**2022年研究计划**

目录

[1. 基于节点稳定度的区块链共识算法 3](#_Toc94478623)

[1.1 模型假设 3](#_Toc94478624)

[（一）区块链模型 3](#_Toc94478625)

[（二）区块生成过程 4](#_Toc94478626)

[（三）其它 4](#_Toc94478627)

[1.2 研究问题 4](#_Toc94478628)

[1.3 研究方案 5](#_Toc94478629)

[（一）定义稳定度 5](#_Toc94478630)

[（二）共识算法 5](#_Toc94478631)

[（三）奖惩机制 6](#_Toc94478632)

[1.4 仿真实验 7](#_Toc94478633)

[（一）实验目标 7](#_Toc94478634)

[（二）实验方案 7](#_Toc94478635)

[（三）技术难点 7](#_Toc94478636)

[2. 稳定的委员会区块链共识算法 7](#_Toc94478637)

[2.1 模型假设 7](#_Toc94478638)

[（一）区块链模型 8](#_Toc94478639)

[（二）区块生成过程 8](#_Toc94478640)

[（三）其它 9](#_Toc94478641)

[2.2 研究问题 9](#_Toc94478642)

[2.2 研究方案 9](#_Toc94478643)

[（一）定义稳定度 9](#_Toc94478644)

[（二）共识算法 10](#_Toc94478645)

[（三）奖惩机制 11](#_Toc94478646)

[2.4 仿真实验 12](#_Toc94478647)

[（一）实验目标 12](#_Toc94478648)

[（二）实验方案 12](#_Toc94478649)

[（三）技术难点 12](#_Toc94478650)

[3. 稳定的分片区块链共识算法 12](#_Toc94478651)

[3.1 模型假设 12](#_Toc94478652)

[（一）区块链模型 13](#_Toc94478653)

[（二）区块生成过程 13](#_Toc94478654)

[（三）其它 14](#_Toc94478655)

[3.2 研究问题 14](#_Toc94478656)

[3.3 研究方案 15](#_Toc94478657)

[（一）定义稳定度 15](#_Toc94478658)

[（二）共识算法 15](#_Toc94478659)

[（三）奖惩机制 17](#_Toc94478660)

[3.4 仿真实验 17](#_Toc94478661)

[（一）实验目标 17](#_Toc94478662)

[（二）实验方案 18](#_Toc94478663)

[（三）技术难点 18](#_Toc94478664)

[4. 基于节点稳定度的DAG区块链共识算法 18](#_Toc94478665)

[4.1 模型假设 18](#_Toc94478666)

[（一）区块链模型 18](#_Toc94478667)

[（二）区块生成过程 19](#_Toc94478668)

[（三）其它 19](#_Toc94478669)

[4.2 研究问题 19](#_Toc94478670)

[4.3 研究方案 20](#_Toc94478671)

[（一）定义稳定度 20](#_Toc94478672)

[（二）共识算法 20](#_Toc94478673)

[（三）奖惩机制 22](#_Toc94478674)

[4.4 仿真实验 23](#_Toc94478675)

[（一）实验目标 23](#_Toc94478676)

[（二）实验方案 23](#_Toc94478677)

[（三）技术难点 23](#_Toc94478678)

[5. 接下来主要的工作 23](#_Toc94478679)

[5.1 节点自启机制 23](#_Toc94478680)

[5.2 基于稳定度的节点选举 24](#_Toc94478681)

[5.3 门限签名机制的原理 25](#_Toc94478682)

[5.4 可验证随机函数的原理 28](#_Toc94478683)

在2022年准备完成四篇关于区块链共识算法的小论文，具体内容如下。

# 基于节点稳定度的区块链共识算法

## 模型假设

【简单描述：（一）区块链模型，包括节点之间的网络结构和特征、区块结构、存储结构等，例如，节点通信模型（节点拓扑或路由结构、信噪比模型等）、区块链存储模型（链式、DAG、…）等；（二）区块生成过程，包括交易打包、区块生成（包括共识）、区块上链等过程；（三）其它，包括其它与本论文紧密相关的部分。注意：重点剖析与本论文紧密相关的部分。】

### （一）区块链模型

在无线自组织网络环境中，链式存储的区块链。

1. 网络模型：考虑一个无线自组织网络，个节点随意部署在一个二维平面中。记为两个节点之间的欧氏距离， 为以节点为中心，通信半径为的圆盘。每个节点都拥有唯一的ID。假设节点可以在网络区域中随意移动，并且节点可以随意进入和离开这个区域。
2. 区块结构：每个节点局部地维护一个区块链。各区块通过引用前一个区块的哈希最终形成一条链的形式。每个区块中包含多个交易、自身区块的哈希、前一个区块的哈希、时间戳、区块的组合签名、区块的高度等信息。假设节点可以被公钥基础设施支持，并且系统中采用的密码学原语是安全的，因此没有恶意实体可以伪造消息。
3. 干扰和SINR模型：采用信号干扰模型能够很好的捕获无线网络的干扰。标准信号干扰的信噪比模型为

其中是节点接收到的节点的信号的功率，是平均信号发射功率，在节点处的干扰为

其中是在当前传输节点的集合，为环境噪声，路径损耗指数为，阈值取决于节点的硬件。假设节点可以进行物理载波监听。

### （二）区块生成过程

1. 交易的提交和广播：每个节点产生新交易之后，广播交易到网络。其他节点接收到新的交易之后，需要验证交易的合法性，验证成功后放入本地交易池。
2. 区块的生成：根据节点的稳定度来确定节点被选中成为出块节点的概率，采用随机抽签的方式确定抽中的节点。当节点发现自己获得出块权限之后，会从交易池中取出交易打包成区块，并分发密钥份额给该区块的签名者，广播区块到网络。
3. 区块确认和上链：接收到区块的节点验证区块和签名的合法性，如果拥有该区块的密钥份额，则会对该区块签名，并广播签名结果。当签名份额达到某一阈值之后，会对该区块形成一个最终签名，此时区块被确认并添加到各节点的本地链上。

### （三）其它

## 研究问题

【从技术层面描述：各个问题产生的背景和原因，针对每个问题分别给出若干个可能可行的方案。重点描述“研究问题”产生的原因和进行研究的必要性，对问题分析得越清晰、透彻，越有利于后面的研究；对方案只需进行简单描述，在下一节中再详细描述研究方案。】

在无线多跳网络环境中，单首领的共识算法无法确保所有的节点同时维护相同的区块链。首领节点的选择也面临着比较大的资源消耗，对代币依赖、高带宽要求等问题。这些区块链共识算法并不适用于设备资源有限、节点具有高动态性和节点随时离开网络的无线多跳网络环境中，因此需要适用于无线多跳网络环境的区块链共识算法。

1. 资源消耗：原因？【首领节点选取时需做工作量证明的计算，因此消耗大量算力】方案？【用一种替代工作量证明的、对算力要求相对较低的首领选择方式；降低节点的挖矿难度减少工作量证明的消耗；】
2. 节点动态性：原因？【节点的网络拓扑变化大且不可预测，因此节点可能会突然离开系统影响共识过程】方案？【将节点的稳定度作为首领选举的依据，确保选举的首领节点稳定性高，短期内不会离开系统；将节点到其他节点的跳数或者节点的位置作为首领选举的依据，确保首领节点能够尽快将结果发送给其他节点，快速地达成共识；】

## 1.3 研究方案

【详细描述“研究问题”中各方案的关键技术方案或算法，包括：方案或算法的细节、重点和难点、该技术方案解决“研究问题”中的哪个问题等。】

### （一）定义稳定度

区块链系统中，新节点加入后要质押金钱获得在系统中活动的时间。活动的时长与交付的押金成正比。

记为节点在区块链系统中的剩余活跃时间，记为节点在最近个确认区块中参与共识比值，定义节点的稳定度为

其中，权重系数可根据偏好设置。在区块链系统运行初期，确认区块数量不足个时记节点的共识比为零，此时节点的稳定度主要受节点的活动时间的影响。

重点：计算节点的剩余活动时间、节点的共识比和这两个度量的权重系数。

难点：计算影响节点稳定度的度量的权重系数，测量节点的共识比，计算其他节点的稳定度，验证首领节点的合法性。

解决的问题：解决工作量证明选取首领节点消耗巨大算力，解决首领节点突然离开系统导致最终无法达成共识的问题，防止女巫攻击。

### （二）共识算法

区块链系统需要共识算法确保所有节点维护相同的区块链。共识算法主要分为两部分：首领节点的选举和区块确认。我们将根据节点的稳定度随机选举首领节点。稳定度高的节点具有更大的概率被选中，稳定度低的节点被选中的概率将更小。区块的确认则是采用签名方式，让区块被大部分节点都认可后就被确认。

1. 随机选举首领节点：我们采用随机抽签的方式选举首领节点需要满足几点：一是选择的概率与节点的稳定度相关且必须是随机的，二是随机选择是唯一的，三是随机计算的结果必须可以被其他节点验证。首领选举采用随机抽签算法，将上一个区块的高度和最终签名的哈希作为随机种子输入随机可验证函数中得到抽签结果和证明，其他节点可以根据证明验证该节点的合法性。
2. 随机抽签算法

随机抽签算法根据节点的稳定度决定节点被选中的概率。记是节点的稳定度，所有节点的稳定度之和为，那么节点被选中的概率为且有。为了确定被选中的节点，将区间分为连续的多个区间

.

随机可验证函数将区块的高度和最终签名作为输入计算得到一个值和证明

若落在某个节点所属的区间之内，则该节点被选举为首领。

1. 验证随机抽签结果

根据随机抽签算法输出的随机选举值和证明，其他节点也可以验证首领选举结果的合法性。

VerifyVRF(*pk*, *value*, *proof*, )

如果验证结果为，则首领节点的验证成功，该首领是合法的；如果结果为，则首领节点的合法性将不被承认。

1. 区块密钥份额：节点得知自己成为首领后，会生成密钥并且将密钥份额分发到系统中。随后，首领节点生成区块并广播到网络收集其他节点对区块的签名份额。
2. 区块确认：其他节点接收区块后会验证区块和出块节点的合法性。在得到最终签名之前，需要验证每个签名份额，并且有效签名份额的数量不能小于门限值。一旦区块上签名数量达到阈值，则该区块被确认可以被添加到本地区块链上。

重点：采用随机抽签算法选举首领，采用门限签名算法确认区块。

难点：根据节点的稳定度快速计算所有节点被选中概率，门限签名中密钥份额的计算和分发，区块签名份额的收集和最终组合。

解决的问题：解决节点公平性问题，确保每个节点都可能被选中成为首领获得奖励。解决无利害关系攻击问题，门限签名机制确保节点无法在多个分支上同时挖矿。解决长程攻击问题，门限签名机制确保节点无法篡改早期已经被确认的区块。

### （三）奖惩机制

1. 奖励机制：当区块被确认后，生成区块的节点将获得部分区块奖励和交易费用，剩余部分的奖励将分发给后一个区块的生成者。这样的奖励机制可以使得诚实节点更愿意在新区块后面挖矿，减小分叉的概率提高安全性。同时也能激励系统中的节点积极维护系统区块链，提升系统的活性。
2. 惩罚机制：如果节点在未到活动时间结束之前离开系统，则会扣除部分押金。当发现有节点作恶后系统也会扣除押金。

重点：采用奖励机制提高节点的活性和系统的安全性，使用惩罚机制降低节点作恶的动机。

难点：计算奖励分配比例确保节点私自挖矿成功的概率非常低。

解决的问题：解决节点缺乏活性问题，奖励机制可以激励节点积极地参与共识维护区块链。解决节点长期离线的问题，节点如果长期离线就会蒙受经济损失。

## 1.4 仿真实验

【描述：（一）实验目标，（二）实验方案（详细的实验方案，包括实验环境、实验步骤等），（三）技术难点（目前的技术难点、还需要补充的知识等）。】

### （一）实验目标

通过仿真实验测试分析采用基于稳定度的共识算法的区块系统的性能。衡量性能的两个主要参数指标是交易吞吐量和区块确认延时。

1. 交易吞吐量：单位时间内处理交易的数量；
2. 区块确认延时：区块确认的平均时延。

在仿真实验中需要测试不同区块大小、节点数量、节点密度的情况下区块链系统的交易吞吐量和区块确认延时。

考虑网络带宽，网络通信协议、单位时隙大小、编程语言、运行设备、测试次数等。

影响因素包括：区块大小、网络大小、节点密度等。

### （二）实验方案

【如何来完成实验？在自己设计的区块链中采集数据进行分析？在公链上进行实验？实验步骤是什么？】

由于需要在无线自组织网络中测试区块链系统的性能，因此需要自己设计一个区块链进行数据采集和分析。实验步骤如下：

1. 搭建无线自组织网络：每个节点都以相同的移动速率在一个区域中随机运动，且在区域中的活动时间是有限的。对于节点之间的通信采用CSMA/CA作为通信协议。
2. 记录节点的活动时间：为每个节点赋予不同的活动时间，当活动时间结束则该节点离开网络。记录节点进入网络的时间。
3. 生成交易：构造一批不同的交易，确保他们的哈希不同。发送交易到网络中，并记录开始发送交易的时间
4. 生成区块：从参与共识的节点中选举首领节点，随后生成区块并发送到网络中，记录区块发送时间。
5. 确认区块：查看节点的日志中区块确认的时间并记录。同时还需要计算区块中交易的数量。
6. 计算区块确认延时：计算区块生成时间和确认时间可以得出区块的确认延时。
7. 计算交易吞吐量：计算一个区块中处理交易的数量，除以区块的确认时延，可以得到平均交易吞吐量。

### （三）技术难点

【根据设计的实验方案，目前的技术难点或需要学习的知识有哪些？】

技术难点：无线自组织网络的搭建和参数设置，计算稳定度依据的权重系数，获取其他节点的稳定度。节点活动起止时间记录，区块发送和确认时间记录，区块中交易数量计数。

待学习的知识：虚拟机配置、Socket技术、C++编程语言学习

# 稳定的委员会区块链共识算法

## 模型假设

【简单描述：（一）区块链模型，包括节点之间的网络结构和特征、区块结构、存储结构等，例如，节点通信模型（节点拓扑或路由结构、信噪比模型等）、区块链存储模型（链式、DAG、…）等；（二）区块生成过程，包括交易打包、区块生成（包括共识）、区块上链等过程；（三）其它，包括其它与本论文紧密相关的部分。注意：重点剖析与本论文紧密相关的部分。】

### （一）区块链模型

1. 网络模型：考虑随意部署在一个二维平面中的个节点构造的无线自组织网络。记为两个节点之间的欧氏距离， 为以节点为中心，通信半径为的圆盘。每个节点都拥有唯一的ID。假设节点可以在网络区域中随意移动，并且节点可以随意进入和离开这个区域。
2. 区块结构：每个节点局部地维护一个区块链。各区块通过引用前一个区块的哈希最终形成一条链的形式。每个区块中包含多个交易、自身区块的哈希、前一个区块的哈希、时间戳、区块的组合签名、区块的高度等信息。假设公钥基础设施支持每个节点，并且系统中采用的密码学原语是安全的，因此没有恶意实体可以伪造消息。
3. 干扰和SINR模型：采用信号干扰模型能够很好的捕获无线网络的干扰。标准信号干扰的信噪比模型为

其中是节点接收到的节点的信号的功率，是平均信号发射功率，在节点处的干扰为

其中是在当前传输节点的集合，为环境噪声，路径损耗指数为，阈值取决于节点的硬件。假设节点可以进行物理载波监听。

### （二）区块生成过程

1. 交易的提交和广播：每个节点发现新交易广播到网络。节点接收到新的交易后验证交易的合法性，验证成功后放入在本地交易未处理交易池中。
2. 委员会选举：根据节点的稳定度来确定节点被选中成为委员会成员的概率，采用随机抽签的方式选举委员会。采用基于平均跳数或者基于节点位置的方式从委员会成员中选举每一轮的首领节点。首领节点会生成和分发密钥份额给委员会成员。
3. 区块生成：首领节点从交易池中取出交易打包成区块作为提案广播给其他委员会成员。
4. 区块确认和上链：接收到区块的节点会验证区块、首领和其他签名份额的合法性。如果区块当前的签名份额未达到组合签名的阈值，则接收区块的节点会对区块签名并广播签名结果到网络。当签名份额达到阈值之后，会组合成区块的最终签名，此时区块被确认并添加到各节点的本地链上。

### （三）其它

## 2.2 研究问题

【从技术层面描述：各个问题产生的背景和原因，针对每个问题分别给出若干个可能可行的方案。重点描述“研究问题”产生的原因和进行研究的必要性，对问题分析得越清晰、透彻，越有利于后面的研究；对方案只需进行简单描述，在下一节中再详细描述研究方案。】

在规模较大的无线自组织网络中，单首领节点共识算法达成共识过程缓慢，且只具有弱一致性。为了提高共识效率降低区块链出现分叉的可能性，需要设计一个适用于大规模无线自组织网络的委员会共识算法。

1. 共识时延长：原因？【首领节点广播区域有限，需要多跳才能将区块传输到较远的节点，因此网络规模较大时网络传输区块所需的时间较长】方案？【多个节点达成共识之后同时传输区块到网络，降低网络广播区块到全网的时延；将节点到其他节点的跳数作为选择首领节点的一个依据，尽可能确保从该节点到其他节点的平均跳数较低低，可以有效的降低系统达成共识的时延；】
2. 算法弱一致性：原因？【网络传输存在延迟，节点传输区块到全网需要一段不确定时间，且每个节点确认该区块的时间也是不一致的。】方案？【选举出一个委员会，在委员会内对于区块达成一致确保区块共识的强一致性；】

## 研究方案

【详细描述“研究问题”中各方案的关键技术方案或算法，包括：方案或算法的细节、重点和难点、该技术方案解决“研究问题”中的哪个问题等。】

### （一）定义稳定度

区块链系统中，新节点加入后要质押金钱获得在系统中活动的时间。活动的时长与交付的押金成正比。

记为节点在区块链系统中的剩余活跃时间，记为节点在最近个确认区块中参与共识比值，定义节点的稳定度为

其中，权重系数可根据偏好设置。在区块链系统运行初期，确认区块数量不足个时记节点的共识比为零，此时节点的稳定度主要受节点的活动时间的影响。

重点：计算节点的剩余活动时间、节点的共识比和这两个度量的权重系数。

难点：计算影响节点稳定度的度量的权重系数，测量节点的共识比，计算其他节点的稳定度，验证首领节点的合法性。

解决的问题：解决工作量证明选取首领节点消耗巨大算力，解决首领节点突然离开系统导致，押金机制也可以防止敌手发起女巫攻击。

### （二）共识算法

区块链系统需要共识算法确保所有节点维护相同的区块链。共识算法主要分为两部分：委员会成员和首领节点的选举、一致性协议和委员会重置。我们将根据节点的稳定度随机选举委员会成员和首领节点。稳定度高的节点具有更大的概率被选中，稳定度低的节点被选中的概率将更小。一致性协议则是采用门限签名方式，让委员会成员不需要二次通信就能对区块达成一致。

1. 随机选举委员会成员：我们采用随机抽签算法选举委员会节点，将上一个区块的高度和最终签名的哈希作为随机种子输入随机可验证函数中得到抽签结果和证明，其他节点可以根据证明验证该节点的合法性。
2. 随机抽签算法

随机抽签算法根据节点的稳定度决定节点被选中的概率。记是节点的稳定度，所有节点的稳定度之和为，那么节点被选中的概率为且有。为了确定被选中的节点，将区间分为连续的多个区间

.

随机可验证函数将区块的高度和最终签名作为输入计算得到一个值和证明

满足的前个节点被选举为委员会成员。

1. 验证随机抽签结果

根据随机抽签算法输出的随机选举值和证明，其他节点也可以验证首领选举结果的合法性。

VerifyVRF(*pk*, *value*, *proof*, )

如果验证结果为，则首领节点的验证成功，该首领是合法的；如果结果为，则首领节点的合法性将不被承认。

1. 首领节点选举：每个委员会将有一个任期，每个任期又分为多个轮。每轮需要选举首领节点生成区块在委员会内部达成一致。为了降低共识时延，可以选择委员会中相互之间通信少的节点作为首领，降低网络资源消耗的同时提高共识的效率。

【方案一】通过路由算法委员会成员可以得知到其他成员节点的跳数，最终选择平均跳数最少的节点作为首领。记委员会成员数量为，则委员会节点到其他节点跳数的矩阵记为

其中表示节点到节点 之间的路由跳数，当时，表示节点到其自身的跳数为零。

【方案二】在无线网络通信中，节点的欧式距离会反映节点之间的通信情况。因此可以根据节点的位置和通信半径，采用最大独立子集的方式构建节点之间的通信骨架，最终选择出比较中心的节点作为首领。

1. 一致性协议：确定委员会成员和首领之后，首领节点会生成和分发密钥份额给委员会其他成员。首领节点生成新的区块广播给委员会成员。委员会成员会验证区块、首领节点的合法性。委员会成员需要验证区块当前签名份额的有效性，并且有效签名份额的数量不能小于门限值。当签名数量达到阈值后会组成区块的最终签名，区块会被确认达成一致。委员会成员将区块链接到区块链并广播给其他非委员会成员。接收到确认区块的节点验证区块合法性成功后将区块连接到本地链上。
2. 委员会重置：委员会任期结束之后，需要更换委员会成员。根据委员会的容错率来决定更换委员会成员的数量。为了更好的确保系统的安全性，委员会成员每次最多只更换稳定度最低的⌋个节点。

重点：利用随机抽签算法选举委员会成员，基于跳数或者位置的方式选举首领节点。采用基于门限签名的一致性协议在委员会内对区块达成一致。

难点：快速计算每个节点的稳定度和被选中概率，快速选举委员会成员和首领。获取其他节点的跳数信息和位置信息。计算门限签名中密钥份额的计算和分发，区块签名份额的收集和最终组合。

解决的问题：解决节点公平性问题，确保每个节点都可能被选中成为委员会成员获得奖励。委员会机制确保所有的节点都维护相同的区块链，解决区块链分叉问题。

### （三）奖惩机制

1. 奖励机制：委员会任期结束，委员会内所有节点将平分任期内所有生成区块的奖励和交易费用。这样的奖励机制能激励系统中的节点积极维护系统区块链，提升系统的活性。
2. 惩罚机制：如果节点在未到活动时间结束之前离开系统，则会扣除部分押金。当发现有节点作恶后系统也会扣除押金。这个机制会降低节点离线和作恶的机会。

重点：采用奖励机制提高节点的活性和系统的安全性，使用惩罚机制降低节点作恶的动机。

难点：交易费用的计算，快速分配奖励给委员会成员。

解决的问题：解决节点缺乏活性问题，奖励机制可以激励节点积极地参与共识维护区块链。节点如果长期离线就会蒙受经济损失，解决节点长期离线的问题。

## 2.4 仿真实验

【描述：（一）实验目标，（二）实验方案（详细的实验方案，包括实验环境、实验步骤等），（三）技术难点（目前的技术难点、还需要补充的知识等）。】

### （一）实验目标

通过仿真实验测试交易吞吐量和区块确认延时分析区块系统的性能。

1. 交易吞吐量：单位时间内处理交易的数量；
2. 区块确认延时：区块确认的平均时延。

在仿真实验中需要测试不同区块大小、节点数量、节点密度的情况下区块链系统的交易吞吐量和区块确认延时。

考虑网络带宽，网络通信协议、单位时隙大小、编程语言、运行设备、测试次数等。

影响因素包括：区块大小、网络大小、节点密度等。

### （二）实验方案

如何来完成实验？在自己设计的区块链中采集数据进行分析？在公链上进行实验？实验步骤是什么？

无线自组织网络中测试区块链系统的性能需要在自己设计一个区块链进行数据采集和分析。实验步骤如下：

1. 搭建无线自组织网络：每个节点都以相同的移动速率在网络区域中随机移动，且在区域中的活动时间是有限的。对于节点之间的通信采用CSMA/CA作为通信协议。
2. 记录节点的活动时间：为每个节点赋予不同的活动时间，当活动时间结束则该节点离开网络。记录节点进入网络的时间。
3. 生成交易：构造一批不同的交易，确保他们的哈希不同。发送交易到网络中，并记录开始发送交易的时间。
4. 选举委员会成员：记录委员会选举开始的时间,根据任期长度记录委员会结束的时间。
5. 生成区块：每一轮开始从委员会成员中选举首领节点，首领节点生成区块并广播到网络中，记录每轮开始时间和区块发送时间。
6. 确认区块：委员会对区块达成一致结果确认区块。记录委员会节点的日志中区块确认的时间、每轮轮结束的时间和区块中交易的数量。
7. 计算区块确认延时：计算区块生成时间和确认时间可以得出区块的确认延时。
8. 计算平均交易吞吐量：计算一个委员会任期中所有区块中处理交易的数量，除以任期时长，可以得到平均交易吞吐量。

### （三）技术难点

根据设计的实验方案，目前的技术难点或需要学习的知识有哪些？

技术难点：在无线自组织网络上搭建区块链系统，计算稳定度依据的权重系数，获取其他节点的稳定度。获取到其他委员会成员的跳数或者其他节点的位置。获取节点活动起止时间记录，区块发送和确认时间记录，区块中交易数量计数，更换委员会成员。

待学习的知识：虚拟机配置、Socket编程、C++编程语言学习

# 稳定的分片区块链共识算法

## 模型假设

【简单描述：（一）区块链模型，包括节点之间的网络结构和特征、区块结构、存储结构等，例如，节点通信模型（节点拓扑或路由结构、信噪比模型等）、区块链存储模型（链式、DAG、…）等；（二）区块生成过程，包括交易打包、区块生成（包括共识）、区块上链等过程；（三）其它，包括其它与本论文紧密相关的部分。注意：重点剖析与本论文紧密相关的部分。】

### （一）区块链模型

在无线自组织网络环境中，链式存储的区块链。

1. 网络模型：考虑一个无线自组织网络，个节点随意部署在一个二维平面中。记为两个节点之间的欧氏距离， 为以节点为中心，通信半径为的圆盘。每个节点都拥有唯一的ID。假设节点可以在网络区域中随意移动，并且节点可以随意进入和离开这个区域。
2. 区块结构：每个节点局部地维护一个区块链。各区块通过引用前一个区块的哈希最终形成一条链的形式。每个区块中包含多个交易、自身区块的哈希、前一个区块的哈希、时间戳、区块的组合签名、区块的高度等信息。假设节点可以被公钥基础设施支持，并且系统中采用的密码学原语是安全的，因此没有恶意实体可以伪造消息。
3. 干扰和SINR模型：采用信号干扰模型能够很好的捕获无线网络的干扰。标准信号干扰的信噪比模型为

其中是节点接收到的节点的信号的功率，是平均信号发射功率，在节点处的干扰为

其中是在当前传输节点的集合，为环境噪声，路径损耗指数为，阈值取决于节点的硬件。假设节点可以进行物理载波监听。

### （二）区块生成过程

1. 交易的提交和广播：节点发现新交易后广播到网络。节点接收到新的交易验证交易的合法性后放入在本地交易池中。
2. 分片委员会选举：根据节点的稳定度决定节点被选中的概率。采用随机抽签算法选举当前任期每个分片委员会，使用基于平均跳数或者基于节点位置的方式选择出每个分片委员会的首领节点。首领节点将作为根委员会的成员，采用与分片委员会相同的方式选举根委员会的首领。
3. 分片区块生成：每个分片首领会从交易池中取出交易打包成区块作为提案广播给分片委员会成员。每个分片委员会内执行基于门限签名的一致性协议对分片区块达成一致。随后分片首领将区块提交给根委员会。
4. 最终区块的确认和上链：根委员会首领节点收集并验证分片区块，最终形成一个总区块广播给根委员会成员。根委员会内部执行基于门限签名的一致性协议对总区块达成一致，总区块被确认添加到委员会的本地链上并广播总区块到各个分片中。分片中各节点对于接收到的区块放入自己的本地链上，实现全局一致性。

### （三）其它

## 3.2 研究问题

【从技术层面描述：各个问题产生的背景和原因，针对每个问题分别给出若干个可能可行的方案。重点描述“研究问题”产生的原因和进行研究的必要性，对问题分析得越清晰、透彻，越有利于后面的研究；对方案只需进行简单描述，在下一节中再详细描述研究方案。】

在无线多跳网络环境中，当节点数量增加会导致节点之间的通信增加。为了降低网络资源的消耗，提高交易处理效率，需要设计一个适用于无线多跳网络中的分片委员会共识算法。

1. 通信资源耗费巨大：原因？【共识节点之间的通信会随着节点数量增加而增加，导致达成共识所需的网络资源非常大】方案？【采用网络分片的方式减少共识节点之间的相互通信；基于位置/跳数的方式选择委员会中的成员，确保委员会中的成员能够覆盖尽可能大的区域，降低共识节点网络通信资源的消耗】
2. 交易处理效率低：原因？【区块的大小是有限的，因此单一委员会处理交易的效率比较低】方案？【将节点按照网络特性（比如位置）进行分片，并行处理交易提高效率；将节点的位置和跳数作为选择首领节点的依据，降低节点达成一致的网络时延，提高交易的处理效率；】
3. 跨分片交易死锁：原因？【跨分片通信延时高，由于分片内交易处理速度快导致跨分片交易处理过程出现死锁】方案【采用原子提交协议确保跨分片交易处理时相关交易不会再分片中被处理；采用分片融合的方式使得跨分片交易相关交易处于同一个分片中，避免出现跨分片交易死锁的问题；将一个跨分片交易拆分为多个交易，并在不同分片中处理，从而避免了跨分片通信的问题；】

## 3.3 研究方案

【详细描述“研究问题”中各方案的关键技术方案或算法，包括：方案或算法的细节、重点和难点、该技术方案解决“研究问题”中的哪个问题等。】

### （一）定义稳定度

区块链系统中，新节点加入后要质押金钱获得在系统中活动的时间。活动的时长与交付的押金成正比。

记为节点在区块链系统中的剩余活跃时间，记为节点在最近个确认区块中参与共识比值，定义节点的稳定度为

其中，权重系数可根据偏好设置。在区块链系统运行初期，确认区块数量不足个时记节点的共识比为零，此时节点的稳定度主要受节点的活动时间的影响。

重点：计算节点的剩余活动时间、节点的共识比和这两个度量的权重系数。

难点：计算影响节点稳定度的度量的权重系数，测量节点的共识比，计算其他节点的稳定度，验证首领节点的合法性。

解决的问题：解决工作量证明选取首领节点消耗巨大算力，解决首领节点突然离开系统导致，押金机制也可以一定程度上防止敌手发起女巫攻击。

### （二）共识算法

区块链系统需要共识算法确保所有节点维护相同的区块链。共识算法主要分为几部分：分片委员会、根委员会和首领节点的选举、一致性协议和委员会重置。我们将根据节点的稳定度和分片情况随机选举分片委员会成员、根委员会成员和首领节点。稳定度高的节点具有更大的概率被选中，稳定度低的节点被选中的概率将更小。一致性协议则是采用门限签名方式，让委员会成员不需要二次通信就能对区块达成一致。

1. 随机选举分片委员会成员：我们采用随机抽签算法分别选举每个分片委员会，将上一个区块的高度和最终签名的哈希作为随机种子，计算随机可验证函数得到抽签结果和证明，其他节点可以根据证明验证结果的有效性。
2. 随机抽签算法

随机抽签算法根据节点的稳定度决定节点被选中的概率。记是节点的稳定度，所有节点的稳定度之和为，那么节点被选中的概率为且有。为了确定被选中的节点，将区间分为连续的多个区间

.

随机可验证函数将区块的高度、最终签名以及分片序号作为输入计算得到一个值和证明

满足的前个节点被选举为委员会成员。

1. 验证随机抽签结果

根据随机抽签算法输出的随机选举值和证明，其他节点也可以验证首领选举结果的合法性。

VerifyVRF(*pk*, *value*, *proof*, , )

如果验证结果为，则首领节点的验证成功，该首领是合法的；如果结果为，则首领节点的合法性将不被承认。

1. 分片委员会和根委员会中首领节点选举：每个委员会将有一个任期，每个任期又分为多个轮。每轮需要选举首领节点生成区块在委员会内部达成一致。为了降低共识时延，可以选择委员会中相互之间通信少的节点作为首领，降低网络资源消耗的同时提高共识的效率。

【方案一】通过路由算法委员会成员可以得知到其他成员节点的跳数，最终选择平均跳数最少的节点作为首领。记委员会成员数量为，则委员会节点到其他节点跳数的矩阵记为

其中表示节点到节点 之间的路由跳数，当时，表示节点到其自身的跳数为零。

【方案二】在无线网络通信中，节点的欧式距离会反映节点之间的通信情况。因此可以根据节点的位置和通信半径，采用最大独立子集的方式构建节点之间的通信骨架，最终选择出比较中心的节点作为首领。

1. 委员会一致性协议：确定委员会成员和首领之后，首领节点会生成和分发密钥份额给委员会其他成员。首领节点生成新的区块广播给委员会成员。委员会成员会验证区块、首领节点的合法性。委员会成员需要验证区块当前签名份额的有效性，并且有效签名份额的数量不能小于门限值。当签名数量达到阈值后会组成区块的最终签名，区块会被确认达成一致。委员会成员将区块链接到区块链并广播给其他非委员会成员。接收到确认区块的节点验证区块合法性成功后将区块连接到本地链上。
2. 跨分片交易：对于跨分片交易，我们采取一个原子提交协议。当出现跨分片交易时，与该交易相关的分片中的交易将被锁住。如果与该跨分片交易相关的交易都是合法有效的，确认该交易的有效性。否则该跨分片交易将被拒绝，随后分片中的交易被解锁。
3. 委员会重置：委员会任期结束之后，需要更换委员会成员。根据委员会的容错率来决定更换委员会成员的数量。为了更好的确保系统的安全性，委员会成员每次最多只更换稳定度最低的⌋个节点。

重点：利用随机抽签算法选举委员会成员，基于跳数或者位置的方式选举首领节点。采用基于门限签名的一致性协议在委员会内对区块达成一致。

难点：快速计算每个节点的稳定度和被选中概率，快速选举委员会成员和首领。获取其他节点的跳数信息和位置信息。计算门限签名中密钥份额的计算和分发，区块签名份额的收集和最终组合。跨分片交易死锁的问题。

解决的问题：解决节点公平性问题，确保每个节点都可能被选中成为委员会成员获得奖励。解决区块链分叉问题，委员会机制确保所有的节点都维护相同的区块链。解决跨分片交易死锁问题。

### （三）奖惩机制

1. 奖励机制：委员会任期结束，委员会内所有节点将平分任期内所有生成区块的奖励和交易费用。这样的奖励机制能激励系统中的节点积极维护系统区块链，提升系统的活性。
2. 惩罚机制：如果节点在未到活动时间结束之前离开系统，则会扣除部分押金。当发现有节点作恶后系统也会扣除押金。这个机制会降低节点离线和作恶的机会。

重点：采用奖励机制提高节点的活性和系统的安全性，使用惩罚机制降低节点作恶的动机。

难点：交易费用的计算，快速分配奖励给委员会成员。

解决的问题：解决节点缺乏活性问题，奖励机制可以激励节点积极地参与共识维护区块链。节点如果长期离线就会蒙受经济损失，解决节点长期离线的问题。

## 3.4 仿真实验

【描述：（一）实验目标，（二）实验方案（详细的实验方案，包括实验环境、实验步骤等），（三）技术难点（目前的技术难点、还需要补充的知识等）。】

### （一）实验目标

通过仿真实验测试交易吞吐量和区块确认延时分析区块系统的性能。

1. 交易吞吐量：单位时间内处理交易的数量；
2. 区块确认延时：区块确认的平均时延。

在仿真实验中需要测试不同区块大小、节点数量、节点密度的情况下区块链系统的交易吞吐量和区块确认延时。

考虑网络带宽，网络通信协议、单位时隙大小、编程语言、运行设备、测试次数等。

影响因素包括：区块大小、网络大小、节点密度等。

### （二）实验方案

如何来完成实验？在自己设计的区块链中采集数据进行分析？在公链上进行实验？实验步骤是什么？

无线自组织网络中测试区块链系统的性能需要在自己设计一个区块链进行数据采集和分析。实验步骤如下：

1. 搭建无线自组织网络：每个节点都以相同的移动速率在网络区域中随机移动，且在区域中的活动时间是有限的。对于节点之间的通信采用CSMA/CA作为通信协议。
2. 记录节点的活动时间：为每个节点赋予不同的活动时间，当活动时间结束则该节点离开网络。记录节点进入网络的时间。
3. 生成交易：构造一批不同的交易，确保他们的哈希不同。发送交易到网络中，并记录开始发送交易的时间。
4. 选举委员会成员：记录委员会选举开始的时间,根据任期长度记录委员会结束的时间。
5. 生成区块：每一轮开始从委员会成员中选举首领节点，首领节点生成区块并广播到网络中，记录每轮开始时间和区块发送时间。
6. 确认区块：委员会对区块达成一致结果确认区块。记录委员会节点的日志中区块确认的时间、每轮轮结束的时间和区块中交易的数量。
7. 计算区块确认延时：计算区块生成时间和确认时间可以得出区块的确认延时。
8. 计算平均交易吞吐量：计算一个委员会任期中所有区块中处理交易的数量，除以任期时长，可以得到平均交易吞吐量。

### （三）技术难点

根据设计的实验方案，目前的技术难点或需要学习的知识有哪些？

技术难点：在无线自组织网络上搭建区块链系统，计算稳定度依据的权重系数，获取其他节点的稳定度。节点活动起止时间记录，区块发送和确认时间记录，区块中交易数量计数，更换委员会成员。

待学习的知识：虚拟机配置、Socket编程、C++编程语言学习

# 基于节点稳定度的DAG区块链共识算法

## 模型假设

【简单描述：（一）区块链模型，包括节点之间的网络结构和特征、区块结构、存储结构等，例如，节点通信模型（节点拓扑或路由结构、信噪比模型等）、区块链存储模型（链式、DAG、…）等；（二）区块生成过程，包括交易打包、区块生成（包括共识）、区块上链等过程；（三）其它，包括其它与本论文紧密相关的部分。注意：重点剖析与本论文紧密相关的部分。】

### （一）区块链模型

在无线自组织网络环境中，链式存储的区块链。

1. 网络模型：考虑一个无线自组织网络，个节点随意部署在一个二维平面中。记为两个节点之间的欧氏距离， 为以节点为中心，通信半径为的圆盘。每个节点都拥有唯一的ID。假设节点可以在网络区域中随意移动，并且节点可以随意进入和离开这个区域。
2. 区块结构：每个节点局部地维护一个区块链。各区块通过引用前一个区块的哈希最终形成一条链的形式。每个区块中包含多个交易、自身区块的哈希、前一个区块的哈希、时间戳、区块的组合签名、区块的高度等信息。假设节点可以被公钥基础设施支持，并且系统中采用的密码学原语是安全的，因此没有恶意实体可以伪造消息。
3. 干扰和SINR模型：采用信号干扰模型能够很好的捕获无线网络的干扰。标准信号干扰的信噪比模型为

其中是节点接收到的节点的信号的功率，是平均信号发射功率，在节点处的干扰为

其中是在当前传输节点的集合，为环境噪声，路径损耗指数为，阈值取决于节点的硬件。假设节点可以进行物理载波监听。

### （二）区块生成过程

1. 交易的生成和广播：节点生成新交易根据主链相关性选择父单元，广播交易到网络。其他节点验证新交易的合法性后将交易链接上本地区块链。
2. 见证交易的生成和广播：根据节点的稳定度用随机抽签算法选举见证委员会成员和首领。首领节点生成交易并选择父交易单元后将新交易广播到见证委员会。见证委员会内部执行基于门限签名的一致性协议达成共识，最终将交易单元添加到本地区块链上并广播见证交易单元到网络。
3. 交易确认：根据见证交易单元确定主链并为每一个交易单元分配主链号全局排序。主链上稳定见证单元之前的交易单元都是固定不变的，因此这些交易单元被确认。此时被确认的交易单元的交易费用将会被分发给最小子交易单元和最近子见证单元。

### （三）其它

## 4.2 研究问题

【从技术层面描述：各个问题产生的背景和原因，针对每个问题分别给出若干个可能可行的方案。重点描述“研究问题”产生的原因和进行研究的必要性，对问题分析得越清晰、透彻，越有利于后面的研究；对方案只需进行简单描述，在下一节中再详细描述研究方案。】

无线自组织网络上的区块链系统的扩展性是有限的，更改区块链的结构可以提高区块链的扩展性加快交易处理效率。采用DAG作为存储结构的区块链系统可以并行处理交易，且节点数量的增加只会提高交易的处理效率，最终提高扩展性。但是，当交易流低时旧的交易会出现确认时延长甚至无法达成共识的问题。因此，需要设计适用于无线自组织网络的DAG区块链共识算法。

1. 交易确认延时长：原因？【无线设备网络资源有限且数量庞大，区块共识延时会受限于节点带宽】方案？【减小区块的规模提高区块达成共识的速率，降低区块确认时延；采用DAG区块链形式并发处理交易，即使拥有大量的无线设备，也能快速确认交易，并且提高扩展性】
2. 交易率低时无法确认交易：原因？【节点动态性高拓扑变化大，当节点生成交易数量低时无法通过交易数量来确认旧交易】方案？【主链方式来确认交易，即使交易数量少也能最终确认交易；采用委员会投票的方式确认交易可以确保最终所有交易最终都会被确认；】

## 4.3 研究方案

【详细描述“研究问题”中各方案的关键技术方案或算法，包括：方案或算法的细节、重点和难点、该技术方案解决“研究问题”中的哪个问题等。】

DAG区块链中节点可以同时生成交易，采用构建主链为交易分配主链号确认交易并解决冲突交易单元的问题。根据见证交易单元选择系统主链并且确定主链上的稳定点，稳定点之前的所有交易单元可以被确定全序。根据这个全序可以解决冲突交易单元，全序中最早出现的交易单元是合法的，另一个则是非法的。见证交易单元需要值得信任的节点生成，因此需要设计一个基于可信见证委员会DAG区块链共识算法。

### （一）定义稳定度

区块链系统中，新节点加入后要质押金钱获得在系统中活动的时间。活动的时长与交付的押金成正比。

记为节点在区块链系统中的剩余活跃时间，记为节点在最近个确认区块中参与共识比值，定义节点的稳定度为

其中，权重系数可根据偏好设置。在区块链系统运行初期，确认区块数量不足个时记节点的共识比为零，此时节点的稳定度主要受节点的活动时间的影响。

重点：计算节点的剩余活动时间、节点的共识比和这两个度量的权重系数。

难点：计算影响节点稳定度的度量的权重系数，测量节点的共识比，计算其他节点的稳定度，验证首领节点的合法性。

解决的问题：解决工作量证明选取首领节点消耗巨大算力，解决首领节点突然离开系统导致，押金机制也可以防止敌手发起女巫攻击。

### （二）共识算法

DAG区块链系统需要一个基于见证委员会的共识算法决定主链对交易全局排序。基于见证委员会的共识算法主要是节点生成新交易后，根据见证交易选择父单元。从顶端交易单元往创世交易单元回溯的路径可以找到一条主链。根据见证交易单元最终确定一条系统主链，并确定主链上的稳定点。共识算法中见证委员会机制主要包括几个部分：委员会成员和首领节点的选举、一致性协议和委员会重置。我们根据节点的稳定度决定节点被选中的概率。一致性协议则是采用门限签名方式，让委员会成员不需要二次通信就能对区块达成一致。

1. 随机选举见证委员会成员：我们采用随机抽签算法选举委员会节点，将上一个见证交易单元的哈希作为随机种子，通过随机可验证函数计算得到抽签结果和证明，其他节点可以根据证明验证该节点的合法性。
2. 随机抽签算法

随机抽签算法根据节点的稳定度决定节点被选中的概率。记是节点的稳定度，所有节点的稳定度之和为，那么节点被选中的概率为且有。为了确定被选中的节点，将区间分为连续的多个区间

.

随机可验证函数将区块的高度和最终签名作为输入计算得到一个值和证明

满足的前个节点被选举为见证委员会成员。

1. 验证随机抽签结果

根据随机抽签算法输出的随机选举值和证明，其他节点也可以验证首领选举结果的合法性。

VerifyVRF(*pk*, *value*, *proof*, )

如果验证结果为，则首领节点的验证成功，该首领是合法的；如果结果为，则首领节点的合法性将不被承认。

1. 首领节点选举：每个委员会将有一个任期，每个任期又分为多个轮。每轮需要选举首领节点生成区块在委员会内部达成一致。选择委员会中相互之间通信资源消耗少的节点作为首领，提高委员会达成一致的效率。

【方案一】通过路由算法委员会成员可以得知到其他成员节点的跳数，最终选择平均跳数最少的节点作为首领。记委员会成员数量为，则委员会节点到其他节点跳数的矩阵记为

其中表示节点到节点 之间的路由跳数，当时，表示节点到其自身的跳数为零。

【方案二】在无线网络通信中，节点的欧式距离会反映节点之间的通信情况。因此可以根据节点的位置和通信半径，采用最大独立子集的方式构建节点之间的通信骨架，最终选择出比较中心的节点作为首领。

1. 一致性协议：确定委员会成员和首领之后，首领节点会生成和分发密钥份额给委员会其他成员。首领节点广播新的交易给委员会成员。委员会成员会验证交易、首领节点的合法性以及当前签名份额的有效性。当对于交易的签名份额数量达到阈值后会组成见证交易的最终签名，委员会对见证交易达成一致。委员会成员将见证交易单元链接到DAG区块链并广播给其他非委员会成员。接收到确认区块的节点验证区块合法性成功后将见证交易连接到本地链上。
2. 委员会重置：委员会任期结束之后，需要更换委员会成员。根据委员会的容错率来决定更换委员会成员的数量。为了更好的确保系统的安全性，委员会成员每次最多只更换稳定度最低的⌋个节点。
3. 主链机制：可以根据见证交易单元来确定系统主链，并且确定稳定点。系统主链中稳定点之前的交易单元是完全相同的，因此可以为主链上的交易单元分配主链号，稳定点之前的所有交易可以被确定全序。对于冲突交易只承认最早出现交易的合法性，解决了交易双花的问题。

重点：利用随机抽签算法选举委员会成员，基于跳数或者位置的方式选举首领节点。采用基于门限签名的一致性协议在委员会内对见证交易达成一致。

难点：快速计算每个节点的稳定度和被选中概率，快速选举委员会成员和首领。获取其他节点的跳数信息和位置信息。计算门限签名中密钥份额的计算和分发，区块签名份额的收集和最终组合。

解决的问题：解决见证交易的信任问题，确保见证交易的可信性。解决见证委员会成员稳定性问题，确保每个被选中成为委员会成员都是可信的且短期内都不会离开系统。

### （三）奖惩机制

1. 奖励机制：当交易给定系统主链号只会，该交易的交易费会分发给其最小子交易和稳定见证交易所属的见证委员会成员。
2. 惩罚机制：如果节点在未到活动时间结束之前离开系统，则会扣除部分押金，如果发现有节点作恶，也会扣除押金，从而降低节点离线和作恶的机会。

重点：采用奖励机制提高节点的活性和系统的安全性，使用惩罚机制降低节点作恶的动机。

难点：交易费用的计算，快速分配奖励给委员会成员。

解决的问题：解决节点缺乏活性问题，奖励机制可以激励节点积极地参与共识维护区块链。节点如果长期离线就会蒙受经济损失，解决节点长期离线的问题。

## 4.4 仿真实验

【描述：（一）实验目标，（二）实验方案（详细的实验方案，包括实验环境、实验步骤等），（三）技术难点（目前的技术难点、还需要补充的知识等）。】

### （一）实验目标

通过仿真实验测试交易吞吐量和交易确认延时分析区块系统的性能。

1. 交易吞吐量：单位时间内处理交易的数量；
2. 交易确认延时：交易确认的平均时延。

在仿真实验中需要测试不同交易到达率、节点数量、节点密度的情况下DAG区块链系统的交易吞吐量和交易确认延时。

考虑网络带宽，网络通信协议、单位时隙大小、编程语言、运行设备、测试次数等。

影响因素包括：交易到达率、网络大小、节点密度等。

### （二）实验方案

如何来完成实验？在自己设计的区块链中采集数据进行分析？在公链上进行实验？实验步骤是什么？

无线自组织网络中测试区块链系统的性能需要在自己设计一个区块链进行数据采集和分析。实验步骤如下：

1. 搭建无线自组织网络：每个节点都以相同的移动速率在网络区域中随机移动，且在区域中的活动时间是有限的。对于节点之间的通信采用CSMA/CA作为通信协议。
2. 记录节点的活动时间：为每个节点赋予不同的活动时间，当活动时间结束则该节点离开网络。记录节点进入网络的时间。
3. 生成交易：为每个节点设置相同的交易到达率，构造一批不同的交易，确保他们的哈希不同，并记录开始发送交易的时间。
4. 选举见证委员会成员：记录委员会选举开始的时间,根据任期长度记录委员会结束的时间。并记录每个见证交易的发送时间。
5. 确认交易：根据见证交易单元确定系统主链和稳定点。对于稳定点之前的交易可以被确认，并记录交易的确认时间。
6. 计算交易确认延时：记录两个稳定点之间交易的确认时延，可以得到最大确认时延、最小确认时延和屁股军确认时延。
7. 计算平均交易吞吐量：计算系统主链中两个稳定点之间的交易数量，除以稳定点的确认时间间隔，可以得到平均交易吞吐量。

### （三）技术难点

根据设计的实验方案，目前的技术难点或需要学习的知识有哪些？

技术难点：在无线自组织网络上搭建区块链系统，计算稳定度依据的权重系数，获取其他节点的稳定度。节点活动起止时间记录，交易发送和确认时间记录，更换委员会成员。

待学习的知识：虚拟机配置、Socket编程、C++编程语言学习。

# 接下来主要的工作

## 节点自启机制

无线移动自组织网络具有抗单点故障、网络拓扑结构动态变化、节点路由转发以及资源有限等特性。无线自组织网是一个对等网络，节点能够随时加入和离开网络。单个节点故障并不会影响整个网络的运行。无线移动自组织网络的网络拓扑结构是动态变化的。节点可以随时开机和关机、节点发送功率变化、无线信道之间的相互干扰以及地形等因素都会影响网络的拓扑结构。由于节点发射功率和覆盖范围有限，节点与通信范围之外的节点通信时需要中间节点转发。无线自组网中的多跳路由是由普通节点共同协作完成，并不需要专门的路由设备。无线信道本身的物理特性决定了无线自组织网络的带宽比有线信道要低很多，而竞争共享无线信道产生的碰撞、信号衰减、噪音干扰及信道干扰等因素使得节点的实际带宽远远小于理论值。同时节点虽然具有轻便和移动性好的优点，但是也有电源有限、内存小、CPU性能低的缺点。

无线自组织网络上的区块链系统需要考虑信号干扰噪声模型。采用信号干扰噪声模型，能够很好的捕获无线网络的干扰。标准信号干扰的信噪比模型为

其中是节点接收到的节点的信号的功率，是平均信号发射功率，在节点处的干扰为

其中是在当前传输节点的集合，为环境噪声，路径损耗指数为，阈值取决于节点的硬件。假设节点可以进行物理载波监听。

无线区块链网络中，新节点自启机制包括几个部分：节点身份广播、其他节点身份信息获取、同步区块链。

1. 节点身份广播：节点第一次进入网络之后，通过广播自身ID(IP地址)给单跳邻居节点。接收到新节点信息的节点会将新的节点信息广播给它的单跳邻居节点。最终全网会知道新节点的ID（IP地址）。
2. 节点其他节点信息：节点会向邻居节点索取他们已知的其他节点的ID(IP地址)，可以获取其他节点的信息，方便之后建立与其他节点的通信连接。
3. 数据同步：节点进入网络之后会选择与邻居节点同步。节点选择比对多个单跳邻居节点的区块链信息（区块链高度和区块链哈希），选择具有公共前缀的最长链。可以比较选择最近节点同步区块链、随机选择四个单跳邻居节点比对来同步区块链，两种方式同步区块链的优劣。

## 5.2 基于稳定度的节点选举

区块链系统中，新节点加入后要质押金钱获得在系统中活动的时间。活动的时长与交付的押金成正比。

记为节点在区块链系统中的剩余活跃时间，记为节点在最近个确认区块中参与共识比值，定义节点的稳定度为

其中，权重系数可根据偏好设置。在区块链系统运行初期，确认区块数量不足个时记节点的共识比为零，此时节点的稳定度主要受节点的活动时间的影响。还可以设计一个过滤函数避免节点由于稳定度过高或者共识比率过大长期被选中成为委员会成员或者首领节点。

## 5.3 门限签名机制的原理

委员会内部可以执行基于门限签名的一致性协议避免节点之间二次通信，提高委员会内达成一致的效率和安全性。门限签名是基于双线性映射构造的。

1. 基于椭圆曲线的门限签名原理：
2. 双线性映射：对于一个质数双线性群可以由五元组来描述。五元组中是一个与给定安全常数相关的大质数，均是阶为的乘法循环群，为双线性映射满足以下3个条件：
   * + - 1. 双线性（Bilinearity）：对于任意的，有;
         2. 非退化性（Non-degeneracy）：至少存在元素，满足；
         3. 可计算性（Efficiency）：对于任意的，存在有效算法高效计算。

双线性映射，即利用一个特殊的函数，把一条或两条不同曲线上的两个点和映射为一个数：

1. 门限签名：可实现签名聚合和密钥聚合。BLS签名包括：初始化、密钥生成、签名、验证四个部分。
2. 初始化：是阶为的乘法循环群，生成元分别是，为双线性映射，安全哈希函数：实现签名消息映射到循环群中的一点，公开参数为
3. 密钥生成：选择随机数，将作为私钥，公钥为，得到公私钥对。
4. 签名：将消息（区块、交易等数据）映射到循环群中的一点记为，并使用私钥签名
5. 验证：公钥验证签名是否成立。证明过程为
6. 基于RSA的门限签名算法：

门限签名方案是指由个成员组成一个签名群体，该群体有一对公钥和私钥，群体内大于等于个合法、诚实的成员组合可以代表群体用群私钥进行签名，任何人可利用该群体的公钥进行签名验证。这里是门限值，只有大于等于个合法成员才能代表群体进行签名，群体中任何个或更少的成员不能代表该群体进行签名，同时任何成员不能假冒其他成员进行签名。

1. RSA算法
2. RSA加解密：
3. 密钥生成：选择两个互异的大素数，两者保密，计算，公开。计算并保密，选择一个公开的随机数满足。计算并保密。公钥为, 私钥为。
4. 加密：加密结果，已知条件，公钥为。
5. 解密：解密结果，已知条件，公钥为。
6. RSA签名验证：选取整数，消息空间与签名空间均为整数空间，即，定义密钥集合为。对于签名即为，验证为是否成立。
7. 门限签名算法

门限签名算法包括初始化、密钥分享、生成门限签名份额、组合签名份额以及签名验证。

1. 初始化：系统中有个参与者，Alice选择两个大素数,其中也是素数。计算，并且选择一个素数指数，公钥为
2. 密钥分享: Alice选择满足，其中是Alice要分享的秘密。设，Alice随机选择，其中为门限值。构成多项式。其余参与者的密钥值为。计算验证密钥用于验证签名的是否有效。Alice选择随机数并计算。计算拉格朗日系数：记，对于大小为的子集。对热议元素，定义拉格朗日系数 ，计算拉格朗日公式得到。
3. 生成门限签名份额：计算关于消息（区块或者交易数据）的签名份额。令，其余参与者计算作为其签名份额。计算每个签名份额的正确性证明以及如何验证这个签名份额：记为的比特长度，是一个哈希函数，输出为一个比特的整数。为了生成正确性证明，参与者选择随机数，计算

正确性的验证变成了，即只需证明下列等式成立

1. 组合签名份额：在组合所有签名份额之前，先要验证每一个签名份额，并且要满足有效的签名份额个数不能小于门限。假设此处有一组有效的签名份额集合。令，假设，组合签名的份计算为

根据可得。由于可计算得到组合后的签名为且都是整数。

1. 签名验证：验证签名与RSA签名验证逻辑一样：计算，其中是组合后的签名结果。验证者只需要验证是否成立。

## 5.4 可验证随机函数的原理

随机可验证函数有两种，一种是基于椭圆曲线的VRF，一种是基于RSA的VRF。

1. 随机抽签算法

随机抽签算法根据节点的稳定度决定节点被选中的概率。记是节点的稳定度，所有节点的稳定度之和为，那么节点被选中的概率为且有。为了确定被选中的节点，将区间分为连续的多个区间

.

随机可验证函数将区块的高度和最终签名作为输入计算得到一个值和证明

满足的前个节点被选举为委员会成员。

1. 验证随机抽签结果

根据随机抽签算法输出的随机选举值和证明，其他节点也可以验证首领选举结果的合法性。

VerifyVRF(pk, value, proof, )

如果验证结果为，则首领节点的验证成功，该首领是合法的；如果结果为，则首领节点的合法性将不被承认。