基于信用分组投票的电网区块链共识算法

**摘 要：**区块链技术通过智能合约的执行和交易数据的安全存储促进了智能电网的进一步发展，但由于用户个体电能产量不确定性及个体趋利性等特点，相较于传统电能交易市场，智能电网的电力交易存在着大量的失信、违约现象，导致用于电网区块链系统中的共识算法共识效率较低、资源浪费较严重等问题，限制了电网电能交易系统进一步发展。针对以上问题，本文首先分析电网能源交易的区块链账户节点属性，设计了基于智能合约的电能交易流程。其次，提出了一种基于信用分组投票的电网区块链共识算法（CGPBFT），通过公平分组、正反向投票等方法的设计，保证了区块链主节点选取的可靠性；通过对实用拜占庭容错算法（PBFT）的一致性协议进行有效优化，在不影响系统容错性能的条件下，降低了一致性处理的消息复杂度。实验结果表明，所提方案能有效减少系统中的拜占庭节点造成的影响，降低通信开销，提高系统的稳定性和安全性。

**关键字：**区块链；共识机制；分组优化；投票机制；PBFT；智能合约；

**0概述**

随着分布式能源技术的发展及国家对能源供给侧改革的不断推进，我国配电系统分布式发电已取得较大进展，为倡导分布式电能就地消纳，国家能源局与发改委出台了《关于开展分布式发电市场化交易试点的通知》，提倡分布式发电项目采取多能互补方式建设，提升供电灵活性和稳定性。在政策和技术的双重推动下，分布式电能的直接交易将成为新趋势[1][2][3]。

和一般商品交易不同，电能交易合约的达成通常发生在交易实际执行前，这使得电能交易存在一定的信用风险，例如交易双方的实际发用电量可能会与协议发用电量不同[4]，导致电网内部出现各种违约问题，引发电网内部交易双方失信，进而不能完成交易[5]。因此，在电能交易系统中，建立一个高效、透明、安全的交易机制成为中国电力体制改革的关键。

以“去中心化”著称的区块链技术，由于其数据公开透明、不可篡改性、智能合约自动执行等优点，与分布式电能交易需求完美契合[6][7][8]，同时，区块链技术对系统内节点的信用管控上也有着不可替代的优势。

区块链技术与电网交易场景的深入融合已经成了一种新的发展趋势[9][10]。文献[4]提出了一种基于区块链的分布式能源交易市场信用风险管理方法，设计了节点信用评估办法并提出了一种共识算法，但该算法的执行仍基于节点的算力，会造成大量资源消耗。文献[11] ]改进了现有分布式安全校核算法并提出了一种弱中心化的交易机制，但该交易机制并没有完全实现去中心化，依然依赖中心机构。文献[12]设计了基于以太坊的去中心化的配网运行机制，采用VCG(Vickrey-Clarke-Groves)拍卖规则鼓励电能生产者理性报价。文献[13]针对能源服务模式构建了综合能源服务模型，并设计了多链节点的选举方式。文献[14]提出了基于区块链的交易数据云存储方案，以确保交易数据的安全存储和共享。文献[15]针对虚拟电厂的功能特性，建立了多虚拟电厂主从博弈优化运行方法，并从网络层架构、激励机制等方面进行了优化。然而，以上的研究主要关注电力交易机制、方法，却对电力交易系统内用户的信用管理及与电网区块链有着深度融合的共识算法有着较少的探讨。

共识机制作为区块链技术重要组成部分，在区块链研究领域中一直是一个热点话题，吸引了大量科研工作者关注[16]。在目前的共识算法中，比较流行的共识算法有PoW[17]、PoS[18]、DPoS[19]，PBFT[20]等。文献[21]设计了基于发电量的权益证明共识机制，但该方案可能会出现因部分节点权益过大导致系统出现中心化问题。适用于电网交易需求的共识机制的研究仍处于初步阶段，仍然是能源区块链研究领域的一个重要的问题。

因此，本文根据电网电力交易过程，设计了电网能源交易区块链账户节点及基于智能合约的电能交易流程，建立了节点信用评估指标最后，提出了一种基于信用分组投票的电网区块链共识算法，实现以信用值、交易电量属性影响共识过程、约束节点行为，提高系统的安全性和稳定性。

# 2.基于智能合约的电网电能交易机制

为了**规避电网电能交易中存在的信用风险，本文设计了一种基于智能合约的电能交易机制**。在交易发起前，双方协商交易细节，并记录在智能合约中。在交易结算阶段，应用智能合约自动执行的特点根据实际交易电量对交易双方进行信用评估，节点主体的信用值将影响节点在系统的行为，进而影响其收益，进而激励节点在交易过程中守信。

在电网交易区块链中，由于信用值及买卖电量对节点评估的重要性，本文将这两种属性作为节点的基本属性。即

（1）

式中，为电网用于节点的属性集合；为电网节点的地址，为电网节点的账户余额；为电网节点的信用值，为电网节点的交易电量总和。节点初次进入系统时，信用值初始化为50，交易电量初始化为0。

**节点信用值更新**条件：

（1）节点在电网系统中的交易结束后，交易双方的智能电表向智能合约提交各自的用电情况。系统根据智能合约完成度对节点的信用值更新。

（2）节点参与投票过程或者共识过程，系统根据实际情况对节点的信用值更新，既没有参与投票过程也没有参与共识过程的节点信用值将会有一定程度的损耗。

2.1基于区块链的电网电能交易流程.

消费者与产消者在电网区块链中可以自由交易，产消者预测下个时间间隙内可产出的电能向区块链网络中广播，消费者接收到产消者发出的电能信息后，根据自身电能需求，可通过线上或者线下的方式与产消者协商，并完成链上电能交易。基于区块链的电网电能交易流程大致分成以下3个阶段。

1)协议达成。在交易开展前,电能交易双方在电网区块链系统外就交易细节(交易时间、交易电能、交易电价及责任划分等)进行协商或在电网区块链中通过广播的方式去寻找交易对象并进行协商。

2)智能合约生成。交易双方针对交易细节协商完成后，双方将交易信息记录在区块链智能合约。

3)交易结算。交易结束后,双方智能电表向智能合约提交各自的电量记录。智能合约根据实际传输电量进行结算,同时对交易双方的信用值进行更新。

基于区块链的电网电能交易方法,电能交易数据进行上链存储就不可篡改,保证了交易的公开透明。利用智能合约执行不受外部条件影响的优势,智能合约完成了电能交易细节的执行及交易结算。电网企业负责电能的传输,因此在交易完成后,会收取一部分费用。当交易中的生产者不能满足消费者需求电量时,电网企业面向消费者售电,其售电价格为电网电价。当消费者实际用电量低于协议电量时,电网企业对剩余的协议电量进行回收,其购电价格低于电网电价。

## 2.2 节点合约信用评估指标

电网系统以电量进行交易,即交易双方通过智能合约签订即将交易的电量、电价、交易期限等信息。在交易过程中,对买卖双方而言,分别存在以下失信情况。

(1)对卖方来说,如果买方信用较差,不按照智能合约记录的交易量用电,若用电量比智能合约中记录的电量要多,则对卖方无影响,相反,若用电量比智能合约中记录的电量要少,则对卖方产生经济损失。

(2)对买方来说,如果卖方信用较差,不按照智能合约记录的交易量发电,若发电量比智能合约中记录的电量要多,则对买方无影响,相反,若发电量比智能合约中记录的电量要少,则对买方产生经济损失。

因此，为了评估电网电能交易系统中参与交易的节点信用，需要评估买卖双方的智能合约执行情况。本文以智能合约完成度作为节点的信用评估指标，反应节点电能交易完成情况。

对于买方，合约信用评估由式（2）确定：

（2）

式中：和 分别为买方本次和上一次的信用值，； 为智能合约规定的电量；为买方在合约规定时间内的实际用电量。

对卖方，合约信用评估由式（3）确定：

（3）

式中：和分别为售电方本次和上一次交易的信用值，；为售电方在合约规定时间内的实际发电量。

# 3 基于信用分组投票的电网区块链共识算法（CGPBFT）

针对传统的实用拜占庭容错算法(PBFT)中执行一致性协议过程通信开销大、主节点选取比较随机等问题，本文提出基于信用投票模型的PBFT共识机制（CGPBFT）。主要包括分组优化，信用投票模型，一致性协议简化，以及节点替换机制。

## 3.1分组优化

考虑电网场景实际需求，系统在分组过程中。从经济效益和可靠性两方面出发，同时兼顾“交易电量”和“信用值”两个分组量化因素。在本方案设计中，分组策略分为“电量均衡”和“信用均衡”两个层次。具体规则如下：

规则1：“电量均衡”指系统执行分组时，满足各分组之间的交易电量之和基本相同。[[1]](#footnote-1)

规则2：“信用均衡”指在满足“电量均衡”的条件下，再对各个组的节点进行调节，使得各组内的信用值总和基本相同。1

## 3.2信用投票机制

信任投票机制可以有效评估每个节点的投票质量，鼓励节点维护系统的安全性。系统内各节点在投票阶段，有赞成票、反对票或弃权三种选择权。各组内节点根据组内节点在系统中的交易历史、信用值、交易电量等属性，有选择性地对其他节点投票。

（1）投票结果统计

节点根据投票策略，投票完成后，系统计算各个节点票数，计算方式为：

（4）

其中，为节点*i*最终的投票结果为节点*i*的信用值，表示节点*i*的赞同票数，表示节点*i*收到的反对票数，可以根据系统的节点数量进行调整，*μ、ω*是常量，且*μ+ω*=1,通常取*μ*=0.5，*ω*=0.5。

通过公式（4）可以看到，对于信用值低的节点，需要获取更多的投票才能成为代理人节点。因此，异常节点成为代理人的概率将会降低。

（2）主节点及代理节点选举

投票结果生成后，系统根据投票规则选出组内代理人节点及系统主节点，同时通过引入备选主节点来增强系统的稳定性。具体投票规则如下：

规则1：对节点的总票数排序，组内票数最高者为组内代理节点。

规则2：代理节点票数最多者为系统主节点。

规则3：节点票数相同时，比较节点历史交易电量，交易电量大者优先成为组内代理节点及系统主节点。

（3）惩罚机制

针对节点可能出现投票消极、随意等行为，引入惩罚机制，即监督节点在共识过程或出块过程的行为，如**出现没有产生区块、产生错误区块、节点宕机**等异常时，对异常节点及组内对该节点投票的节点进行惩罚，降低其信用值。具体如下：

定义,*i*为代理人节点，*j*为对*i*投票的节点，为代理人节点的信用值，为投票节点的信用值，则有：

（5）

其中，*δ<γ，α<β*，即惩罚大于奖励。节点信用值积累难，但易丢失，因此，可通过适当增大β、γ参数值，使异常节点及相关节点的信用值较大幅度降低，促使系统内节点诚实投票，通过每个节点的合法参与，使得整个系统更趋向于稳定性。

## 3.3节点替换机制

为了避免节点在共识过程中可能出现（异常行为）主机故障、带宽时延太高，退出电网系统等情况影响系统正常运行，因此，引入节点替换机制，旨在替换发生故障的共识节点，增强系统的安全性。节点替换机制重点加强对共识节点的监管，通常，节点替换发生在以下情况下：

1. 共识节点被发现失职
2. 节点有恶意行为

当主节点出现以上情况时，备选主节点升级为主节点，重新执行优化一致性协议。当代理节点出现以上情况时，本次共识结束后，该节点所在的组重新执行信用投票机制，选出组内新的代理节点。通过该机制，有效降低拜占庭节点参与共识过程的概率，确保了系统安全。

## 3.4信用损耗

当系统内节点活跃度较低、参与共识的节点数量较少时，区块链中共识效率及安全性就会有所降低。为了确保节点的活跃程度，引入信用损耗，鼓励节点 积极参与投票、共识。节点信用值损耗算法如下：

（6）

式中：为该节点连续未参与投票或共识的次数；为区块链系统设置的惩罚因子。信用损耗机制的引入，提升了节点在系统中的活跃度，确保了区块链系统中有足够的节点参与共识过程,保障了区块链系统的安全性。

## 3.5简化PBFT算法

传统的 PBFT 算法由五个步骤组成。当系统中有 n 个节点时，达成一致所需的消息数大约等于。随着系统中节点数量的增加，达成共识所需的消息数量将以平方顺序增加。消息数量的爆炸性增长将大大延长达成共识所需的时间，从而成为系统性能的瓶颈，并限制系统的规模。

为了解决这个问题，本文简化了传统的 PBFT 算法，如图1所示。节点c为客户端，节点0为主节点，节点1到3为从节点，其中节点1也为备选主节点。



**图1简化的PBFT共识流程图**

简化后的PBFT算法具体执行流程如下：

1）请求阶段

客户端向主节点发送请求信息，消息格式为*<CGREQUEST,o,t,c>*。

2）预准备阶段

主节点收到请求后生成预准备信息，并将该信息广播给参与共识的所有从节点，该预准备信息格式为*<CGPRE-PREPARE,v,n,d，message>*，其中*v*为视图编号，*n*为消息标号，*message*为Client发送的消息，*d*为*message*进行hash运算后的结果。

3）准备阶段

从节点接收到CGPRE-PREPARE消息后，检查该消息的合法性，若验证消息是正确的，且没有被篡改过，则从节点进行签名，并对消息加时间戳，接收并广播准备消息，其消息格式为*<CGPREPARE,v,n,d,i>*，*i*为节点编号。

4）提交阶段

主节点和备选主节点收到共识节点中大于*f*+1个PREPARE消息后，则主节点和备选主节点向其他节点发送提交信息*<CGCOMMIT,v,n,d,i>*。

5）响应阶段

客户端等待来自不同节点的响应信息 *<CGREYLY,v,t,c,i,r>*，若有*f*+1个共识节点的响应相同，则该响应即为算法的一致结果。

执行完优化后的一致性协议，主节点将已经达成共识的数据写入区块链系统；如果主节点没有将数据写入区块链或出现其他异常行为，则系统认定主节点为拜占庭节点，系统根据节点快速剔除机制选出新的主节点继续完成共识过程。

## 3.6 CGPBFT机制执行流程

CGPBFT机制的执行流程如2图所示。CGPBFT机制执行分组优化机制，将系统节点划分为互不相关的组，各个组内根据信用投票机制，选出每个组内的代理节点，进而构成共识节点集合。此后的共识过程均在该共识集合完成,如果共识集合中的节点达成共识,则将这一段时间内的交易信息写入区块链;若没有达成共识,则剔除该交易数据。



图2 CGPBFT机制执行流程

# 4实验与结果分析

## 4.1基于智能合约的电网电能交易测试

为测试本文提出的基于智能合约的电网电能交易机制，本文基于以太坊平台对基于智能合约的电能交易进行仿真。本节设置一个电能生产者，一个消费者及电网企业，根据可能出现的5中交易情况进行仿真测试。其中，交易电价根由双方进行协定并将写入智能合约。交易结束后，区块链系统根据合约完成情况更新双方账户信用值及交易电量。实验假设电网企业售电价为0.62元/（kW·h），电网公司对系统内节点产出的电能收购电价为0.4元/（kW·h）。实验结果如表2所示。

表2 基于智能合约的电网电能交易测试结果

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 编号 | 合约单价/ | 合约电量/ | 过网费/ | 消费者实际用电量/ | 生产者实际发电量/ | 消费者支出/元 | 生产者收入/元 | 电网收入/元 | 累计交易量/ | 当次消费者信用 | 当次生产者信用 |
| 1 | 0.65 | 100 | 0.02 | 100 | 100 | 67 | 65 | 2 | 100 | 100 | 100 |
| 2 | 0.64 | 100 | 0.02 | 120 | 100 | 78.4 | 64 | 14.4 | 200 | 100 | 100 |
| 3 | 0.66 | 100 | 0.02 | 80 | 100 | 54.4 | 60.4 | -6 | 280 | 98 | 100 |
| 4 | 0.65 | 100 | 0.02 | 150 | 150 | 100.5 | 97.5 | 3 | 430 | 100 | 100 |
| 5 | 0.64 | 100 | 0.02 | 80 | 80 | 52.8 | 51.2 | 1.6 | 510 | 98 | 98 |

第一次测试中，电能交易双方都按照交易前达成的协议发用电，双方均无违约失信情况。第二次测试中，买方实际购电量大于卖方的发电量，且卖方根据协议完成发电，交易双方均完成了事前签订的协议，双方都无造成经济损失，双方信用值不受影响。第三次测试中，交易的买方实际购电量小于卖方的发电量，且卖方根据协议完成发电。此时，电网公司根据实验假设的电价进行回收买方剩余电量，由于收购电价较低，对买方造成经济损失，因此，会影响卖方的信用值。第四次测试中，交易双方的发用电量均超出事前达成的协议电量，此时，不影响双方信用值。第五次实验中，交易双方的发用电量均低于实现达成的协议电量，此时，对交易双方信用值都有影响。

## 4.2CGPBFT机制吞吐量测试

吞吐量是检测区块链系统运行效率高低的标准。区块链系统中对于吞吐量的定义为：

（7）

其中，为出块所消耗时长，*tx*为时间段内打包进区块的交易数。

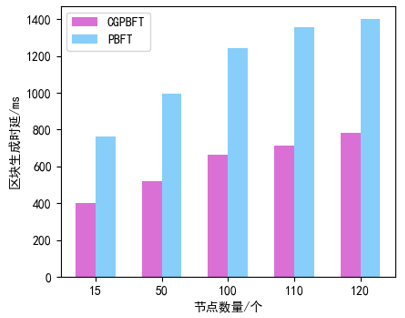
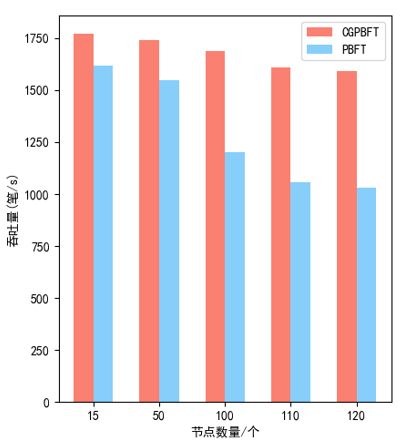


图3吞吐量对比测试图 图4区块生成时延测试

实验对CGPBFT算法与PBFT算法进行吞吐量对比测试及区块链生成对比测试，测试结果如图3、4所示，从图中可知，随着节点数量的增加，两种算法的吞吐量都有减少，但CGPBFT算法的吞吐量高于PBFT算法；随着节点数量的增加，区块生成时延均在增加，但CGPBFT算法的区块生成时延低于PBFT算法。

出现这种情况的原因如下：1）根据分组优化机制，有效减少了参与共识的节点数量，降低了通信量；2）主节点和代理人节点由信用投票机制选出，节点可靠性较高，出现错误的概率极低，视图切换的次数会随之减少，完成共识的时间相应减少。4）简化了PBFT算法，共识过程减少了通信量，缩短了共识时间。

## 4.3分组优化机制效率测试

为了验证分组优化机制的效率，实验假设系统内有1000个节点，测试各组间交易电量及信用值的差值在不同范围内时，分组优化机制的效率；及测试在不同分组数量下，分组优化机制完成所需的时间。实验测试10次，取平均值作为实验结果，如图5所示。

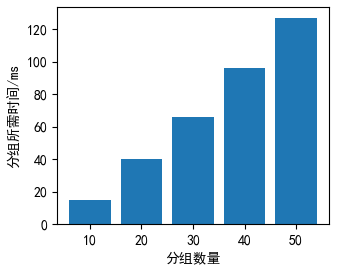


图5 分组优化机制效率测试

由图5可以看出，随着分组数量的增加，分组优化机制所消耗的时间越长。但总体而言，分组所消耗的时间相对于CGPBFT整个共识流程而言，仍在可接受范围。实验证明，CGPBFT机制能够高效的完成分组过程，有效减少了共识节点的数量，降低了通信量，提高了共识效率。

# 5结束语

针对当前智能电网系统存在交易失信、违约现象及用户个体电能产量不确定性等问题，本文设计了基于智能合约的电能交易流程；针对电网区块链系统中共识算法共识效率较低、资源浪费较严重等问题，本文提出了一种基于信用分组投票的电网区块链共识算法，在不影响系统容错性能的条件下，降低了一致性处理的消息复杂度，使得系统在系统硬件和网络条件下，可以容纳更多的节点，提高了系统安全性。大规模网络节点涌入的情况下，如何提高分组优化的执行效率，缩短系统进入良性循环时间是进一步要研究的问题。

参考文献

1. 曾鸣, 杨雍琦, 刘敦楠,等. 能源互联网"源–网–荷–储"协调优化运营模式及关键技术[J]. 电网技术, 2016, 40(1):114-124.
2. Welisch M . Multi-unit renewables auctions for small markets - Designing the Danish multi-technology auction scheme[J]. Renewable Energy, 2019, 131(FEB.):372-380.
3. Mengelkamp E , Staudt P , Garttner J , et al. Trading on local energy markets: A comparison of market designs and bidding strategies[C]// European Energy Market. IEEE, 2017.
4. 平健, 严正, 陈思捷,等. 基于区块链的分布式能源交易市场信用风险管理方法[J]. 中国电机工程学报, 2019, 39(24).
5. 秦金磊, 孙文强, 李整,等. 适用于微电网区块链的信用共识机制[J]. 电力系统自动化, 44(15):10.
6. 武赓, 曾博, 李冉,等. 区块链技术在综合需求侧响应资源交易中的应用模式研究[J]. 中国电机工程学报, 2017(13):3717-3728.
7. SijieCHEN, Chen-ChingLIU. From demand response to transactive energy: state of the art[J]. Journal of Modern Power Systems and Clean Energy, 2017, 5(1):10–19.
8. Alam M T , Li H , Patidar A . Bitcoin for smart trading in smart grid[C]// 2015 IEEE International Workshop on Local and Metropolitan Area Networks (LANMAN). IEEE, 2015.
9. 佘维, 胡跃, 杨晓宇,等. 基于能源区块链网络的虚拟电厂运行与调度模型[J]. 中国电机工程学报, 2017, 37(013):3729-3736.
10. Mengelkamp E , Notheisen B , Beer C , et al. A blockchain-based smart grid: towards sustainable local energy markets[J]. Computer Science - Research and Development, 2018, 33(1-2):207-214.
11. 邰雪, 孙宏斌, 郭庆来. 能源互联网中基于区块链的电力交易和阻塞管理方法[J]. 电网技术, 2016(12):3630-3638.
12. 平健, 陈思捷, 张宁,等. 基于智能合约的配电网去中心化交易机制[J]. 中国电机工程学报, 2017(13):3682-3690.
13. 杨晟,孙跃,龚钢军,杨佳轩,周波.基于能源区块链的综合能源服务研究[J].华电技术,2020,42(08):11-16.
14. 张利华,万源华,付东辉.基于区块链的用电数据存储方案[J].计算机应用与软件,2021,38(09):21-27+52.
15. 周步祥,张越,臧天磊,曹强,张远洪,彭昊宇.基于区块链的多虚拟电厂主从博弈优化运行[J/OL].电力系统自动化:1-13[2021-09-28].
16. 谭敏生、杨杰、丁琳、李行健、夏石莹. 区块链共识机制综述[J]. 计算机工程, 2020, v.46;No.521(12):7-17.
17. Jakobsson M , Juels A . Proofs of Work and Bread Pudding Protocols[J]. Kluwer, B.V. 1999.
18. Kiayias A , Russell A , David B , et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol[C]// Springer, Cham. Springer, Cham, 2017.
19. 张永, 李晓辉. 一种改进的区块链共识机制的研究与实现[J]. 电子设计工程, 2018.
20. CASTRO M, LISKOV B. Practical Byzantine fault tolerance［C］//Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. [S.I.]: USENIX Association，1999:173-186.
21. 刘明川. 基于能源区块链的分布式电能交易系统设计[D]. 华北电力大学(北京), 2018.

1. 在分组过程中，各个组之间的电量、信用值差距可以根据系统内具体情况进行设置，以达到最优分组结果。 [↑](#footnote-ref-1)