

考虑节点重要性的区块链共识框架与方法



王鑫，湖南大学

✉ wangxin01@hnu.edu.cn

简介

针对区块链共识算法普遍存在的资源消耗大、共识效率低、节点属性易被忽略的问题，本研究提出了一种考虑节点重要性的区块链共识框架与共识方法。首先在区块链网络中，构建包括节点度中心、接近中心、介数中心、网络位置和忠诚度等指标在内的多维评价体系，提出一种区块链节点重要性计算方法。之后，根据节点重要性按规则抽取部分节点作为共识节点，并按照投票原则选举出当期主节点负责数据的接收、排序和区块生成，而其他非主节点的共识节点则拥有对区块有效性的投票权。最后，对有效性验证通过的区块进行分发和二次验证，完成上链过程。本研究提出的方法能够在一定程度上解决共识算法高能耗、效率低的问题，对节点属性的考虑也能够激励区块链网络中的非活跃节点，有助于维护区块链网络稳定和良性发展。

研究方法

1. 节点重要性的计算

- 选择节点度中心 DC_i 、接近中心 CC_i 、介数中心 BC_i 、网络位置 NL_i 和忠诚度 RL_i 等指标构建节点重要性评价体系。
- 定义特征向量 $Q_i=[q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}]=[DC_i, CC_i, BC_i, NL_i, RL_i]$ ，且定义节点 v_i 的重要性评价向量 S_i 为 Q_i 的加权，即 $S_i=[s_{i1}, s_{i2}, s_{i3}, s_{i4}, s_{i5}]$ ， $s_{ij} = \frac{q_{ij}}{\max\{q_{ij}\}}$ ， $i \in [1, N]$ ， $j \in [1, 5]$ 。
- 定义区块链网络中最重要虚拟节点 v^{most} 和最不重要虚拟节点 v^{least} 的重要性评价向量分别为 $S^{most}=[s_1^{most}, s_2^{most}, s_3^{most}, s_4^{most}, s_5^{most}]$ 和 $S^{least}=[s_1^{least}, s_2^{least}, s_3^{least}, s_4^{least}, s_5^{least}]$ ，其中 s_j^{most} 是节点在第 j 个属性上的最优取值， s_j^{least} 是节点在第 j 个属性上的最差取值。
- 定义节点 v_i 到虚拟节点 v^{most} 和 v^{least} 的差异量化公式为 $R_i^{most} = \sum_j^m [s_j^{most} \log \frac{s_{ij}^{most}}{s_j^{most}} + (1 - s_j^{most}) \log \frac{1-s_{ij}^{most}}{1-s_j^{most}}]$ 和 $R_i^{least} = \sum_j^m [s_j^{least} \log \frac{s_{ij}^{least}}{s_j^{least}} + (1 - s_j^{least}) \log \frac{1-s_{ij}^{least}}{1-s_j^{least}}]$ 。由于 $f(x)=\log x$ 为凸函数，因此存在不等式 $-R_i^{most} = \sum_j^m [s_j^{most} \log \frac{s_{ij}^{most}}{s_j^{most}} + (1 - s_j^{most}) \log \frac{1-s_{ij}^{most}}{1-s_j^{most}}] \leq \sum_j^m \{\log[(s_j^{most} \times \frac{s_{ij}}{s_j^{most}}) + (1 - s_j^{most}) \times \frac{1-s_{ij}}{1-s_j^{most}}]\} = \sum_j^m \log 1 = 0$ 。由此可得， $R_i^{most} \geq 0$ ，当且仅当 $\frac{s_{ij}}{s_j^{most}} = \frac{1-s_{ij}}{1-s_j^{most}}$ ，即 $s_{ij} = s_j^{most}$ 时， $R_i^{most} = 0$ 。同理可得， $R_i^{least} \geq 0$ ，当且仅当 $s_{ij} = s_j^{least}$ 时， $R_i^{least} = 0$ 。
- 以虚拟节点 v^{most} 和 v^{least} 作为区块链网络中的参考点，定义节点 v_i 的重要性计算公式为 $I_i^{most} = \frac{R_i^{most}}{R_i^{most} + R_i^{least}}$ 。

2. key值的计算

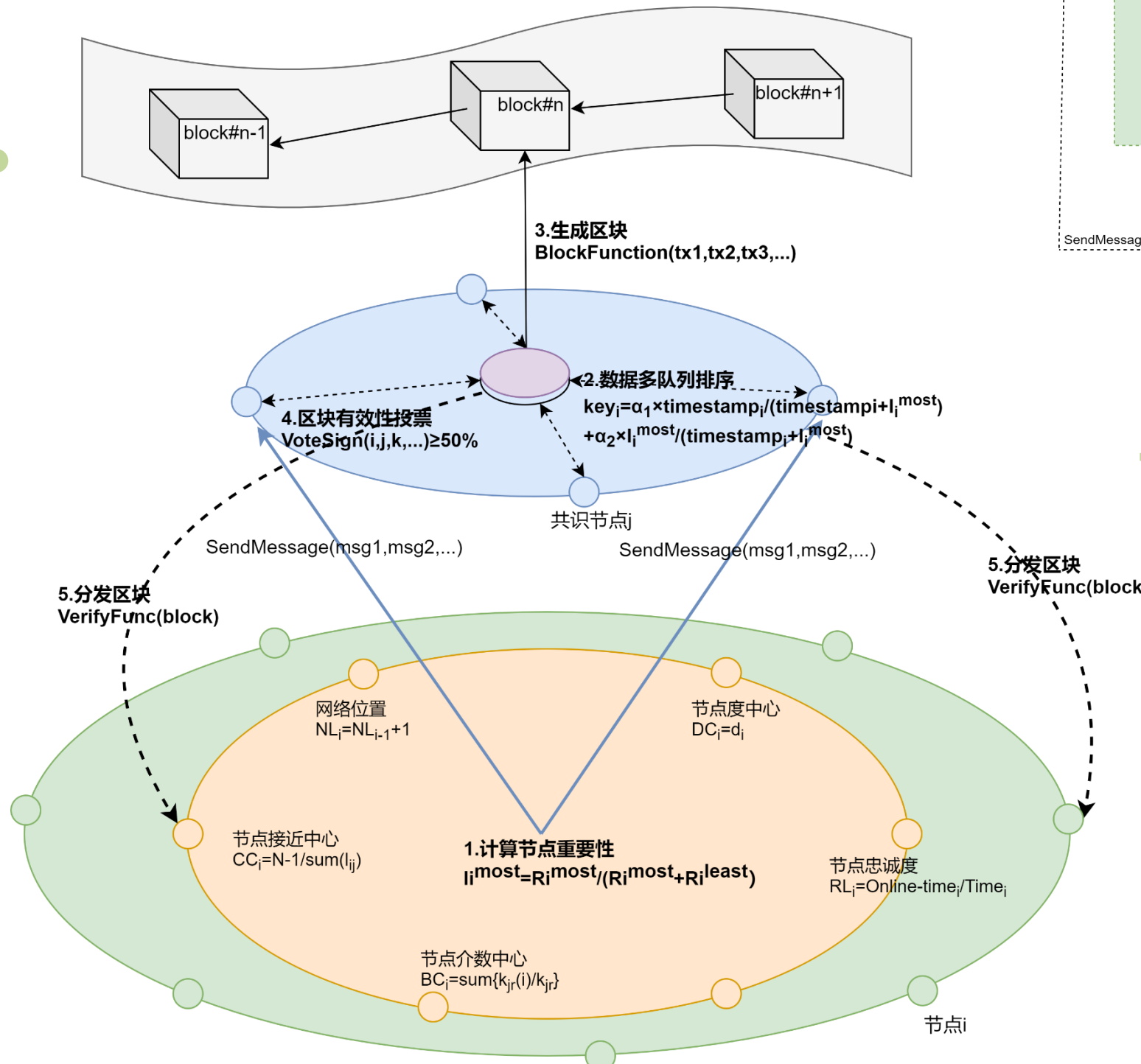
- key值由主节点对接收到的数据进行唯一性赋值，主要用于主节点对数据的多队列排序。
- 定义 $key = \alpha_1 \times \frac{\text{Timestamp}_i}{\text{Timestamp}_i + I_i^{most}} + \alpha_2 \times \frac{I_i^{most}}{\text{Timestamp}_i + I_i^{most}}$ ， $\alpha_1, \alpha_2 \in (0, 1)$ 且 $\alpha_1 + \alpha_2 = 1$ 。

3. 主节点对数据进行多队列排序

- 主节点获取一定时间范围内的数据后，按每笔数据的key值进行多队列排序。
- 排序队列是指主节点服务器划分出的多个独立计算空间，用以快速实现数据一致性。

研究结果

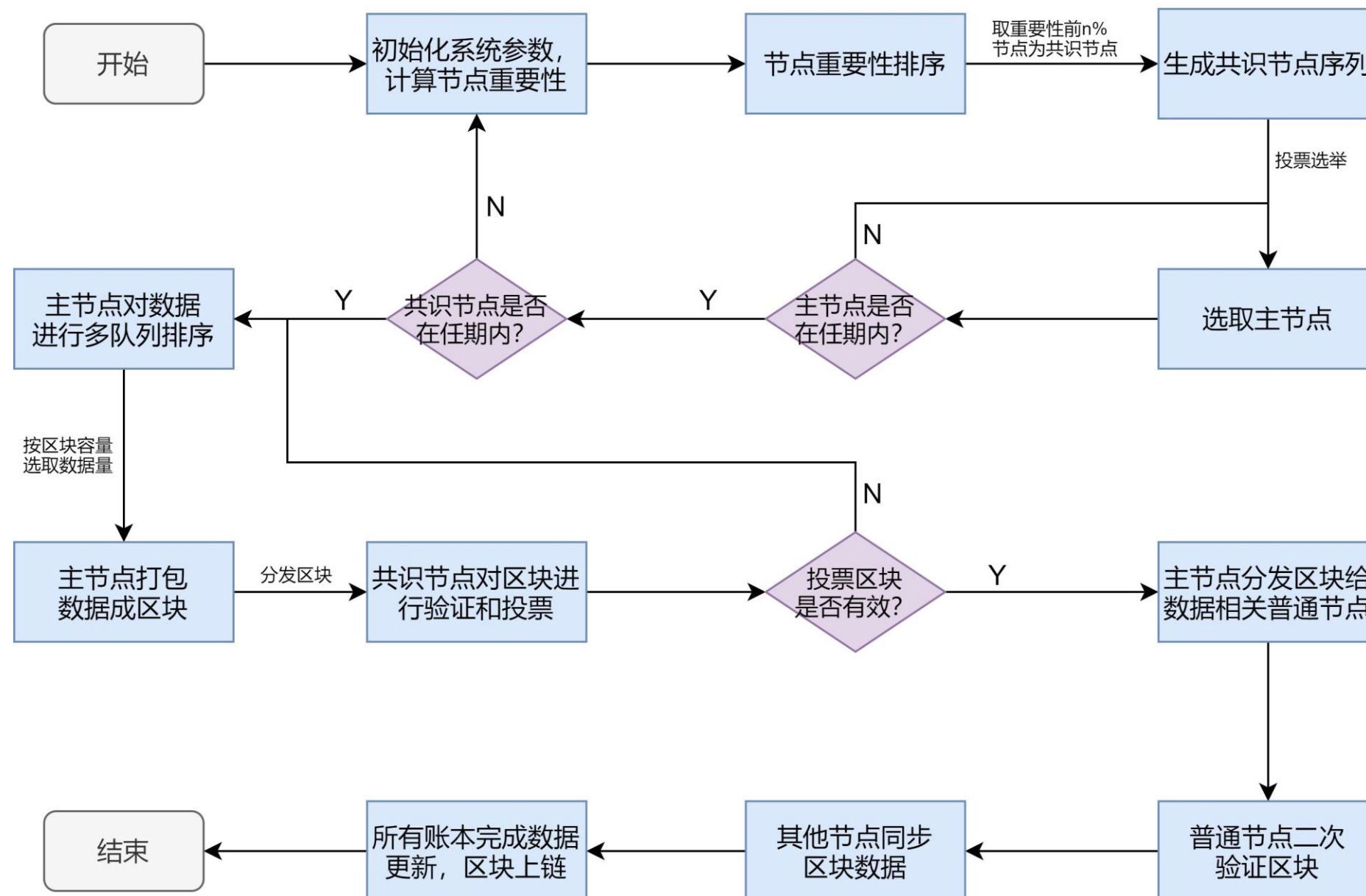
本研究提出了一种考虑区块链节点重要性的共识框架与方法，主要包括四个关键步骤：首先计算区块链网络中的节点重要性，生成重要性排序序列，并按规则从中抽取部分节点作为共识节点。其次，从共识节点中选取主节点，由任期中的主节点对接收到的数据进行多队列排序，打包数据序列生成区块。然后，共识节点对区块内的数据进行模拟交易验证，并对区块有效性发起投票。最后，主节点将投票通过的区块分发给区块内数据相关的节点进行二次验证，若验证通过，则更新本地账本，其他节点再同步区块数据，最终完成区块上链，实现高效的共识过程。



关键问题

本研究的共识方法需要考虑三个关键问题：

- 节点重要性如何计算；
- 主节点如何对数据赋予key值，以及key值如何进行计算；
- 主节点如何根据key值对数据进行多队列排序。



参考文献

- Bouraga S. A taxonomy of blockchain consensus protocols: A survey and classification framework[J]. Expert Systems with Applications, 2021, 168(6): 114-135.
- Leonardos S, Reijnsbergen D, Piliouras G. Presto: A systematic framework for blockchain consensus protocols[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1028-1044.