langle BcGenesisBlock\rangle]$

Convenient sets

$HonestBftNodes \triangleq 1\,..\,BftNodes \setminus ByzBft$
$BftAllNodes \triangleq 1\,..\,BftNodes$
$BcAllNodes \triangleq 1\,..\,BcNodes$

Choose the best *BC* chain (the longest one).

$BestBcChainIdx \triangleq$
  CHOOSE $i \in BcAllNodes$:
    $Len(bc\_chains[i]) = Max(\{Len(bc\_chains[j]) : j \in BcAllNodes\})$

The number of nodes supporting the same chain as node i.

$BftSupport(i) \triangleq Cardinality(\{j \in BftAllNodes : bft\_chains[j] = bft\_chains[i]\})$

Byzantine classic fault tolerance threshold condition

$BftThresholdOK \triangleq BftNodes \geq 3 * Cardinality(ByzBft) + 1$

Choose the best *BFT* chain (the longest one with the most support).

- $Lmax =$ maximum length of all *BFT* chains
- $S =$ set of nodes having the longest chains
- $supMax =$ maximum support among the longest chains
- $T =$ set of nodes having the longest chains with the maximum support

$BestBftChainIdx \triangleq$

LET

$Lmax \triangleq Max(\{Len(bft\_chains[k]) : k \in BftAllNodes\})$

$S \triangleq \{i \in BftAllNodes : Len(bft\_chains[i]) = Lmax\}$

$supMax \triangleq Max(\{BftSupport(k) : k \in S\})$

$T \triangleq \{i \in S : BftSupport(i) = supMax\}$

IN

CHOOSE $i \in T$: TRUE

Definition: Computable efficiently function

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

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

Definition: Locally bounded-available chain

Define the locally bounded-available chain on node i for bc-confirmation-depth μ, as

$$(\mathsf{ba}_\mu)_i^t = \begin{cases} \mathsf{ch}_i^t \lceil^\mu_{\mathsf{bc}}, & \text{if } \mathsf{fin}_i^t \preceq \mathsf{ch}_i^t \lceil^\mu_{\mathsf{bc}} \\ \mathsf{fin}_i^t, & \text{otherwise} \end{cases}$$

$LocalBa(fin, bc) \triangleq$

IF $IsPrefix(fin, PruneFirsts(bc, Sigma))$ THEN

$PruneFirsts(bc, Sigma)$

ELSE

fin