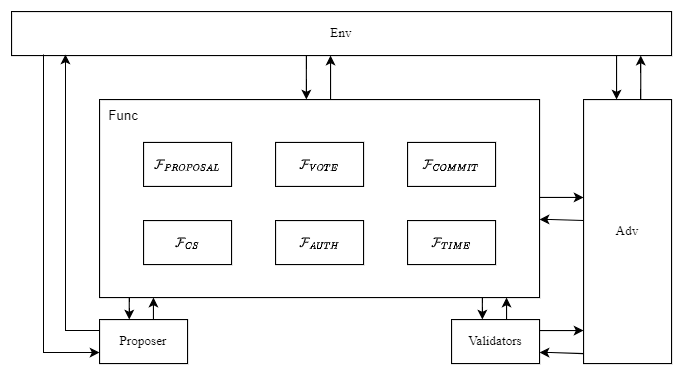
**TBFT建模进度**

**摘要**

本文档介绍了Tendermint-BFT （TBFT）共识机制的初步框架和核心功能。本文主要调整了TBFT的框架图，完善了各功能的描述，加入了F\_{TIME}功能。

1. **初步框架**



**二、功能描述**

（一）功能F\_{AUTH}(V,L(·))

初始化：变量M:=⊥和D:=0。

–当从v\_i∈V接收到输入m时，执行以下操作：

a.设置D:=1和M:=m。

b.将L(M)发送给敌手A。

c.将M广播给v\_j，(v\_j∈V, j!=i)

–当接收到来自敌手A的(delay, T)时，执行以下操作：

如果T是一个以一元表示法编码的自然数，则设置D:=D+T。否则忽略该消息。

–当从敌手A接收到消息(corrupt, v\_i, m′,T′)时，执行以下操作：

如果D>0且T′是有效的延迟值，则设置D:=T′并将M:=m′。否则忽略该消息。

（二）功能F\_{PROPOSAL}(V)

初始化：设置Proposal:=⊥和Round:=0。

–当从F\_{CS}收到消息(Proposal,⊥)时，通过Round-robin规则选定提议者Proposer∈V，设置Round:=r并将Proposal:=B（其中B是由Proposer提出的有效区块）。将(Proposal, B)发送给对手A。然后Proposer将Proposal广播给V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}(V)

初始化：设置Prevotes:=⊥和Precommits:=⊥。

–当从验证者v∈V接收到(prevote, B)消息时，将(p, B)添加到Prevotes，并将其广播给V中的所有验证者。

–当从验证者v∈V接收到(precommit, B)消息时，将(p, B)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}(V)

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

–收到来自v\_i的消息(commit, B)时：

1.设置C\_i:=1，表示v\_i已对区块B进行提交。

2.向所有参与方v\_i∈V广播(commit, B)通知其提交状态。

3.接收来自其他方的(commit, B)命令，如果B为有效区块，则设置C\_i = C\_i+1

4.如果|C|大于等于|P|，其中|C|为C\_i == 1的数量，将区块b标记为已完成并向所有参与方v\_i∈V广播(finalize, B)。

5.如果|C|小于|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(request\_status)时：返回集合C并指示区块B是否已完成。

（五）功能F\_{CS}(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, B)消息时，设置v的LockedBlock:=B,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)。

**三、目前问题**

1． 对于F\_{TIME}的引入目前还没有考虑太多方面，下周会完善这一部分。

2．各功能角色的交互逻辑还不完善，需要继续学习共识协议，加深理解，下周会完善功能内部以及和功能之间交互逻辑。