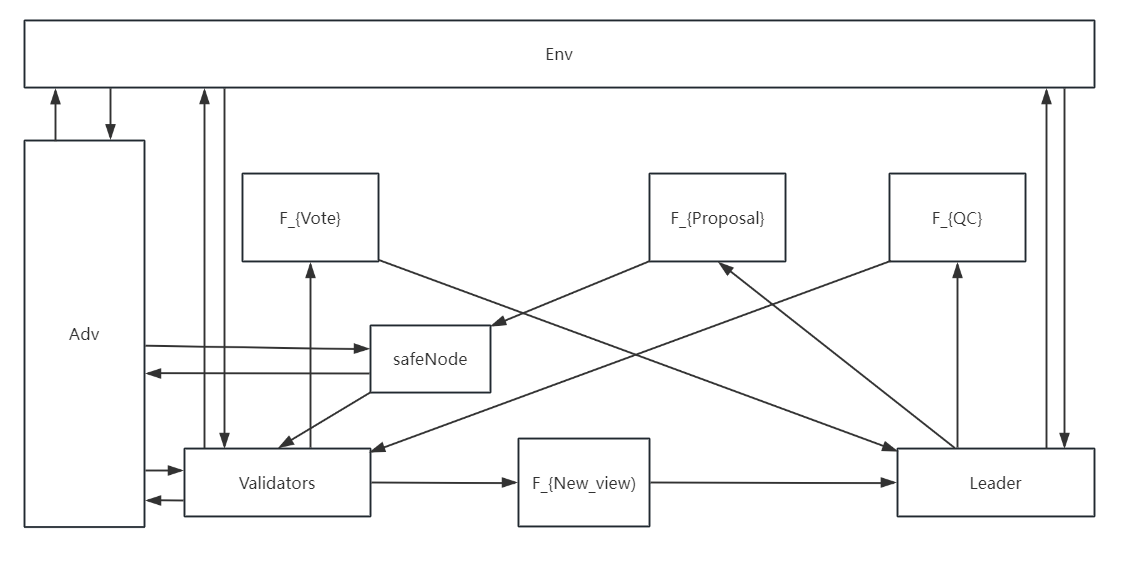
**Hotstuff建模进度**

**摘要：**

这篇文档是关于Hotstuff共识协议的11.3建模进度报告。首先是对整体框架图作了修改简化，删除了原先图中的safeNode结点。在原先的基础上提出了新的定理三和定理四，定理三：若敌手仅能访问 f<k个拜占庭节点，则其生成的部分签名不足以组合成完整签名 σ，伪造签名的概率可以忽略不计。定理四是基于不可篡改性（任意节点只有在共识达成后才能知道最终输出的数据值）提出：任意节点只有在共识达成后才能知道最终输出的数据值。

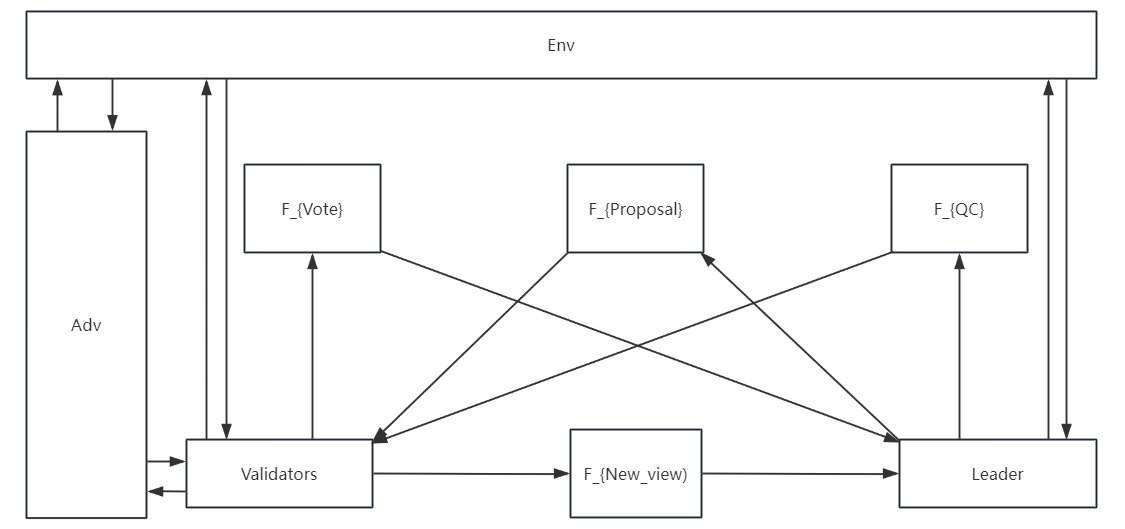
1. **整体框架图：**

**修改前：**



SafeNode：The safeNode predicate is a core ingredient of the protocol. It examines a proposal message m carrying a QC justification m.justify, and determines whether m.node is safe to accept.

**修改后：**



考虑到SafeNode应包含与理想功能F\_{Proposal}中，故在原先的图中将SafeNode结点删去。

1. **实体定义**

* **领导者（Leader）：** 在每一轮视图中有唯一的领导者负责提议区块并发起共识过程。
* **验证者（Validator）：** 验证者对领导者提议的区块进行验证并投票。每个诚实的验证者在满足协议条件的情况下参与共识投票。
* **拜占庭节点（Byzantine Nodes）：** 由敌手控制的恶意节点，可能会发送错误的区块提议或投票，试图破坏共识过程。

1. **定理**

定理一：如果两个区块B1和B2冲突，那么它们不能同时被不同的诚实节点提交。

证明：通过引入HotStuff中的锁机制，每个诚实节点在提交一个区块之前必须验证其投票的QC，并且只有在满足安全条件的情况下才能提交该区块。我们可以证明，在两个冲突的区块同时被提交的情况下，必然会导致矛盾，因为一个节点必须看到前一视图中的锁定状态，并避免与之冲突。

定理二：在拜占庭节点数量不超过f的情况下，诚实的领导者最终能够达成共识，并推动系统前进。

证明：HotStuff协议通过视图切换（view change）机制保证活性。当当前视图中的领导者无法达成共识时，协议会通过视图切换来选择下一个领导者。我们可以证明，只要网络在全局稳定时间（GST）后保持同步，正确的领导者将能够在有限时间内收集足够的投票并达成共识。

定理三：若敌手仅能访问 f<k个拜占庭节点，则其生成的部分签名不足以组合成完整签名 σ，伪造签名的概率可以忽略不计。

证明：阈值签名方案要求 k 个签名节点的部分签名才能生成 σ，在系统总共 n个节点中，假设有至多 f拜占庭节点（其中 f<k ），敌手所能利用的部分签名数量最多为 f，小于阈值 k。因此，即使敌手能够访问这些拜占庭节点的签名权限，其仍然无法获得足够的部分签名来生成有效的完整签名 σ。这意味着，敌手生成一个伪造签名的概率几乎为零。

定理四：任意节点只有在共识达成后才能知道最终输出的数据值。

证明：在 HotStuff 协议中，只有在决定阶段（decide phase）形成有效的 commitQC 后，领导者才会将最终的共识结果发送给所有其他节点。节点在收到包含 commitQC 的决定消息后才会将该数据值作为共识结果存储。由于协议的每个阶段均依赖于 (n - f) 个节点的投票，拜占庭节点无法在协议的决定阶段之前推断出最终数据值。此外，协议的安全性依赖于锁定机制（lockedQC），保证诚实节点在之前阶段无法在未达成共识的情况下确定数据值。因此，任意节点在共识达成之前无法知道最终的输出数据值，满足不可篡改性。

1. **目前存在问题**

1、建模细节：对建模的细节和整个模型的完善性没什么把握，个人认为是对于建模这项工作不够熟悉，仍需要大量阅读论文熟悉建模的流程。

2、定理提出：对于UC框架和hotstuff均不够熟悉，导致不知道引理提出该从何入手，仍需要对二者进行深入理解，并且阅读其他文章学习从什么角度提出引理并且自己能够证明它。