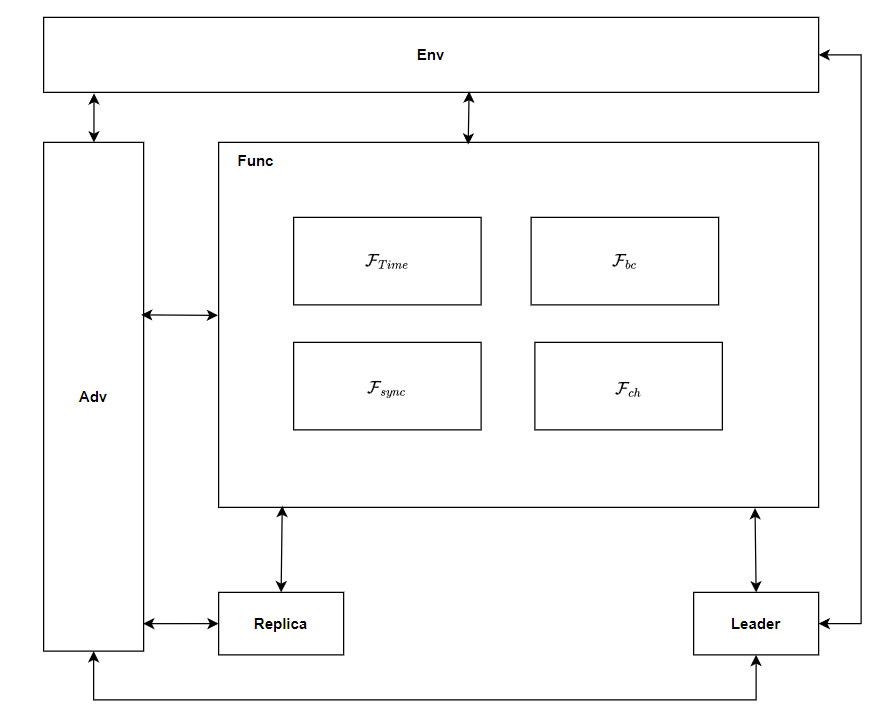
**Hotstuff建模进度**

**摘要：**

这篇文档是关于Hotstuff共识协议的v7建模进度报告：1、对框架图进行了修改，引入了新的广播功能F\_bc保证通信安全2、对协议π\_hotstuff进行更为细致的描述3、协议实现的UC建模完成度比例大概为80%

1. **整体框架图：**



1. **功能描述**

### F\_{Proposal}

初始化：设置。

–当收到消息时，

* 选取这些消息中最高的prepareQC最为highQC：
* 在highQC的节点的叶子上写入客户指令，提出新的提案B：

-将提案B、highQC封装在MSG中广播给replica：

### F\_{Vote} 初始化：设置。

–当收到来自的消息时，

* 先检查m是否与自己状态匹配：
* 检查叶子节点是否是本地lockedQC对应节点后继以及QC是否比本地lockedQC对应节点的视图更高：
* 在highQC的节点的叶子上写入客户指令，提出新的提案B：

-将投票信息结点m、自己的部分签名封装在VOTEMSG中发送给leader。

-当收到来自的消息时，

* 先检查QC是否与自己状态匹配：
* 如果决定投票且type是PREPARE阶段，更新本地状态：
* 如果决定投票且type是PRE-COMMIT阶段，更新本地状态：

-将投票信息m.justify.node、自己的部分签名封装在VOTEMSG中发送给leader：

### F\_{QC}

初始化：设置。

-当收到2f+1条投票消息时：

* 先检查m是否与自己状态匹配：
* 收集replica的投票，把部分签名组合：

-将QC封装在MSG中广播给replica：

### 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. **F\_{Ch}**

我们定义一组参与方，其中 和 表示该集合中的两个参与方，分别是消息 的发送方和接收方。

是基于功能的参数进行定义的。消息标识符 由功能新选定。

在接收到来自 的输入 时，输出 给 。

在接收到来自 的 后，向发送 。

根据以下参数化函数设置 ：

– 对于 设置 , 。在接收到来自 的 后，向 发送 。

– 对于 设置 。

– 对于 设置 。

– 对于 设置 。

– 对于 设置 。在接收到来自 的 后，向 发送 。

– 对于 设置 。

在接收到来自 的 后，向 发送 。

在接收到来自 的 后，向 发送 。

在接收到来自 的 后，输出 给 。

在接收到来自 的 后，向 发送 。

1. **F\_{bc}**

广播功能 由集合 参数化，具体流程如下：

在接收到来自某方 的 后，向集合 中的所有实体以及 发送 。

1. **理想功能**

# **Functionality**

**Network Delay Attack**

**Parameters**:

* : Replica Set
* ：the Maximum timeout duration
* : the Maximum timeout duration of Replica within current view.
* : Ideal functionality for timing.
* : Ideal functionality for broadcast.
* : Ideal functionality for synchronization.

**Symbol Explanation:**

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

1. .
2. If is corrupted:

* Send to .

1. Send to wait for a response of the form :
   * Set which .

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

1. Send to and wait for a response of the form :
   * If :
     + set
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
   * else,Send to .
2. If :
   * Set .
   * If ,Send to and wait for a response of the form :
     + Create.
     + If no is received from :
       - send to .
       - Set .
     + Else:
       - set .
       - send to and .
       - Send to .
       - Send to ,receive its response .
         * If ,set .
         * else re-execute this step.
3. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
   * else,Send to .
2. If :
   * If the is higher than , update
   * If and no has been received from :
     + Send to .
     + Send to and wait for a response of the form :
       - Set .
   * else:
     + set .
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
3. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
   * else,Send to .
     + If :
     + Set
     + If :
     + Create.
     + If no is received from :
       - send to .
       - Send to and wait for a response of the form :
         * Set .
     + Else:
       - set .
       - send to and .
       - Send to .
       - Send to ,receive its response .
         * If ,set .
         * else re-execute this step.
2. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set .
     + send to and .
   * else,Send to .
2. If :
   * If no has been received from :
     + Set .
     + Send to .
     + Send to and wait for a response of the form :
       - Set .
   * else:
     + set .
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
3. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
   * else,Send to .
     + If :
     + Set
     + If :
     + Create.
     + If no is received from :
       - send to .
       - Send to and wait for a response of the form :
         * Set .
     + Else:
       - set .
       - send to and .
       - Send to .
       - Send to ,receive its response .
         * If ,set .
         * else re-execute this step.
2. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set .
     + send to and .
   * else,Send to .
2. If :
   * If no has been received from :
     + Set .
     + Send to .
     + Send to and wait for a response of the form :
       - Set .
   * else:
     + set .
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
3. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
   * else,Send to .
     + If :
     + Set
     + If :
     + Create.
     + If no is received from :
       - send to .
       - send to and .
       - Send to .
       - Send to ,receive its response .
         * If ,set .
         * else re-execute this step.
     + Else:
       - set .
       - send to and .
       - Send to .
       - Send to ,receive its response .
         * If ,set . set .
         * else re-execute this step.
2. Else，ignore this message.

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

1. Send to and wait for a response of the form :
   * If :
     + set .
     + send to and .
   * else,Send to .
2. If :
   * If no has been received from :
     + Execute new commands through
     + Send to .
     + Send to ,receive its response .
       - If ,set ,set .
       - else re-execute this step.
   * else:
     + set .
     + send to and .
     + Send to .
     + Send to ,receive its response .
       - If ,set .
       - else re-execute this step.
3. Else，ignore this message.

1. **协议描述**

# **The protocol**

|  | Leader |  | Replica |  |
| --- | --- | --- | --- | --- |
|  | 1: Send to |  |  |  |
|  | 2: Send to ,receive |  |  |  |
|  | 3: Send to |  |  |  |
|  | 4: If a message is received from ,Send to |  |  |  |
|  | 5: Else,broadcast to Replicas |  |  |  |
|  | 6: Send to |  |  |  |
|  |  |  | 7: Send to |  |
|  |  |  | :If a message is received from ,Send to |  |
|  |  |  | 8: Else,if ,call |  |
|  | 9: Send to |  |  |  |
|  | 10: Call |  |  |  |
|  |  |  | 11: Send to |  |
|  |  |  | 12: Set |  |
|  |  |  | 13: Call |  |
|  | 14: Send to |  |  |  |
|  | 15: Call |  |  |  |
|  |  |  | 16:Send to |  |
|  |  |  | 17: Set |  |
|  |  |  | 18: Call |  |
|  | 19: Send to |  |  |  |
|  | 20: Call |  |  |  |
|  | 21: Send to |  |  |  |
|  |  |  | 22: Send to |  |
|  |  |  | 23: If a message is received from ,Send to |  |
|  |  |  | 24: Else,execute new commands through |  |
|  |  |  | 25: Send to |  |
|  |  |  |  |  |

### **The Functionality**

| REPLICA |  |  |
| --- | --- | --- |
|  |  | Initialize: |
| 1: Send to |  |  |
|  |  | 2: set ,return |
|  |  | 3: When |
|  |  | 4: Send |

## **The Functionality**

|  | Replica |  |  |
| --- | --- | --- | --- |
| Prepare | 1: Send to |  |  |
|  |  |  | 2 : Send to |
|  |  |  | 3 : If no is received from : send to Leader |
|  |  |  |  |
| Precommit | 1: Send to |  |  |
|  |  |  | 2 : Send to |
|  |  |  | 3 : If no is received from : send to Leader |
| Commit | 1: Send to |  |  |
|  |  |  | 2 : Send to |
|  |  |  | 3 : If no is received from : send to Leader |

### **The Functionality**

|  | Leader |  |  |
| --- | --- | --- | --- |
| **PreCommit** | 1: Send to |  |  |
|  |  |  | 2: Send to |
|  |  |  | 3: If no is received from and more than prepare votes are received: broadcast |
| **Commit** | 1: Send to |  |  |
|  |  |  | 2: Send to |
|  |  |  | 3: If no is received from and more than precommit votes are received: broadcast |
| **Decide** | 1: Send to |  |  |
|  |  |  | 2: Send to |
|  |  |  | 3: If no is received from and more than commit votes are received: broadcast |

### **The Functionality**

| Leader/REPLICA |  |  |
| --- | --- | --- |
| 1: Send to |  |  |
|  |  | 2: Return n-f NEW-VIEW messages which |
| 1. Send to |  |  |
|  |  | 2: Set ,return |

相关数据结构：

