**TBFT建模进度**

**摘要**

本文档介绍了Tendermint-BFT（TBFT）共识机制的核心功能，包括F\_{Auth}、F\_{Proposal}、F\_{Vote}、F\_{CSM}，以及新增的F\_{Commit}功能。F\_{Commit}功能用于最终确认共识并提交区块，并为下一轮高度做好准备。

**一、功能介绍**

（一）功能 F\_{Auth}(V, A)

初始化：设置 MsgQueue := ∅ 和 Active := 0。

– 当从验证者集合 V 中的某个 v 接收到消息 m 时，将 m 入队到 MsgQueue，并增加 Active 值。将 (MsgQueue) 发送给对手 A。

– 当从验证者集合 V 中的某个 v 接收到 (fetch) 消息时：

1. 减少 Active 值。

2. 如果 Active = 0，则从 MsgQueue 中取出一条消息并发送给 v；否则，不发送消息，并触发对手的激活。

– 当从 A 接收到 (delay, T) 消息时，如果 T 是有效的自然数，则增加 Active 值 T；否则忽略消息。

– （消息控制）：当从 A 接收到 (corrupt, v, m′, T′) 消息时，如果 Active > 0 且 T′ 有效，将 MsgQueue 中最后一条消息替换为 m′，并设置 Active := T′。

（二）功能 F\_{Proposal}(P, A)

初始化：设置 Proposal := ⊥ 和 Round := 0。

– 当为新的轮次选定提议者 p ∈ P 时，设置 Round := r 并将 Proposal := b（其中 b 是由 p 提出的有效区块）。将 (Proposal, b) 发送给对手 A。

– 当从 p 接收到 (broadcast, b) 消息时，将 Proposal 广播给 P 中的所有验证者。

– （超时处理）：当从 A 接收到 (timeout, T) 消息时，如果 T 有效，增加 Round，并选择新的提议者。

（三）功能 F\_{Vote}(P, V)

初始化：设置 Prevotes := ∅ 和 Precommits := ∅。

– 当从验证者集合 P 中的 p 接收到 (prevote, block) 消息时，将 (p, block) 添加到 Prevotes，并将其广播给 V。

– 当从验证者 p ∈ P 接收到 (precommit, block) 消息时，将 (p, block) 添加到 Precommits，并将其广播给 V。

– 当从 P 中的任意验证者 p 接收到 (collect, stage) 消息时：

1. 如果 stage = "prevote"，将 Prevotes 发送给 p。

2. 如果 stage = "precommit"，将 Precommits 发送给 p。

（四）功能 F\_{Commit}(P)

初始化: 对每个验证者 p\_i \in P，设置 C\_i := 0 表示验证者是否已提交区块。

– 收到来自 p\_i 的消息 (\text{commit}, B) 时：

1. 设置 C\_i := 1，表示 p\_i 已对区块 B 进行提交。

2. 向所有参与方 p\_j \in P 广播 (\text{commit}, B) 通知其提交状态。

3. 如果 |C| \geq \frac{2}{3} \times |P|，其中 C 为发送 (\text{commit}, B) 的验证者集合：将区块 B 标记为已完成并向所有参与方 p\_j \in P 广播 (\text{finalize}, B)。

4. 如果 |C| < \frac{2}{3} \times |P|，则区块无法完成，提交过程仍未完成。

– 收到来自任意方 p\_k 的消息 (\text{request\\_status}) 时：返回集合 C 并指示区块 B 是否已完成。

（五）功能 F\_{CSM}(V)

初始化：设置 Height := 0，Round := 0 和 LockedBlock := ⊥。

– 当从 V 中的任意验证者 v 接收到 (newHeight, h) 消息时，更新 Height := h 并将 Round 重置为 0。

– 当从 v 接收到 (newRound, r) 消息时，更新 Round := r，并准备进入新的提议阶段。

– 当从 v 接收到 (lock, block) 消息时，设置 LockedBlock := block，并确保该区块在后续轮次中有效。

– 当从 v 接收到 (queryState) 消息时，返回 (Height, Round, LockedBlock)。

**二、目前问题**

1．建模目标：对于如何实现建模的具体目标还没有太多思路，对于模型需要保证的性质还需要学习判断，应该多阅读论文来学习如何实现模型要求。

2．定理提出：对于定理证明方法的应用理解不够透彻，需要多学习优秀论文的证明方法，并且还需要继续加深对于共识协议的理解。

3．与敌手的交互：对于协议中各角色与敌手的交互操作了解还不多，需要多了解对共识协议的攻击操作，然后再来完善各功能的描述。