**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、……

【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、区块入链、区块确认、……

【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经常离开的网络的无线多跳网络环境中。但是现在很多无线网络环境中也需要应用区块链技术，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

### （2）共识算法

对于共识算法设计出初始的伪代码，尤其是其中的需要包含的功能函数，随后细化实现这些功能函数。共识算法分为两个部分：出块节点的选择和区块的确认。

1. 出块节点的选择：确定节点的稳定度定义，分析影响稳定度的因素，并通过实验确定每个因素合适的权重系数。
2. 区块确认：了解门限签名的原理，并且分析门限值如何设计可以确保区块确认的安全性，分析影响区块确认时延的主要因素。

### （3）奖惩机制

区块的奖励和交易费用分发给出块者和确认区块的成员，确保系统的活性和安全性。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。仿真实验中需要清楚参数的设计，即网络带宽，网络通信协议，网络传输效率等。对于节点自启机制，可以测试选择多个方向邻居节点获得的区块链信息的情况。

# 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】

【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】

## 2.2 研究问题

在无线多跳网络环境中，单节点共识算法共识过程缓慢，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无线多跳网络中的委员会共识算法。

## 2.3 研究方案

### （1）定义稳定度

### （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以及一些其他的影响因素作为委员会成员的选举度量，根据这些变量对于这个过程的影响大小，通过实验分析确定每个因素的权重系数，最终确定选举函数。
2. 一致性协议作为共识算法中重要部分，需要根据流程图详细设计各个功能函数。
3. 委员会重置需要一个重置函数更换部分成员，需要分析更换多少数量的成员可以保证委员会中诚实成员的到达一定比例。
4. 深入了解随机可验证函数与门限签名机制的原理。

### （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。

## 2.4 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；节点数量、带宽大小、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。