共识过程

背景

考虑在无线网络中实现区块链

网络模型

我们考虑是一个由 N 个全连接的随机分布在一个二维地理平面的节点构成的无线网络，即网络中任意两个节点在彼此的通信范围之内。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。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。记 d_{ij} 是节点 i,j 之间的欧式距离，而 $D_i(R)$ 是以节点 i 为圆心 R 为通信半径的圆形区域，$N_i(R)$ 表示在节点 i 的通信范围中的所有节点。我们假设每个节点拥有唯一的ID，并且知道所有其他节点的身份和公钥。每个节点的传输功率可以被控制以降低干扰对通信的影响。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。此外，我们假设每个节点在一个区域中的活动时间是有限的。

目的

在无线网络中，单出块节点共识算法无法确保所有的节点同时维护相同的区块链。出块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、节点具有高动态性的无线网络环境中，因此需要设计一个适用于无线网络环境的区块链共识算法。

无线网络拓扑变化大且不可预测，节点可能会突然离开系统影响共识过程。将节点的稳定度作为首领选举的依据，选举出比较稳定的节点作为出块节点，确保选举的首领节点稳定性高，短期内不会离开系统，所有节点能够快速、安全地对新区块达成一致。

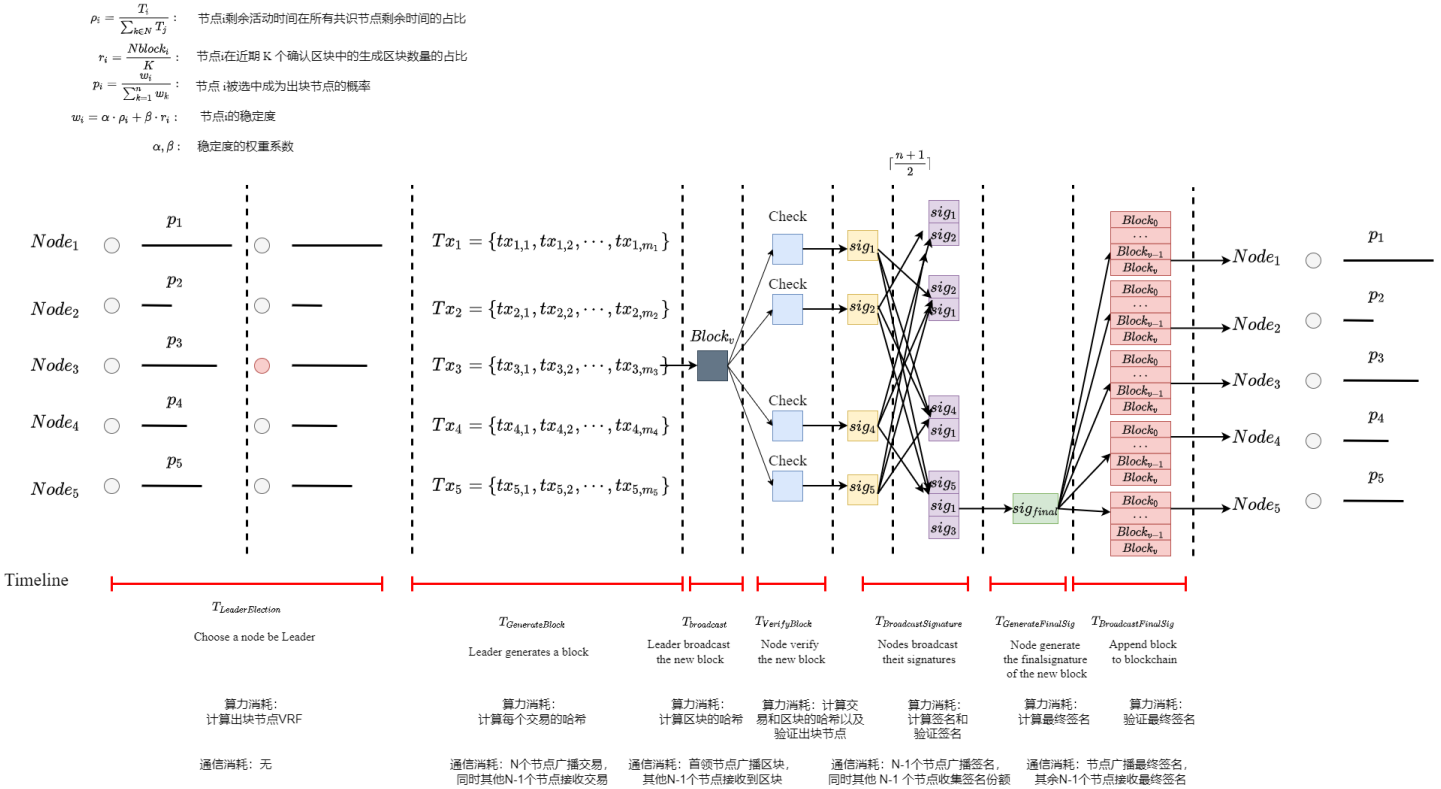
共识过程

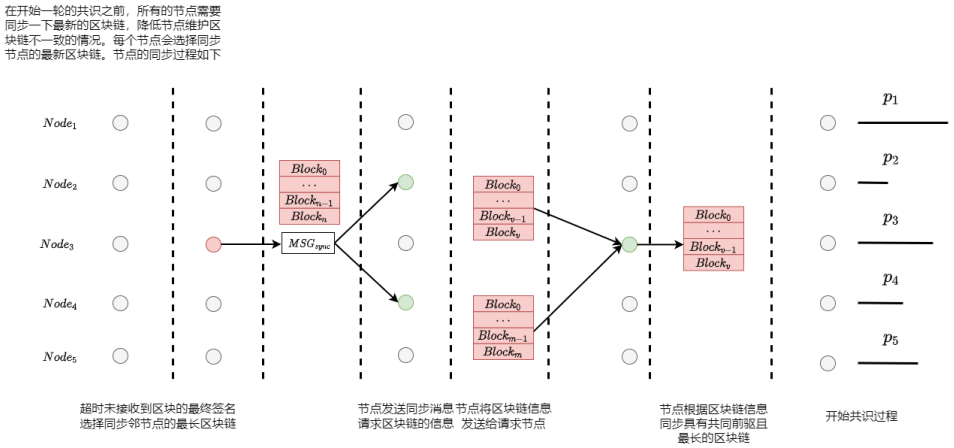
我们设计的共识协议的共识过程是由四个阶段组成：出块节点选举阶段、区块生成阶段、区块验证阶段和链更新节点，具体如下：

- 出块节点选举阶段：在这个阶段有一个共识节点将被选举为出块节点；
- 区块生成阶段：被选中的出块节点将会将近期的交易打包并创建一个新区块。随后，该区块会被广播给所有共识节点；
- 区块验证阶段：接收到新区块之后，节点会验证出块节点和区块的有效性。一旦新区块被确认有效，节点会广播签名给所有共识节点，其他共识节点会收集并验证接收的签名。

- 链更新阶段：当节点接收到有效签名数量超过阈值形成最终签名时确认区块，将区块添加到本地链上并广播最终签名给其他共识节点。其他节点接收到最终签名后，也会将区块添加到本地区块链上。至此，所有共识节点对新区块达成共识，开始新一轮的共识过程。

区块链共识具体过程可见下图：





在稳定区块链协议中，主要是根据节点的稳定度来随机选举出块节点。新节点加入系统要质押金钱获得有限的活动时间。活动的时长与交付的押金成正比。记 T_v 为无线网络节点 v 在区块链系统中的活跃时间，所有共识节点的剩余活动时间之和为 $\sum_{i\in N} T_i$，定义节点的活动时间比为 $\rho_v = \frac{T_v}{\sum_{i\in N} T_i}$。记 $r_v = \frac{N_v}{K}$ 为节点在最近 K 个确认区块中参与共识比值，其中，N_v 是节点 v 生成区块的数量。定义无线网络节点 v 的稳定度为

$$S_v = \alpha \times \rho_v + \beta \times r_v$$

其中，权重系数 α, β 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 K 个时记节点的共识比 $r_v = 0$，此时节点的稳定度主要受节点的活动时间的影响。协议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。

测试指标

稳定度

影响稳定度主要因素有：节点活动时间比和共识比。这两者会对所选节点的稳定度产生影响，但是所占的权重还不能确定。节点的剩余活动时间会逐渐减少，如果节点的活动时间不曾延长，选举剩余活动时间比小的节点可能会导致生成空区块，降低交易处理的效率。出块节点的选举算法的思想，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。所以需要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：区块链网络中有 N 个节点，其中 $\frac{N}{4}$ 个节点具有较大的活动时间占比和较小共识比；$\frac{N}{4}$ 个节点具有较小的活动时间占比和较大共识比；$\frac{N}{4}$ 个节点具有较小的活动时间占比和较小共识比；$\frac{N}{4}$ 个节点具有较大的活动时间占比和较大共识比。每个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：

- $\alpha = 1, \beta = 0$:
- $\alpha = 0, \beta = 1$:
- $\alpha = 0.5, \beta = 0.5$:
- $\alpha = 0.9, \beta = 0.1$:
- $\alpha = 0.1, \beta = 0.9$:

我们通过多次共识中，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。

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。

时延测试

测试不同场景（节点数量、节点密度）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，其他都相同；

通过实验测试在不同节点数量和节点密度时的共识的时延，并将多次实验的结果取平均值。

对于共识时延，我们测量不同网络节点数量时的情况：

- 网络大小 $N = 100$
- 网络大小 $N = 200$
- 网络大小 $N = 400$
- 网络大小 $N = 600$
- 网络大小 $N = 800$
- 网络大小 $N = 1000$

测试不同节点密度时的共识时延：

- 节点密度 $density = 0.2$：
- 节点密度 $density = 0.5$：
- 节点密度 $density = 0.1$：
- 节点密度 $density = 0.15$：
- 节点密度 $density = 2$：

吞吐量测试

测试不同场景（节点数量、节点密度）下交易处理的效率。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，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

通过实验测试在不同节点数量和节点密度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。

对于交易吞吐量，我们测量不同网络节点数量时的情况：

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

- 网络大小 $N = 600$
- 网络大小 $N = 800$
- 网络大小 $N = 1000$

测试不同节点密度时的交易吞吐量：

- 节点密度 $density = 0.2$：
- 节点密度 $density = 0.5$：
- 节点密度 $density = 0.1$：
- 节点密度 $density = 0.1.5$：
- 节点密度 $density = 2$：

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%:

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?