一种无线网络中的稳定区块链共识协议

1. 问题

当前互联网中的区块链共识算法通常具有能耗高、依赖代币和可靠通信等特点；而在无线网络中的区块链节点通常（计算、存储等）资源有限，且具有移动性和网络拓扑不可预测等特征，特别地，节点突然离开网络会影响区块链共识过程。因此，无线网络中的区块链共识算法需要确保共识过程稳定且能耗低。

在这里，我们设计一种用于无线网络（网络模型详见“2.网络模型”）的稳定区块链共识协议。在协议中我们计算节点的稳定度（稳定度的定义见“3.共识过程”），将稳定度作为选择出块节点的依据，确保选出的节点稳定和可信，在短期内不会因为离开系统而影响共识过程，最终保证所有节点能够快速、安全地对新区块达成一致。

2. 网络模型

共识协议是运行于节点随机分布的全连接无线网络，网络中任意两个节点都在彼此的通信范围之内。假设：

- 每个节点配有半双工收发器，可以发送或接收消息，或感知信道，但不能同时发送和接收或发送和感知；每个节点拥有唯一的ID，并且知道其他节点的身份和公钥。
- 系统是开放的，任意节点都不需要事先的身份授权就加入系统；节点可以在网络区域中随意移动，可以随意进入和离开网络。此外，每个节点在一个网络中的活动时间是有限的。

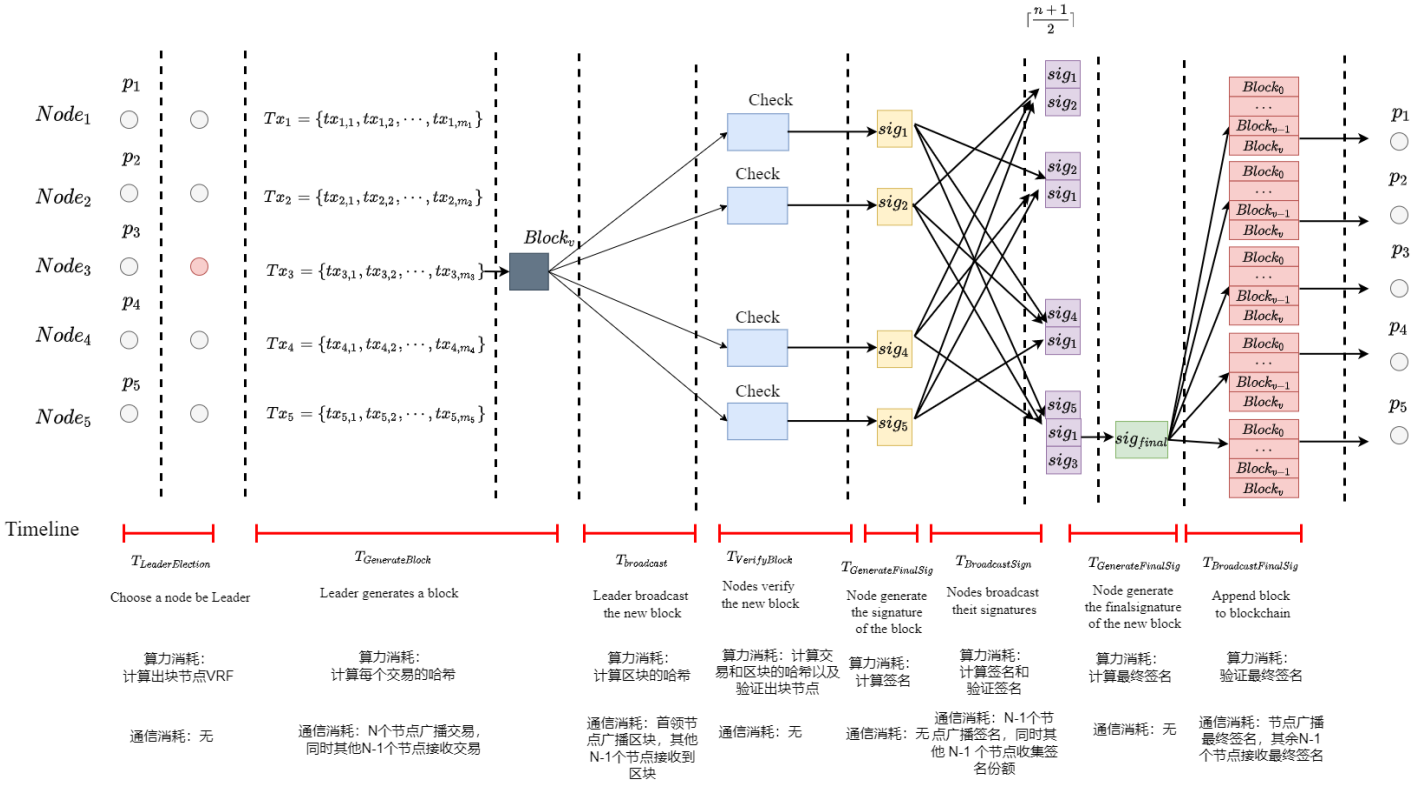
3. 共识过程

共识协议的共识过程是由四个阶段组成：出块节点选举阶段、区块生成阶段、区块验证阶段和链更新阶段，具体如下：

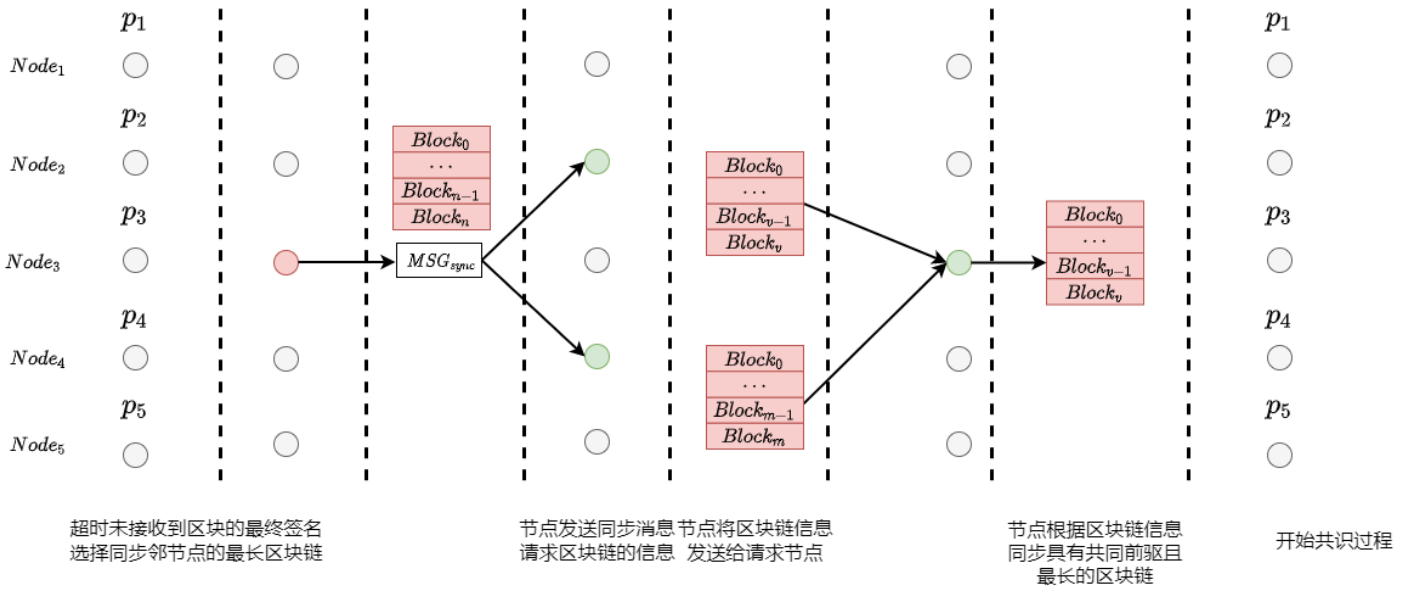
- **出块节点选举阶段：** 网络中有一个节点被选举为出块节点；
- **区块生成阶段：** 被选中的出块节点将近期的交易打包，创建一个新区块，随后广播该区块；
- **区块验证阶段：** 节点接收到新区块之后，验证出块节点的合法性和区块的有效性。一旦出块节点的合法性和区块的有效性都得到确认后，节点对区块进行签名并广播签名。其他节点收集并验证收到签名。

- **链更新阶段：** 当节点接收到的有效签名数量超过某个阈值时，组合形成最终签名，确认区块并将区块添加到本地链上，同时广播最终签名。其他节点接收到最终签名后，将区块添加到本地区块链上。至此，所有节点对新区块达成共识，开始新一轮的共识过程。

区块链共识过程如下图所示，图中符号详见下文“稳定度”部分。



在开始一轮的共识之前，所有的节点需要同步一下最新的区块链，尽量减少节点维护区块链不一致的情况。每个节点会选择同步邻节点的最新区块链。节点的同步过程如下：



稳定度

在稳定区块链共识协议中，主要根据节点的稳定度来选举出块节点。新节点加入系统时，通过保证金质押获得有限的活动时间，活动的时长与交付的保证金成正比。

假设节点 Node_v 在区块链系统中的剩余活动时间为 T_v，则所有共识节点的剩余活动时间之和为 $\sum_v T_v$。定义节点 Node_v 的 **剩余活动时间比值** 为

$$\rho_v = \frac{T_v}{\sum_v T_v}$$

假设在最近的 K 个确认区块中，由节点 Node_v 生成的区块数量为 N_v。定义节点 Node_v 的 **共识比值** 为

$$r_v = \frac{N_v}{K}$$

定义节点 Node_v 的 **稳定度** 为

$$S_v = \alpha \times \rho_v + \beta \times r_v \qquad (\alpha + \beta = 1,\ \alpha \geq 0,\ \beta \geq 0)$$

其中，α 为剩余活动时间比权重系数，β 为共识比权重系数，可根据偏好设置。在系统运行初期，当确认区块数量不足 K 个时，记节点的共识比为 $r_v = 0$。此时，节点的稳定度主要受节点的剩余活动时间的影响。

在稳定区块链共识协议中，节点 Node_v 被选为出块节点的概率为

$$p_v = \frac{S_v}{\sum_v S_v}$$

根据节点的稳定度决定节点被选中的概率，稳定度越高的节点越容易被选中。为了尽可能使系统中节点维护相同的区块链，在每次同时开始之前，节点会执行一次区块链同步操作。节点会随机请求几个邻节点的区块链信息，最终同步拥有共同链前驱且有最长有效区块链。

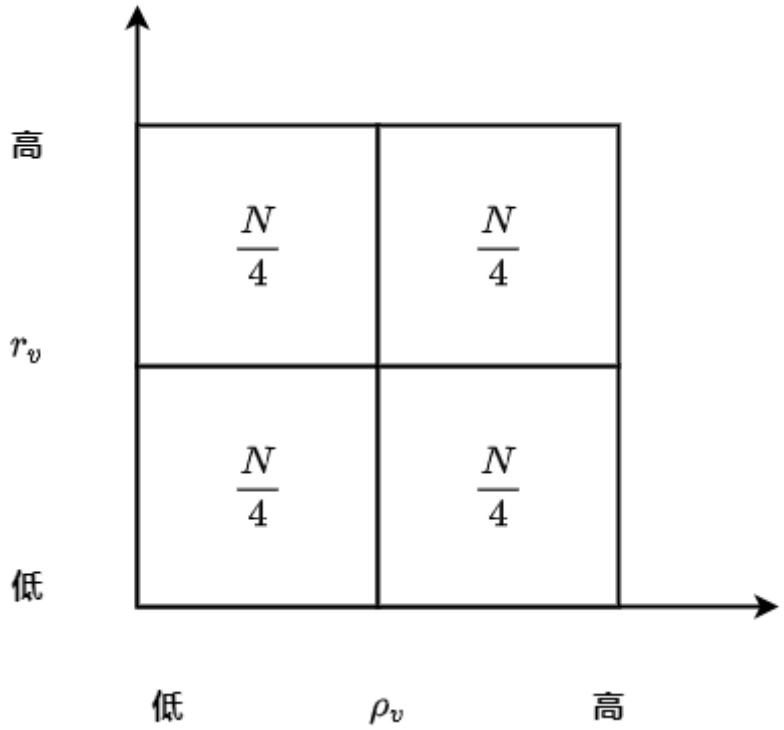
4. 测试

4.1 权重系数影响分析

根据定义，节点稳定度的主要因素是节点活动时间比和共识比，以及它们的权重系数。稳定区块链共识协议的思想是，出块节点应该尽可能是稳定和可信的，确保能够生成有效区块，并在完成区块确认之前不会出现故障。因此，选择一个优质的节点作为出块节点是非常重要的。为了确定权重系数，需要对不同的权重系数做多次对比实验。

实验场景设置：

- 在无线区块链网络中，有 $\frac{1}{4}$ 节点具有较大的活动时间占比和较小共识比，$\frac{1}{4}$ 节点具有较小的活动时间占比和较大共识比，$\frac{1}{4}$ 节点具有较小的活动时间占比和较小共识比，$\frac{1}{4}$ 节点具有较大的活动时间占比和较大共识比；
- 每轮共识结束之后都需要更换出块节点。



对于权重系数 α, β 的实验我们分别测试了以下几种情况进行实验：我们通过多次共识中，测试不同权重系数时优质节点（活动时间占比高且共识比高）被选中的次数来确定比较合理的权重系数。

- $\alpha = 1, \beta = 0$（只考虑活动时间比时，优质节点被选中的次数）
- $\alpha = 0.9, \beta = 0.1$
- $\alpha = 0.8, \beta = 0.2$
- $\alpha = 0.7, \beta = 0.3$
- $\alpha = 0.6, \beta = 0.4$
- $\alpha = 0.5, \beta = 0.5$
- $\alpha = 0.4, \beta = 0.6$
- $\alpha = 0.3, \beta = 0.7$
- $\alpha = 0.2, \beta = 0.8$
- $\alpha = 0.1, \beta = 0.9$
- $\alpha = 0, \beta = 1$（只考虑共识比时，优质节点被选中的次数）

4.2 协议性能

共识协议性能的主要度量指标共识时延和交易吞吐量。我们主要测量不同情况下两个指标的变化情况来分析协议的性能。此外，我们还测试女巫攻击时两个指标的情况来分析其对性能的影响。

(1) 时延测试

测试不同节点数量下区块的确认时间。为了方便对照，需要对条件和变量进行控制。

- 每个区块设置相同的大小；
- 每个节点除了稳定度的指标不同，其他指标都相同。

通过实验测试在不同节点数量时的共识的时延，并将多次实验的结果取平均值。测量不同网络节点数量时时延的变化趋势分析协议的性能：

- 网络大小 $N = 100$
- 网络大小 $N = 200$
- 网络大小 $N = 300$
- 网络大小 $N = 400$
- 网络大小 $N = 500$

(2) 吞吐量测试

测试不同节点数量下交易处理的效率，对条件和变量进行控制。

- 每个区块设置相同的大小，区块中交易的数量也相同；
- 每个节点除了稳定度的指标不同，其他都相同；
- 不考虑生成空区块的情形。

实验测试在不同节点数量时的共识的时延和交易数量，计算得到交易吞吐量，并将多次实验的结果取平均值。通过分析不同网络大小时交易吞吐量的变化趋势分析性能。

- 网络大小 $N = 100$
- 网络大小 $N = 200$
- 网络大小 $N = 300$
- 网络大小 $N = 400$
- 网络大小 $N = 500$

(3) 女巫攻击

测试节点发起女巫攻击时，共识时延和交易吞吐量的变化情况。测试节点数量固定时，不同数量的女巫节点对于协议性能指标共识时延和交易吞吐量的情况，进一步分析女巫攻击对系统性能的影响。

- 女巫节点占比 10%

- 女巫节点占比 20%
- 女巫节点占比 30%
- 女巫节点占比 40%
- 女巫节点占比 50%

5. 现存问题

- 关用户购买活动时间应该如何定价比较合理?
- 区块奖励给多少比较合理?
- 用户购买活动时间的钱通常应该怎么处理?