**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。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。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、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连上。

【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；】
2. 节点动态性：原因？【节点可移动，随时出入区块链系统，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；】

## 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。通常这个份额根据前个被确认区块的生成节点数量来决定的，并将节点对应的密钥份额发送给这些节点。出块节点随后广播区块到网络，并且收集这些拥有密钥份额节点的签名份额。
2. 区块确认：其他节点接收区块之后，会验证区块和出块者的合法性。在组合所有签名份额之前，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。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、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连上。

【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网络延时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；】

## 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

设计伪代码，并对每个功能模块进项详细的设计分析。基于委员会的共识算法主要包括委员会成员选举、一致性协议、委员会重置。

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，则该节点作为被选中的委员会成员。

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：每个委员会将由一个任期，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，并将区块的密钥惊醒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。

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】

【简单描述区块生成过程】

【重点剖析与研究问题紧密相关的几个部分】

## 3.2 研究问题

对于大型无线多跳网络，由于巨大的通信开销和交易的多样性，采用单一委员会的机制完全无法满足性能的需求。为了提高交易处理效率，降低区块确认延时，需要设计一个适用于大型组网的区块链共识算法。

## 3.3 研究方案

由于大规模无线多跳网络通信都非常复杂，需要的通信资源都非常地巨大，因此可以根据节点的特性（位置、功能等），将节点分片降低节点之间的通信能耗。对于分片的无线多跳网络中的共识算法将面临新的问题，需要相应的解决方案。

### （1）定义稳定度

### （2）共识算法

委员会成员选举、一致性协议、委员会重置、跨分片交易处理。

1. 委员会选举根据节点的稳定度、位置、通信跳数等选举出具有较好稳定度的分片委员的成员和这个分片的簇头，每个分片的簇头将会构成一个根委员会。因此，需要确定分片的影响因素，了解聚类算法相关的知识，实验确定各个影响因素的权重系数。
2. 一致性协议中最终共识是根委员会只生成一个最终区块的区块头，随后将区块头发送到其他成员，其他成员则添加自己提案的区块作为区块体中的内容，最终达成一致性结果，并分发到分片中。因此，需要设计相应的数据收集和发送功能函数。
3. 跨分片交易通常需要分片之间通信，为了防止交易死锁，需要采用一个原子交易提交协议确保跨分片交易的处理不会死锁。需要了解防止死锁的原子提交协议的原理。

### （3）奖惩机制

区块奖励和交易费用将会平均分发给委员会成员。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

仿真验证区块链的性能：吞吐量和确认延时。仿真设置参数：节点数量、网络分区设置、带宽大小，区块大小等。

# 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】

【简单描述区块生成过程】

【重点剖析与研究问题紧密相关的几个部分】

## 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而降低性能，且具有区块链分叉的危险。为了提高区块链的扩展性，加快交易处理效率，采用DAG区块链不经能够允许分叉，随着节点数量的增加还能降低交易的确认时延。

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. 分叉：原因

## 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

### （2）共识算法

共识算法包括见证委员会选举机制、一致性协议、见证委员会重置。

1. 根据节点的稳定度选举出见证委员会成员，随后根据节点的位置、网络延时等作为委员会首领选举的影响因素，给出选举函数，并通过实验得到相应的权重系数。
2. 采用基于可验证随机函数和门限签名一致性协议，需要了解这两种机制的原理，并且根据一致性协议的执行流程设计出相应的功能函数，并给出伪代码。
3. 主链可以采用见证委员会交易来确定。合理的实际主链机制，给出相应的主链号。给出主链的选择原则，并一一讨论。

### （3）奖惩机制

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。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

仿真验证区块链的性能：吞吐量和确认延时。如果可以的话，还可以测试不同交易流下的吞吐量和确认延时。分析交易生成速率对于交易吞吐量、交易确认时延的影响。考虑在CSMA/CA作为MAC协议时的情况。

# 接下来主要的工作

## 5.1 节点自启机制

考虑获取多个节点区块信息，通过比对选择具有公共前缀的最长链。分别分析单跳邻居、两跳邻居的效率和区块链信息。

## 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。
2. 分析稳定度函数中变量的权重系数。
3. 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。

## 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。对于门限签名机制需要了解，并且看能否进习性改进使得这个机制具有动态自适应的功能，可以很好的用于我们的场景中。

## 5.4 可验证随机函数的原理

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来添加一个随机扰动。需要深入了解该机制的原理，随后根据需要做改进，使得适用于共识算法中。