**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](#_Toc94273349)

[1.1 模型假设（框架） 3](#_Toc94273350)

[1.2 研究问题 3](#_Toc94273351)

[1.3 研究方案 3](#_Toc94273352)

[（1）定义稳定度 4](#_Toc94273353)

[（2）共识算法 4](#_Toc94273354)

[（3）奖惩机制 4](#_Toc94273355)

[1.4 仿真实验 4](#_Toc94273356)

[2. 稳定的委员会区块链共识算法 4](#_Toc94273357)

[2.1 模型假设（框架） 4](#_Toc94273358)

[2.2 研究问题 4](#_Toc94273359)

[2.3 研究方案 5](#_Toc94273360)

[（1）定义稳定度 5](#_Toc94273361)

[（2）共识算法 5](#_Toc94273362)

[（3）奖惩机制 5](#_Toc94273363)

[2.4 仿真实验 5](#_Toc94273364)

[3. 稳定的分片区块链共识算法 5](#_Toc94273365)

[3.1 模型假设（框架） 5](#_Toc94273366)

[3.2 研究问题 6](#_Toc94273367)

[3.3 研究方案 6](#_Toc94273368)

[（1）定义稳定度 6](#_Toc94273369)

[（2）共识算法 6](#_Toc94273370)

[（3）奖惩机制 7](#_Toc94273371)

[3.4 仿真实验 7](#_Toc94273372)

[4. 基于节点稳定度的DAG区块链共识算法 7](#_Toc94273373)

[4.1 模型假设（框架） 7](#_Toc94273374)

[4.2 研究问题 7](#_Toc94273375)

[4.3 研究方案 7](#_Toc94273376)

[（1）定义稳定度 8](#_Toc94273377)

[（2）共识算法 8](#_Toc94273378)

[（3）奖惩机制 8](#_Toc94273379)

[4.4 仿真实验 8](#_Toc94273380)

[5. 接下来主要的工作 8](#_Toc94273381)

[5.1 节点自启机制 8](#_Toc94273382)

[5.2 基于稳定度的节点选举 9](#_Toc94273383)

[5.3 门限签名机制的原理 9](#_Toc94273384)

[5.4 可验证随机函数的原理 9](#_Toc94273385)

在2022年准备完成四篇关于区块链共识算法相关的小论文，工作具体内容如下。

# 基于节点稳定度的区块链共识算法

## 模型假设（框架）

【简单描述区块链模型】在无线多跳网络环境中，链式存储的区块链。在这种区块链中包括：网络模型（什么样的？）、区块结构（什么样的？）、区块链的存储结构、……

1. 网络模型：考虑一个多跳无线自组织网络，个节点随意部署在一个二维平面中移动。记为两个节点之间的欧氏距离， 是以节点为中心，以节点通信半径为半径的圆盘。每个节点都拥有唯一的ID。假设节点可以随意移动，这意味着节点可以进入这个区域，也可以离开这个区域。
2. 区块结构：每个节点局部的维护一个区块链。每个区块都是通过引用前一个区块的哈希最终形成一条链的形式。每个区块都包含有多个交易、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。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欺骗消息。
3. 干扰和SINR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。标准信号干扰噪声比模型为

其中是节点从节点处接收信号功率，而 是均匀信号发射功率；在节点处的干扰为，其中是在当前轮中传输的节点的集合。记环境噪声为，路径损耗指数为，阈值取决于硬件。假设节点可以进行物理载波监听。

【简单描述区块生成过程】交易提交、交易广播、区块生成（共识过程）、区块广播、区块确认、区块入链、……

1. 交易的提交和广播：每个节点发现新交易之后，可以提交交易到网络。通常采用广播的形式发送给其他节点。节点接收到新的交易之后，需要验证交易的合法性，验证成功后放入在本地交易未处理交易池中。
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。

【重点剖析与研究问题紧密相关的几个部分】网络特征、节点参与共识过程、节点自启机制、区块确认机制、区块奖惩机制、……

## 研究问题

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比较大且不可预测，导致首领节点或者首领节点的邻居突然消失，最终无法达成共识】方案？【将节点的稳定度作为首领选举的依据，最终选定的首领不会出现突然离线的情况；将节点到其他节点的跳数作为首领选举的依据，降低网络资源的消耗；见节点的位置作为首领选举的依据，尽可能确保首领节点覆盖足够多的节点；】

## 1.3 研究方案

### （1）定义稳定度

区块链系统中，新节点进入网络之后，需要质押金钱来获得在这个区块链系统中活动的时间，根据活动时间的长短来选择质押金额的多少【租约时长可以通过租约机制+时间戳实现;或者可以根据权益的大小确定节点的活跃度（节点的活跃度也极大的表明节点是否愿意继续在系统中工作）；】

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【可以多次实验分析计算】。在区块链系统运行初期，确认区块数量不足个时节点的共识比记为零，此时主要通过节点的剩余时间来挖矿。

### （2）共识算法

共识算法中，每个节点都拥有自己的稳定度，根据节点的稳定度随机选举出块节点。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。共识算法分为两个部分：出块节点的选择和区块的确认。

1. 出块节点的随机选举：采用随机抽签的方式选择出块节点的方法需要满足几点：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。随机抽签中将上一个区块的高度和最终签名的哈希作为随机种子，采用可验证随机函数选出新的出块者，其他节点可以验证该节点的合法性。
2. 随机抽签算法：

记是节点的稳定度，所有节点的稳定度之和记为，那么节点被选中的概率为且服从二项分布。为了确定被选中的节点，将区间分为连续的多个区间

.

利用随机可验证函数可计算得到一个值和证明

若在某个区间之内，则该区间的所属节点作为被选中的出块节点。

1. 可验证抽签结果

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

如果为，则验证成功，如果为则出块节点的权限合法性将会受到质疑。

1. 区块密钥分割：出块节点生成区块之后，会计算关于区块的签名份额。通常这个份额根据系统中节点数量来决定的，并将节点的密钥份额广播给这些节点，出块节点随后广播区块到网络。
2. 区块确认：其他节点接收区块之后，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。

### （3）奖惩机制

1. 奖励机制：区块的奖励和交易费用分发给出块者和确认区块的节点，确保系统的活性和安全性。或者也可以拿出一笔费用奖励给后一个区块的
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。

## 1.4 仿真实验

通过仿真实验验证共识算法的性能：吞吐量和确认延时。

吞吐量：单位时间内处理交易的数量；

区块确认延时：区块确认的平均时延。

仿真实验中需要考虑网络带宽，网络通信协议、环境噪声、信号传输功率、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：网络大小、信号干扰噪声比参数、节点密度等。

# 稳定的委员会区块链共识算法

## 模型假设（框架）

【简单描述区块链模型】在无线多跳网络环境中，链式存储的区块链。在这种区块链中包括：网络模型（什么样的？）、区块结构（什么样的？）、区块链的存储结构、……

1. 网络模型：考虑一个多跳无线自组织网络，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， 是以节点为中心，以节点通信半径为半径的圆，每个节点都拥有唯一的ID。假设节点可以以相同的速率随意移动，这意味着节点可以进入这个区域，也可以离开这个区域。
2. 区块结构：每个节点局部的维护一个区块链。每个区块都是通过引用前一个区块的哈希最终形成一条链的形式。每个区块都包含有多个交易、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。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欺骗消息。
3. 干扰和SINR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。标准信号干扰噪声比模型为

其中 是节点从节点处接收信号功率，而 是均匀信号发射功率；在节点处的干扰为，其中是在当前轮中传输的节点的集合。记环境噪声为，路径损耗指数为，阈值取决于硬件。假设节点可以进行物理载波监听。

【简单描述区块生成过程】交易提交、交易广播、委员会选举、区块生成（共识过程）、区块确认、区块入链、区块广播、……

1. 交易的提交和广播：每个节点发现新交易之后，可以提交交易到网络。通常采用广播的形式发送给其他节点。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：根据节点的稳定度决定节点被选中的概率，采用随机可验证的方式来选择一个委员会，同时采用基于平均跳数或者基于节点位置的方式选择出一个首领节点。
3. 区块的生成：节点发现自己成为首领节点之后，会从交易池中取出交易打包成分片区块作为提案广播给其他委员会成员。同时也会根据委员会的大小分割密钥份额给其他成员（委员会成员的数量最好是奇数），随后广播区块到网络。
4. 区块确认和上链：接收到区块的节点验证区块、首领和签名份额的合法性，如果拥有该区块的密钥份额，则还需要对该区块签名，并广播签名结果。当签名份额达到某一阈值之后，会形成一个区块的最终签名，此时区块被确认并添加到各节点的本地链上。

【重点剖析与研究问题紧密相关的几个部分】网络特征、节点参与共识过程、节点自启机制、区块确认机制、区块奖惩机制、……

## 2.2 研究问题

在无线多跳网络环境中，单首领共识算法过程缓慢，且只具有弱一致性，达成共识时间比较长。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无线多跳网络中的委员会共识算法。

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，因此需要网络传输时延比较长】方案？【多个节点达成共识之后，同时广播新区块广播区域会更大，广播区块到全网所需要的时延将降低；】
2. 算法具有弱一致性：原因？【节点生成区块之后需要一段不确定时间之后才能获得其他节点的认可，且每个节点认可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。只要委员会认可的区块，其他非委员会的成员必须认可，从而确保对每个区块都能达成强一致性；】
3. 节点的网络传输延时：原因？【节点需要多跳才能将区块传输到较远的节点，跳数越多则延时越高】方案？【将委员会内每个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，可以有效的降低节点达成一致的时延；】

## 2.3 研究方案

### （1）定义稳定度

区块链系统中，新节点进入网络之后，需要质押金钱来获得在这个区块链系统中活动的时间，根据活动时间的长短来选择质押金额的多少【租约时长可以通过租约机制+时间戳实现;或者可以根据权益的大小确定节点的活跃度（节点的活跃度也极大的表明节点是否愿意继续在系统中工作）；】

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【可以多次实验分析计算】。在区块链系统运行初期，确认区块数量不足个时节点的共识比记为零，此时主要通过节点的剩余时间来挖矿。

### （2）共识算法

共识算法每个节点都拥有自己的稳定度，根据节点的稳定度随机选举委员会。共识算法分为以下几个部分：委员会成员和首领选举、委员会对新区块达成一致、区块上链、委员会重置。委员会选举机制采用稳定度作为委员会成员的选举度量，采用随机抽签中将上一个区块的高度和最终签名的哈希作为随机种子，采用可验证随机函数选出新的出块者，其他节点可以验证该节点的合法性。

1. 委员会的随机选举：采用随机抽签的方式选择委员会成员和首领。随机抽签中将上一个区块的高度和最终签名的哈希作为随机种子，采用可验证随机函数选出委员会成员，其他节点可以验证各个成员的合法性。
2. 随机抽签算法：

记是节点的稳定度，所有节点的稳定度之和记为，那么节点被选中的概率为且服从二项分布。为了确定被选中的节点，将区间分为连续的多个区间

.

利用随机可验证函数可计算得到一个值和证明

若，选择前个节点成为委员会成员。

1. 可验证抽签结果

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

如果为，则验证成功，如果为则委员会成员权限的合法性将会受到质疑。

1. 首领节点的选举：每个委员会将有一个任期，每个任期又分为多个轮。吗，每一轮都会执行一次一致性协议。每轮开始都需要选择一个首领生成区块，并作为提案让委员会内部达成一致。委员会中节点的数量相对较少，为了降低共识时延，可以选择相互之间通信较少的节点作为首领，降低网络资源消耗的同时提高共识的效率。

【方案一】通过路由算法我们可以获得委员会内成员到其他成员的跳数，最终选择平均跳数最少，且稳定度最高的节点作为首领。记委员会成员数量为，则委员会成员到其他成员跳数的矩阵记为

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】由于在无线网络通信中，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：
2. 密钥分割：首领生成区块，并将区块的密钥进行分割发送给委员会的成员，随后广播区块。
3. 委员会成员签名收集：委员会成员收到区块之后，验证区块和签名份额的合法性，并附上自己的签名。
4. 签名组合：当区块的签名数量达到阈值之后，可以得到一个最终的签名，此时委员会成员对于区块的合法性达成一致。将区块链接到自己的本地链上，并广播给其他非委员会成员。
5. 区块上链：接收到委员会发来区块的节点，验证区块和签名的合法性后接受该区块，并且链接到其本地链上。
6. 委员会重置：新的任期需要重置更换部分委员会成员，分析更换多少数量的成员可以保证委员会的安全。
7. 委员会容错率：采用门限签名机制的委员会的容错率与门限阈值的设计有关，通常可以容错率不超过50%。
8. 委员会更换：委员会中稳定度较低的节点将会被更换，更换数量不得超过委员会成员的一半。为了更好的确保系统的安全性，我们每次可以只更换最多⌋成员。依然采用随机抽签的方式选举出新的委员会成员替换旧的委员会成员。

### （3）奖惩机制

1. 奖励机制：区块奖励和交易费用将会平均分发给委员会成员。
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。

## 2.4 仿真实验

通过仿真实验验证共识算法的性能：吞吐量和确认延时。

1. 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。

仿真实验中需要考虑网络带宽，网络通信协议、环境噪声、信号传输功率、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：网络大小、信号干扰噪声比参数、节点密度、节点数量、区块大小、任期长度、轮长度等。

# 稳定的分片区块链共识算法

## 模型假设（框架）

【简单描述区块链模型】在无线多跳网络环境中，链式存储的区块链。在这种区块链中包括：网络模型（什么样的？）、区块结构（什么样的？）、区块链的存储结构、……

1. 网络模型：考虑一个多跳无线自组织网络，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， 是以节点为中心，以节点通信半径为半径的圆，每个节点都拥有唯一的ID。假设节点可以以相同的速率随意移动，这意味着节点可以进入这个区域，也可以离开这个区域。
2. 区块结构：每个节点局部的维护一个区块链。每个区块都是通过引用前一个区块的哈希最终形成一条链的形式。每个区块都包含有多个交易、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。交易采用UTXO模型可以确保安全性。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欺骗消息。
3. 干扰和SINR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。标准信号干扰噪声比模型为

其中 是节点从节点处接收信号功率，而 是均匀信号发射功率；在节点处的干扰为，其中是在当前轮中传输的节点的集合。记环境噪声为，路径损耗指数为，阈值取决于硬件。假设节点可以进行物理载波监听。

【简单描述区块生成过程】交易提交、交易广播、委员会选举、区块生成（共识过程）、区块确认、区块入链、区块广播、……

1. 交易的提交和广播：每个节点发现新交易之后，可以提交交易到网络。通常采用广播的形式发送给其他节点。节点接收到新的交易之后，需要验证交易的合法性，验证成功后放入在本地交易未处理交易池中。
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，采用随机可验证的方式来选择一个委员会，同时采用基于平均跳数或者基于节点位置的方式选择出一个首领节点。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择根委员会的首领。
3. 分片区块生成：分片首领会提出分片区块，并通过门限签名的方式在委员会内达成一致。随后将分片区块提交给最终委员会成员。根委员会成员首领收集所有的分片区块，最终形成一个总区块并将其作为提案广播给根委员会其他成员。
4. 最终区块的确认和上链：接收到总区块的根委员会成员将验证区块、首领和签名份额的合法性，如果拥有该区块的密钥份额，则还需要对该区块签名，并广播签名结果。当签名份额达到某一阈值之后，会形成一个区块的最终签名，此时区块被确认并添加到各节点的本地链上。根委员会成员将总区块广播到自己的分片中，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。

【重点剖析与研究问题紧密相关的几个部分】网络特征、节点参与共识过程、区块确认机制、区块奖惩机制、……

## 3.2 研究问题

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，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？【节点数量增加，使得参与共识节点之间的通信会增加，最终导致需要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；基于位置来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，确保委员会成员能够在共识达成（委员会成员可能由于位置较远使得需要多跳才能达成共识，共识的网络资源需求依然很大）之后，快速将结果广播给其他非委员会成员。】
2. 节点的网络传输延时：原因？【节点需要多跳才能将区块传输到较远的节点，跳数越多则延时越高】方案？【将节点按照网络特性（比如位置、跳数）进行分片后，依然根据分片内节点的稳定度来选择委员会成员，随后将委员会内每个节点到其他节点的距离和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网络传输延时最低，可以有效的降低节点达成一致的网络时延；】
3. 跨分片交易：原因？【跨分片通信延时高，导致跨分片交易在处理过程中，由于分片内交易快速处理导致跨分片交易出现死锁】方案【采用原子提交协议，一旦出现跨分片交易，在该交易才结束之前，其相关建议都要被锁定，直到跨分片交易提交或者被拒绝，其相关交易才会被解锁；如果两个分片内跨分片交易比较多，分片通信比较频繁，则将两个委员会融合为一个，从而就可以避免出现跨分片交易死锁的问题；采用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

### （1）定义稳定度

区块链系统中，新节点进入网络之后，需要质押金钱来获得在这个区块链系统中活动的时间，根据活动时间的长短来选择质押金额的多少【租约时长可以通过租约机制+时间戳实现;或者可以根据权益的大小确定节点的活跃度（节点的活跃度也极大的表明节点是否愿意继续在系统中工作）；】

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【可以多次实验分析计算】。在区块链系统运行初期，确认区块数量不足个时节点的共识比记为零，此时主要通过节点的剩余时间来挖矿。

### （2）共识算法

共识算法每个节点都拥有自己的稳定度，根据节点的稳定度随机选举分片委员会。共识算法分为以下几个部分：分片委员会成员和首领选举、分片委员会对区块达成一致、根委员会首领节点选举、根委员会对总区块达成一致、区块上链、委员会重置。委员会选举机制采用稳定度作为委员会成员的选举度量，将上一个区块的高度和最终签名的哈希作为随机种子，采用可验证随机函数选出新的出块者，其他节点可以验证该节点的合法性。

1. 委员会选举机制采用稳定度作为委员会成员的选举度量，采用随机抽签中将上一个区块的高度和最终签名的哈希作为随机种子，采用可验证随机函数选出新的出块者，其他节点可以验证该节点的合法性。
2. 随机抽签算法：

记是节点的稳定度，所有节点的稳定度之和记为，那么节点被选中的概率为且服从二项分布。为了确定被选中的节点，将区间分为连续的多个区间

.

利用随机可验证函数可计算得到一个值和证明

若，选择前个节点成为委员会成员。

1. 可验证抽签结果

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

如果为，则验证成功，如果为则委员会成员权限的合法性将会受到质疑。

1. 首领节点的选举：每个委员会将有一个任期，每个任期又分为多个轮。吗，每一轮都会执行一次一致性协议。每轮开始都需要选择一个首领生成区块，并作为提案让委员会内部达成一致。委员会中节点的数量相对较少，为了降低共识时延，可以选择相互之间通信较少的节点作为首领，降低网络资源消耗的同时提高共识的效率。

【方案一】通过路由算法我们可以获得委员会内成员到其他成员的跳数，最终选择平均跳数最少，且稳定度最高的节点作为首领。记委员会成员数量为，则委员会成员到其他成员跳数的矩阵记为

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】由于在无线网络通信中，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：
2. 密钥分割：首领生成区块，并将区块的密钥进行分割发送给委员会的成员，随后广播区块。
3. 委员会成员签名收集：委员会成员收到区块之后，验证区块和签名份额的合法性，并附上自己的签名。
4. 签名组合：当区块的签名数量达到阈值之后，可以得到一个最终的签名，此时委员会成员对于区块的合法性达成一致。将区块链接到自己的本地链上，并广播给其他非委员会成员。
5. 区块上链：接收到委员会发来区块的节点，验证区块和签名的合法性后接受该区块，并且链接到其本地链上。
6. 根委员会：根委员会首领选举可以采用与分片委员会相同的方式，从而减少共识节点之间的通信。并且采用与分片委员会相同的一致性协议可以确保对总区块共识的快速达成。
7. 委员会重置：新的任期需要重置更换部分委员会成员，分析更换多少数量的成员可以保证委员会的安全。

委员会容错率：采用门限签名机制的委员会的容错率与门限阈值的设计有关，通常可以容错率不超过50%。

委员会更换：委员会中稳定度较低的节点将会被更换，更换数量不得超过委员会成员的一半。为了更好的确保系统的安全性，我们每次可以只更换最多⌋成员。依然采用随机抽签的方式选举出新的委员会成员替换旧的委员会成员。

### （3）奖惩机制

1. 奖励机制：区块奖励和交易费用将会根据每个分片的参与情况分发到每个分片中，每个分片委员会的成员可以平均分配其所在分片的奖励。
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。

## 3.4 仿真实验

通过仿真实验验证共识算法的性能：吞吐量和确认延时。

1. 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。

仿真实验中需要考虑网络带宽，网络通信协议、环境噪声、信号传输功率、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：网络大小、信号干扰噪声比参数、节点密度、节点数量、区块大小、任期长度、轮长度等

# 基于节点稳定度的DAG区块链共识算法

## 模型假设（框架）

【简单描述区块链模型】在无线多跳网络环境中，链式存储的区块链。在这种区块链中包括：网络模型（什么样的？）、区块结构（什么样的？）、区块链的存储结构、……

1. 网络模型：考虑一个多跳无线自组织网络，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， 是以节点为中心，以节点通信半径为半径的圆盘。每个节点都拥有唯一的ID。假设节点可以随意移动，这意味着节点可以进入这个区域，也可以离开这个区域。系统中存在两种节点类型：一般节点可以生成交易单元，并且通过根据主链相关性选择多个最优父单元；见证节点则需要通过见证委员会才能生成见证单元，并且见证单元之间有前后顺序。见证单元也能通过主链相关性引用多个父单元。
2. 区块结构：每个节点局部的维护一个区块链。每个交易单元只有一个交易，每个区块单元可以引用多个父交易单元的哈希最终形成DAG链的形式。每个单元都包含有多个父交易单元、一个交易、时间戳、单元的签名、主链号等。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欺骗消息。
3. 干扰和SINR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。标准信号干扰噪声比模型为

其中 是节点从节点处接收信号功率，而 是均匀信号发射功率；在节点处的干扰为，其中是在当前轮中传输的节点的集合。记环境噪声为，路径损耗指数为，阈值取决于硬件。假设节点可以进行物理载波监听。

【简单描述区块生成过程】交易生成、交易广播、交易入链、交易确认……

1. 交易的生成和广播：节点生成新交易之后，会根据主链相关性选择多个最优父单元，并采用广播的形式发送给其他节点。节点接收到新的交易之后，需要验证交易的合法性，验证成功后放入在本地交易未处理交易池中。
2. 见证交易的生成和广播：根据节点的稳定度采用随机抽签的方式选举见证委员会成员和首领。当节点发现自己成为首领之后，生成交易单元选中其父单元，将这些信息作为提案发送到见证委员会，见证委员会采用基于门限签名的一致性协议达成共识，将交易单元广播到网络并添加到本地链上。
3. 交易确认：根据见证交易单元确定主链，为每一个交易单元分配主链号，主链上最近成为稳定单元的见证交易单元成为一个类似于检查点的稳定点。在这个见证单元之前的交易都会被确认，他们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。

【重点剖析与研究问题紧密相关的几个部分】网络特征、节点参与共识过程、节点自启机制、区块确认机制、区块奖惩机制、……

## 4.2 研究问题

对于无线多跳网络环境下的区块链，通常会随着节点数量的增加共识节点之间的网络通信会增加，节点带宽受限的情况下会导致系统的性能下降。为了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的扩展性会随着节点数量的增加而增加，并且还能降低交易的确认时延，提高交易的处理效率。但是，当节点数量少或者交易流较低时，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多跳网络的DAG区块链共识算法。

1. 带宽：原因？【由于无线通信协议MAC（例如CSMA/CA）的限制，导致区块传输受限，影响最终一致性的达成】方案？【保持无线通讯协议，使用类PoS的共识算法（打包区块不消耗算力），通过减少区块的大小，提到区块传输的成功率；】
2. 节点动态性：原因？【节点可移动，随时出入区块链系统，见证委员会成员突然消失离开系统，最终无法达成共识】方案？【将节点的稳定度作为委员会选举的依据，最终选定的委员会成员不会出现大批量突然离线的情况；】

## 4.3 研究方案

DAG区块链由于允许分叉，因此需要主链机制来为交易分配一个主链序，从而防止交易双花。此外还需要一个交易确认机制使得交易能够在交易流小的情况下也能够最终被确认。

### （1）定义稳定度

区块链系统中，新节点进入网络之后，需要质押金钱来获得在这个区块链系统中活动的时间，根据活动时间的长短来选择质押金额的多少【租约时长可以通过租约机制+时间戳实现;或者可以根据权益的大小确定节点的活跃度（节点的活跃度也极大的表明节点是否愿意继续在系统中工作）；】

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【可以多次实验分析计算】。在区块链系统运行初期，确认区块数量不足个时节点的共识比记为零，此时主要通过节点的剩余时间来挖矿。

### （2）共识算法

共识算法每个节点都拥有自己的稳定度，根据节点的稳定度随机选举委员会。共识算法分为以下几个部分：委员会成员和首领选举、委员会对新区块达成一致、区块上链、委员会重置。委员会选举机制采用稳定度作为委员会成员的选举度量，采用随机抽签中将上一个区块的高度和最终签名的哈希作为随机种子，采用可验证随机函数选出新的出块者，其他节点可以验证该节点的合法性。

1. 委员会的随机选举：采用随机抽签的方式选择委员会成员和首领。随机抽签中将上一个见证单元的哈希和最终签名的哈希作为随机种子，采用可验证随机函数选出委员会成员，其他节点可以验证各个成员的合法性。
2. 随机抽签算法：

记是节点的稳定度，所有节点的稳定度之和记为，那么节点被选中的概率为且服从二项分布。为了确定被选中的节点，将区间分为连续的多个区间

.

利用随机可验证函数可计算得到一个值和证明

若，选择前个节点成为委员会成员。

1. 可验证抽签结果

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

如果为，则验证成功，如果为则委员会成员权限的 合法性将会受到质疑。

1. 首领节点的选举：每个委员会将有一个任期，每个任期又分为多个轮。吗，每一轮都会执行一次一致性协议。每轮开始都需要选择一个首领生成区块，并作为提案让委员会内部达成一致。委员会中节点的数量相对较少，为了降低共识时延，可以选择相互之间通信较少的节点作为首领，降低网络资源消耗的同时提高共识的效率。

【方案一】通过路由算法我们可以获得委员会内成员到其他成员的跳数，最终选择平均跳数最少，且稳定度最高的节点作为首领。记委员会成员数量为，则委员会成员到其他成员跳数的矩阵记为

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】由于在无线网络通信中，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。

【方案三】采用随机抽签的方式，将上一个见证交易单元作为随机种子选取出新一轮的首领，这样的方式具有更好的敌手干扰抗性。

1. 一致性协议：
2. 密钥分割：首领生成见证交易单元和选中最好的父交易单元，随后将该交易单元和其父交易单元信息的的密钥进行分割广播给委员会的成员。
3. 委员会成员签名收集：委员会成员收到见证交易单元之后验证该单元和其它签名份额的合法性，并附上自己的签名（如果份额数量没达到阈值）。
4. 签名组合：当见证交易单元的签名数量达到阈值之后，可以得到一个最终的签名，此时委员会成员对于见证交易单元的合法性达成一致。将见证单元链接到自己的本地链上，并广播给其他非委员会成员。
5. 见证单元上链：接收到委员会发来见证交易单元的节点，验证区块和签名的合法性后接受该区块，并且链接到其本地链上。
6. 见证委员会重置：新的任期需要重置更换部分见证委员会成员，分析更换多少数量的成员可以保证委员会的安全。
7. 委员会容错率：采用门限签名机制的委员会的容错率与门限阈值的设计有关，通常可以容错率不超过50%。
8. 委员会更换：委员会中稳定度较低的节点将会被更换，更换数量不得超过委员会成员的一半。为了更好的确保系统的安全性，我们每次可以只更换最多⌋成员。依然采用随机抽签的方式选举出新的委员会成员替换旧的委员会成员。
9. 主链机制：主链可以采用见证委员会交易来确定。当见证委员会的交易成为稳定点之后，会有一个从创世交易单元延伸到尖端单元的主链。这条主链中稳定点之前的主链是完全相同的。因此可以根据这条主链为相关的交易单元分配主链号，者意味着可以给交易提供一个全序，对于双花交易也必然存在一个序，因此可以安全地拒绝后出现的交易，避免了交易双花的问题。

### （3）奖惩机制

1. 奖励机制：每个交易的奖励会分发给的最小主链号子交易和最小主链号后代见证交易的见证委员会成员。
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。

## 4.4 仿真实验

通过仿真实验验证共识算法的性能：吞吐量和确认延时。

吞吐量：单位时间内处理交易的数量；

区块确认延时：区块确认的平均时延。

仿真实验中需要考虑网络带宽，网络通信协议、环境噪声、信号传输功率、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：网络大小、信号干扰噪声比参数、节点密度、交易生成速率等。

# 接下来主要的工作

## 5.1 节点自启机制

无线移动自组织网络能够利用节点的路由转发功能，在无基础设施的情况下进行通信，从而弥补了无网络通信基础设施可使用的缺陷。

无线移动自组织网络的网络拓扑结构是动态变化的。在移动自组织网络中，由于节点随时开机和关机、无线发信装置发送功率变化、无线信道之间的相互干扰以及地形等因素的影响，节点之间通过无线信道形成的网络拓扑结构随时变化且变化方式和速度都不可预测。

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。由于无线多跳网络中移动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。

在考虑无线自组织网络上的区块链系统时，需要考虑信号干扰噪声模型： SINR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。标准信号干扰噪声比模型为

其中 是节点从节点处接收信号功率，而 是均匀信号发射功率；在节点处的干扰为，其中是在当前轮中传输的节点的集合。记环境噪声为，路径损耗指数为，阈值取决于硬件。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. 节点获得邻居列表：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。为了同步到最新的区块链，可以选择比对多个邻居节点的区块链数据。节点将请求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。通过比对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

1. 给出稳定度的定义，给出节点计算稳定度的函数。

区块链系统中，新节点进入网络之后，需要质押金钱来获得在这个区块链系统中活动的时间，根据活动时间的长短来选择质押金额的多少【租约时长可以通过租约机制+时间戳实现;或者可以根据权益的大小确定节点的活跃度（节点的活跃度也极大的表明节点是否愿意继续在系统中工作）；根据节点的生存周期和共识比值来决定节点的稳定度（通常节点的生存周期都比较短）】

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【分析稳定度函数中变量的权重系数，可以多次实验分析计算】。在区块链系统运行初期，确认区块数量不足个时节点的共识比记为零，此时主要通过节点的剩余时间来挖矿。

1. 给出一个过滤函数避免节点由于稳定度过高长期获得出块者权限。

当节点的共识比率达到某一个阈值之后，需要进行限制，这个节点将在一定时间内不能被选中成为出块节点。

## 5.3 门限签名机制的原理

区块确认可以采用门限签名，避免节点之间二次通信。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，其中一个选择两个大素数,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。

对于出块节点的选择或者委员会首领的选择可以采用可验证随机函数，通过添加一个随机扰动来确保选举过程的安全性。

1. 随机抽签算法：

记是节点的稳定度，所有节点的稳定度之和记为，那么节点被选中的概率为且服从二项分布。为了确定被选中的节点，将区间分为连续的多个区间

.

利用随机可验证函数可计算得到一个值和证明

若在某个区间之内，则该区间的所属节点作为被选中的出块节点。

1. 可验证抽签结果

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

如果为，则验证成功，如果为则出块节点的权限合法性将会受到质疑。