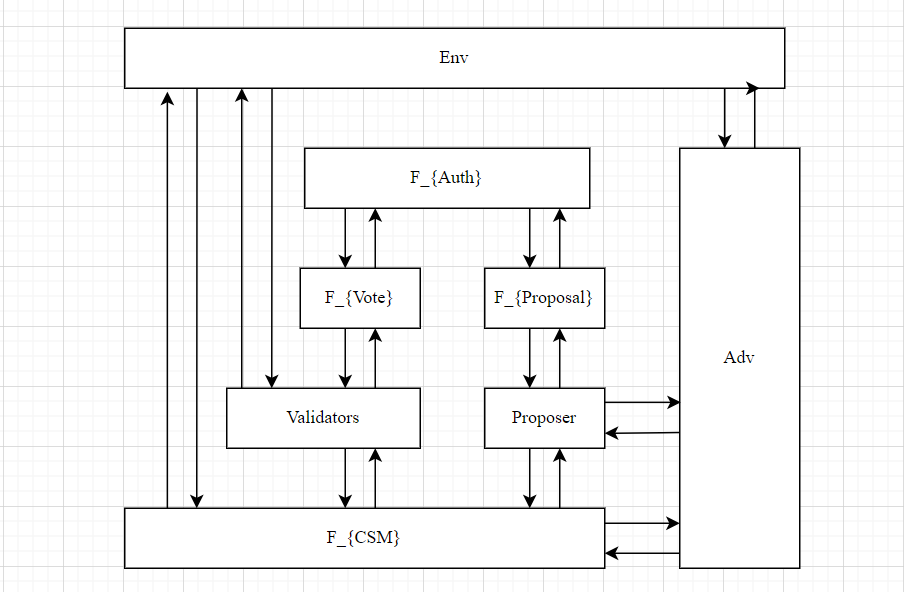
**TBFT建模进度**

**摘要**

本文档汇报了TBFT（Tendermint BFT）共识机制的建模进度，包括其整体框架、角色定义、定理及其证明。文档首先介绍了TBFT的整体框架，然后对协议中的角色进行了定义。此外，文档还尝试提出了两个定理，以证明TBFT在恶意验证者和延时攻击下的表现。

**一、整体框架**



F\_{Auth}：用于节点之间传递提议、投票和状态信息的通信协议，确保消息能够在网络中快速传播。

F\_{Vote}：用于节点对Proposal的投票，包括Prevote、Precommit和Commit，表示对区块的支持或反对。

F\_{Proposal}：用于Proposer提出Proposal

F\_{CSM}：Consensus State Machine，用于管理共识过程的状态，跟踪当前高度、提议区块、投票等信息。

**二、角色定义**

1. Validator（验证者）：负责质押资金并参与共识过程，通过投票力轮流选举出块人，并在共识中对区块提案进行投票。

2. Proposer（提议者/出块人）：每轮从Validators中选举出来，负责提出新区块提案，并触发共识过程的开始。

3. Round-based协议：共识过程通过一系列轮次循环执行，每个轮次包括提议、预投票和预提交阶段，以达成对新区块的共识。

4. 锁定机制：Validators可以锁定在特定的区块上，一旦锁定，只能对该区块进行投票，这有助于防止区块链分叉。

5. Proof of Lock Change（PoLC）：记录Validators在特定高度和轮次下，对某个区块的锁定情况，超过2/3的锁定可以触发区块的最终确认。

**三、定理**

定理一：Tendermint 共识在最多 f < n/3个验证者被恶意控制的情况下，仍能保证协议的安全性和活性（即共识的达成和正确性）。

证明：在 Tendermint 协议中，即使敌手控制的恶意验证者数量不超过总数的三分之一，协议依然能够通过诚实验证者之间的多数投票机制保证共识的安全性和活性。通过轮换提案者和超时机制，恶意验证者无法阻止协议的进展和正确的区块提案，因此共识最终能够在诚实验证者的参与下顺利达成。

定理二：Tendermint 共识协议能够容忍延迟或无效投票的攻击，并在有限时间内达成共识，不影响系统的整体吞吐量。

证明：Tendermint 协议通过预设的超时机制防御恶意验证者的投票延迟或无效投票行为。即使部分验证者企图通过延迟投票或提交无效票来影响共识，协议会通过超时进入新的轮次，并且只接受合法签名的投票，从而确保系统不会陷入停滞，同时维持较高的吞吐量和及时性。

**四、目前的问题**

1．建模流程：自己对于建模的流程掌握的还不熟练，需要通过阅读论文来摸索建模的步骤。

2．定理提出：对于建模时需要提出的定理还没有把握，不知道该从什么角度去提出问题需要继续加深对于共识协议的理解。