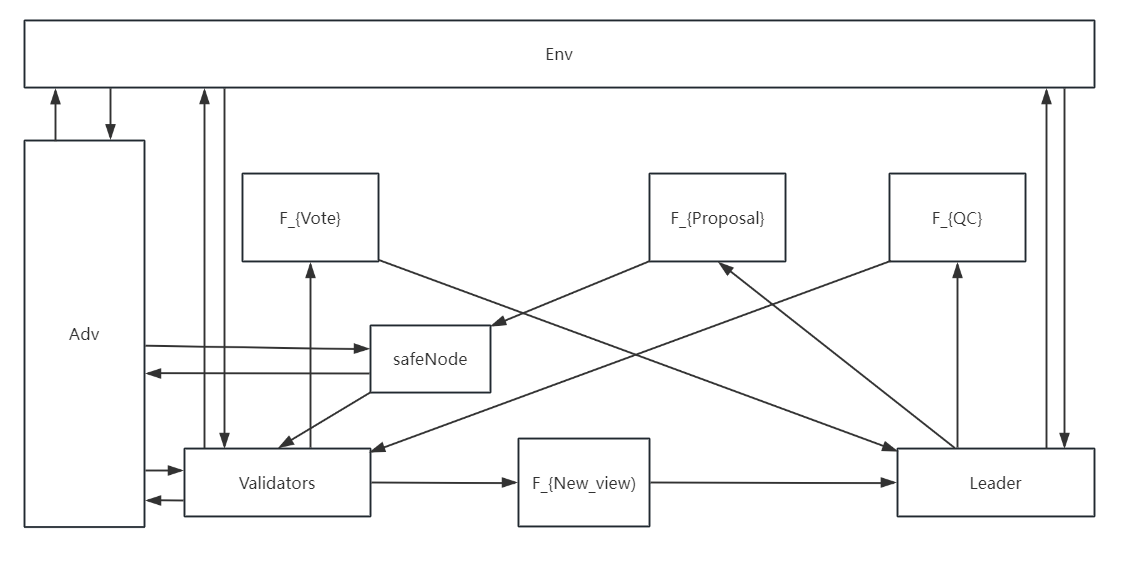
**Hotstuff建模进度**

**摘要：**

这篇文档是关于Hotstuff共识协议的建模进度报告。文档首先介绍了Hotstuff协议的整体框架，包括新视图（New-view）机制和区块共识过程中的关键概念，如领导者、验证者、拜占庭节点等。文档中尝试提出了两个定理：定理一阐述了在Hotstuff协议中，两个冲突的区块不能同时被不同的诚实节点提交；定理二说明了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。文档最后指出了目前建模遇到的问题，包括对建模细节的把握不足和对UC框架及Hotstuff协议的不熟悉，导致难以提出和证明引理，仍需要大量阅读相关文献来加深理解并完善建模工作。

**一、整体框架图：**



**New\_view:**The protocol for a new leader starts by collecting new-view messages from (n − f) replicas.The new-view message is sent by a replica as it transitions into viewNumber (including the first view) and carries the highest prepareQC.

**QC(quorum certificate)：**A key ingredient in the protocol is a collection of (n − f) votes over a leader proposal, referred to as a quorum certificate (or “QC” in short). The QC is associated with a particular node and a view number. The tcombine utility employs a threshold signature scheme to generate a representation of (n − f) signed votes as a single authenticator.

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（Voter）：** 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。

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。