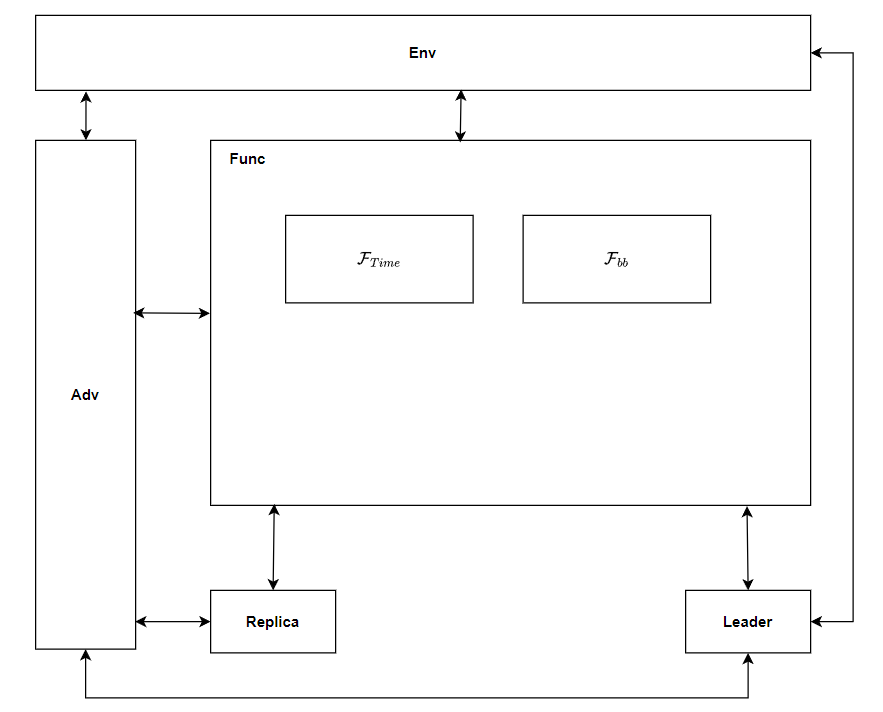
**Hotstuff建模进度**

**摘要：**

这篇文档是关于Hotstuff共识协议的v4建模进度报告。提出了全新的理想功能Fhotstuff

1. **整体框架图：**



1. **功能描述**

### F\_{TIME}

初始化：设置，。

–当从任意replica 接收到请求时，将更新为 ← ，向replica 返回一个消息, 然后开始倒计时。

–当从某一个时，它会向对应的replica 发送一个消息。

1. **F\_{Next\_view}**

初始化：设置，。

–当从任意replica m收到 next\_view请求MSG(⊥，m,prepareQC)时，将更新为，将prepareQC更新为。

–将、封装在NEW-VIEW message中发送给下一视图的leader。

1. **协议描述**

–Party Environment:

调用更新轮次，根据轮次取模GETLEADER()=curView%n选取某个副本作为本轮的leader。

–Party Leader:

**New\_view**：新领导者从功能收集来自(n - f)个副本的"new-view"消息。这些消息包含每个副本在上一轮的（prepareQC）。

**Proposal**: 领导者调用从这些New\_view消息中选择具有最高视图编号prepareQC，（如果没有的话，为⊥)并基于此创建一个新的提案（Proposal）

**Broadcast MSG**: 领导者向所有副本广播这个提案，并附带其选择的最高prepareQC作为安全证明。

**QC**:领导者调用，对来自replica的部分签名进行组合生成QC。并且将其广播给replica。

–Party Replica:

**safeNode**: 在收到来自Leader的提议消息m后，它首先调用功能检查提案消息m，m携带QC的正确性参数（justification）m.justify，检查后确定m.node是否可以安全接受。

**Prepare**: 根据收到的Proposal消息m，调用，将投票发送给leader。

**Pre-commit**: 根据收到的PrepareQC，更新自身PrepareQC，调用。将投票发送给leader。

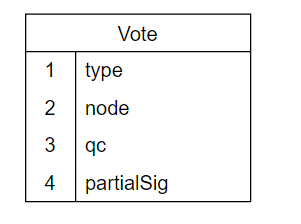
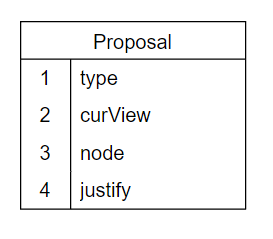
**Commit**: 根据收到的Pre-commitQC，更新lockedQC，调用。将投票发送给leader。

**Next\_view**:

在所有阶段中，副本在视图viewNumber处等待消息的超时时间，超时时间由辅助的确定。如果nextView（viewNumber）中断等待，副本调用,增加viewNumber并开始下一个视图。

**RoundOK**: 副本将等待轮次更新，开始新的轮次。

相关数据结构：



1. **理想功能**

# **Functionality**

**Network Delay Attack**

**Parameters**:

* R: Replica Set
* : the Maximum timeout duration of Replica .
* : Ideal functionality for timing.
* : Ideal functionality for broadcast.

**Symbol Explanation:**

### **Upon receiving message** from :

1. Send to and wait for a response of the form .
2. If :
   * Return to step 1.
3. Otherwise:
   * Elect from .

### **Upon receiving message** from :

1. Send to and wait for a response of the form .
2. If
   * Send to
3. Otherwise:
   * Send to .
   * If ,Send to and wait for a response of the form .
   * If no is received from ,Broadcast .
   * else,send to .

### **Upon receiving message** from:

1. Send to and wait for a response of the form .
2. If :
   * Send to
3. Otherwise:
   * Send to .
   * If and no has been received from :
     + Send to .
   * else,send to .

### **Upon receiving message** from :

1. Send to and wait for a response of the form .
2. If :
   * Send to
3. Otherwise:
   * Send to .
   * If and no has been received from :
     + Broadcast .
   * else,send to .

### **Upon receiving message** from :

1. Send to and wait for a response of the form .
2. If :
   * Send to
3. Otherwise:
   * Send to .
   * If no has been received from :
     + If :
       - Update ,then send to Leader
     + If :
       - Update ,then send to Leader
     + If :
       - execute the client's command
   * else,send to .