计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(11):57−65 [doi: 10.15888/j.cnki.csa.007613]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 基于 PoA 联盟链的微电网无报价交易机制①

夏晨益, 蔡青松, 吴　杰

(北京工商大学 计算机与信息工程学院, 北京 100048)
通讯作者: 蔡青松, E-mail: caiqs@btbu.edu.cn

**摘　要**: 传统微电网电力交易模式存在中心化、数据不透明等问题, 区块链的去中心化、不可篡改、可追溯和无需信任等特点被广泛用于电力交易. 当前的研究主要在共识机制、交易机制和隐私保护方面, 且大多都需要交易者每周期不断进行报价. 本文提出了一种基于权威证明 (Proof of Authority, PoA) 共识的联盟链无报价电力交易机制, 电力消费者无需报价只需预存电费, 即可在电费耗尽前基于智能合约自动进行电力交易, 资金的结算采用能源代币. 最后与其它 4 种现有区块链电力交易方案进行对比分析, 并模拟仿真了 5 个产消者和 5 个消费者的电力交易, 分析了买卖双方的收益. 结果表明本方案让买卖双方同时受益, 经济成本更低, 共识效率高.

**关键词**: 区块链; 微电网; 电力交易机制; 权威证明; 智能合约

引用格式: 夏晨益,蔡青松,吴杰.基于 PoA 联盟链的微电网无报价交易机制.计算机系统应用,2020,29(11):57–65. http://www.c-s-a.org.cn/1003-3254/7613.html

## Microgrid No-Bidding Trading Mechanism Based on PoA Consortium Blockchain

XIA Chen-Yi, CAI Qing-Song, WU Jie

(School of Computer and Information Engineering, Beijing Technology and Business University, Beijing 100048, China)

**Abstract**: The traditional microgrid electricity transaction mode has such problems as centralization and data transparency, and because of the features like decentralized, tamperability, traceability and untrusted characteristics of the Blockchain is widely used in electricity transaction. Current research focuses on consensus mechanism, trading mechanisms and privacy protection, and most of them require traders to make constant bidding every cycle. This paper presents a consortium Blockchain without bidding electricity trading mechanism based on the consensus of proof of authority (PoA), electricity consumers do not need to bid the pre-deposit of electricity, can automatically trade electricity based on smart contracts before the electricity bill runs out, the settlement of funds using energy tokens. Finally, the comparison and analysis of the other 4 existing Blockchain electricity trading schemes, and the simulation of 5 producers and 5 consumers of electricity transactions, analysis of the buyer's and and seller's earnings. The results show that the scheme benefits both buyers and sellers at the same time, with lower economic costs and high consensus efficiency.

**Key words**: Blockchain; microgrid; electricity trading mechanism; Proof of Authority (PoA); smart contract

目前传统能源面临资源枯竭和环境污染等问题, 新能源的出现为各种能源获取、环境恶化提供了解决方案[1]. 尽管传统的集中式发电远距离传输稳定, 但也存在诸如传输成本高和单一电源形式等问题. 因此分布式发电技术近来得到了大力的发展, 具有分布式发电设备的用户可以与小范围内的其他普通用电用户组

① 基金项目: 国家自然科学基金 (61702020); 北京市自然科学基金-海淀联合原创项目 (L182007)
Foundation item: National Natural Science Foundation of China (61702020); Joint Fund of Natural Science Foundation of Beijing Municipality and Haidian Original Innovation Fund (L182007)
收稿时间: 2020-02-17; 修改时间: 2020-03-17; 采用时间: 2020-04-03; csa 在线出版时间: 2020-10-29

成一个微电网系统, 在微电网内进行电力交易, 微电网内的本地能源交易可在提高供电可靠性的同时降低用电成本[2], 同时促进新能源的利用, 减少集中式供电电能损耗, 提高电网峰谷性能.

在传统的电力交易模式中, 参与电力市场的主体一般是电网企业、大型能源生产商和电力消费者. 家庭级别的消费者和生产者没有积极参与电力市场的交易, 仅是向电网企业购买电力. 在微电网中, 用户参与到实时的电力交易当中. 这种市场设计要求参与的用户估算其未来的能源需求或供应总量, 以便能够向市场提交未来一段时间内的交易量[3].

传统微电网电力交易通过中心化交易机构, 这种模式存在一定隐患. 例如用户信息和交易数据由交易机构储存容易被篡改, 不能有效地保证信息安全且中心化交易还存在单点故障的风险. 促进微电网的去中心化交易模式, 降低微电网市场的运营成本, 确保微电网电力交易信息的安全性, 变得尤为重要.

区块链是一种去中心化的解决方案, 不需要任何第三方组织. 区块链将密码学技术、共识机制、智能合约、时间戳等结合, 具有去中心化, 防篡改的特点[4]. 智能合约是可自动运行的代码, 电力交易基于智能合约, 因此无需第三方干预即可自动执行, 实现去中心化交易. 将区块链与微电网结合可以降低微电网市场的运营成本, 可以保证微电网电力交易的安全性, 并使微电网市场的交易过程更加透明.

国内外已经有很多将区块链与电力交易结合的相关研究成果. 文献 [5–7] 分析了区块链在电力行业中的应用场景, 包括能源认证、电力交易、能源金融、数据存储安全、和相关服务等. 文献 [3] 中总结了 3 种分布式电力交易机制及其发展现状, 文献 [8,9] 总结了国内外 140 多个区块链能源项目, 并指出了目前的研究方向与所存在的问题, 但没有给出具体方案. 文献 [10] 提出了基于区块链的微电网能源市场的概念, 其推出的 TransActive Grid 是美国纽约的一个社区区块链电力交易项目, 但存在交易效率差的问题. 文献 [11] 提出了一种基于连续双向拍卖机制的交易方法, 能根据市场实时调整电力报价, 但需要用户不断提交报价. 文献 [12] 对区块链电力交易的具体流程进行了分析, 但其使用公有链存在效率、计算资源浪费的问题. 综合来看, 目前的研究许多都集中在增加交易效率和交易机制上. 现有方案存在的问题包括对参与用户的信息隐私性保护不够, 交易效率不够高以及需要用户每周期不断进行报价, 而普通电力消费者可能更期望能预缴一笔电费, 在预缴电费耗尽前可以不再需要反复提交报价.

本文受以上研究的启发, 设计了区块链微电网电力交易模式, 基于智能合约自动执行电力交易, 实现相互无需信任的用户可以完成去中心化的电力交易. 本文主要工作内容如下:

1) 提出了一种微电网无报价交易机制, 使电力交易去中心化, 电力消费者只需预存电费, 在电费耗尽前无需再次参与电力拍卖, 避免了不断提交报价信息. 通过模糊用户身份信息, 增强隐私性.

2) 采用 PoA 共识算法构建微电网电力交易联盟链, 能减少网络拥堵且无需通过算力竞争出块, 更为节省电力消耗, 减少分叉, 共识效率更高.

3) 模拟仿真 5 个产销者和 5 个消费者的微电网电力交易, 证明本文交易机制的可行性.

## 1 区块链技术

### 1.1 区块链概念

2008 年, 化名为“中本聪”的研究者在一篇关于密码学的论文中提出区块链的概念[13], 随后出现的比特币数字加密货币就是以区块链为底层技术. 区块链是一个分布式数据库, 基本结构如图 1 所示, 它按时间顺序将不同的数据块以链的形式储存, 每一个区块分为区块头和区块体. 区块体储存交易信息, 区块头中记录了父区块的哈希值和 Merkle 根等信息. 修改一个区块的数据将会使得区块的哈希值发生改变, 这将会与之前子区块头中的记录的哈希值不符. 将区块体内所有交易记录取哈希值, 将两个交易哈希值合并后再算出新哈希. 不断重复该操作直到只剩一个哈希值, 即 Merkle 根, 此过程类似于一个倒二叉树. 若修改区块体中数据会造成 Merkle 的值与父区块头所记录的 Merkle 之不同. 父块哈希值和 Merkle 根共同实现区块数据的不可篡改性. 区块链的关键技术涉及数据块, 链结构, P2P 网络, 时间戳, Merkle 树, 哈希函数, 非对称加密, 共识机制等[14], 区块链系统通过数学方法来建立相互信任, 整个系统由所有节点共同维护, 单个节点故障不会引起整个网络故障, 网络的抗干扰能力强. 时间戳技术可实现区块链数据的可验证性和可追溯性, 每个区块的区块体中的交易数据都有时间信息, 这使得数据难以

伪造. 区块链网络中所有节点都保存一份账本数据, 修改数据需要攻击超过 50% 的节点.

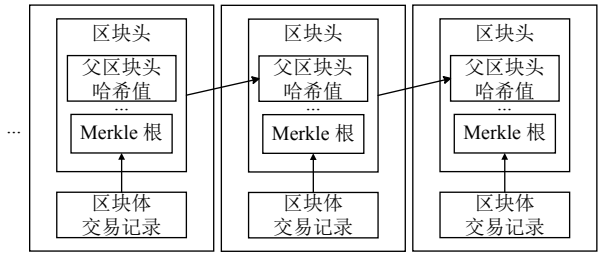


图 1 区块链基本结构

区块链技术现在主要有 3 种模式, 分别是公有链、私有链和联盟链. 公有链是一个完全公开的区块链, 每个节点地位平等, 记账共识由所有节点共同参与; 私有链是一个完全集中的区块链, 更适合用于组织内部的数据管理. 记账权由单一机构控制; 联盟链的分散程度介于两者之间, 记账权由联盟内的特定节点.

### 1.2 智能合约

智能合约使得区块链有更广泛的应用场景[15], 能通过分布式账本确认和转移各种形式的资产, 而不局限于数字货币. 智能合约是一种能根据预定义规则自动执行的链上代码, 无需第三方机构监督. 电力交易由智能合约完成, 大大减少人力成本, 且解决交易者之间的信任问题.

### 1.3 共识机制

共识机制指的是没有中心机构参与时对事务的合法性如何达成一致[16]. 区块链目前较为常见的共识机制有工作量证明 (Proof of Work, PoW)、实用拜占庭容错 (Practical Byzantine Fault Tolerance, PBFT) 和权益证明 (Proof of Stake, PoS) 等.

PoW 共识机制最先被用于比特币[17], 因此基于区块链的能源交易研究中早期共识机制采用 PoW. PoW 需要依靠“矿工”挖矿来实现共识, “矿工”指的是有计算能力的设备, 其通过解决一个困难的数学问题, 即找到一个随机数以形成满足条件的哈希值, 从而实现共识证明. 但是 PoW 存在共识效率差和浪费计算资源的缺点.

PBFT 是一种可以容忍拜占庭故障[18] 的复制算法, 适用于联盟链或私有链. 共识过程需要三轮投票并且每轮都广播, 因此每个节点都需要知道网络中其他每个节点的身份. 与 PoW 不同, PBFT 出块不需要计算复杂的数学难题, 因此可以节省大量能耗. 当恶意节点的数量少于节点总数的 1/3 时, 可以达成正确的共识.

PoS 尝试解决 PoW 算力资源浪费的缺点[19], 以节点账户拥有代币在全网总代币的比值和持有的时间长短来竞争记账权. 但目前 PoS 还未成熟, 还存在安全性和代币分配机制设计等问题.

本文微电网交易机制所采用共识机制是权威证明 (Proof of Authority, PoA), 其通常用于联盟链中, 其优点是达成共识快、耗能低、扩展性强等[20]. 以太坊中的 PoA 基于 clique 算法, 该算法需要预先确定一组授权节点 (signers) 负责出块, 所有 signer 组成委员会, 在委员会中通过投票决定是否删除或新增 singer 节点. PoA 生成区块无需算力竞争, 这大大减少了资源浪费, 增强共识效率.

微电网运营商在联盟链搭建时在创世区块中设置初始 signers. 联盟区块链开始运行后, 委员会的所有 signer 排序后轮流取得优先记账权, 并在区块头签名. 在每一个区块高度对应一个 signer 处于 IN-TURN 状态, 其余的 signer 是 OUT-OF-TURN 状态, IN-TURN 状态的节点打包区块的权值为 2, 其他节点的权值为 1. 在系统中每个节点都维护一条权值总和最高的区块链, 且 IN-TURN 状态的节点能优先广播区块, 因此其打包的区块会被优先上链. 当 IN-TURN 状态节点出现故障宕机未能出块时, 其余 signer 竞争记账权, 通过 GHOST 协议[21] 会处理分叉情况.

为保证区块链中交易的合法性, 每个 signer 在接收新区块后会进行验证. 评估交易合法性的参数主要有:

1) 收到新区块时, 由区块头中的签名算出其出块节点账户地址, 检验区块是否由 singer 广播, 同时根据 signer 是否在 IN-TURN 状态, 确定上链优先级.

2) 校验提交发电量是否符合物理约束.

3) 校验参与交易用户是否已在微电网运营商注册, 防止出现虚假交易.

4) 验证交易签名信息.

5) 校验交易时间的合理性, 对时间戳进行核对, 防止多次交易.

## 2 基于区块链的微电网电力交易模式

### 2.1 总体架构

分布式发电设备的用户在电力富余时作为生产者

出售电力, 电力不足时作为消费者购买电力, 称之为产消者. 在微电网模式下, 电力产消者、普通电力消费者和微电网运营商组成微电网. 微电网系统与大电网的连接通过微电网运营商, 微电网运营商对整个微电网进行控制, 保证电力系统的功率平衡、电压稳定. 当前的电力交易市场一般包括日前市场、日内市场和实时市场 3 种, 因为微电网电力交易量小, 且分布式电源发电的波动性较大, 受天气、温度等因素的影响, 发电量在短期内预存更为准确, 所以实时交易市场是比较适合微电网的.

在基于区块链的微电网电力交易模式下, 用户间的电力交易通过智能合约自动执行, 不再通过传统的交易机构进行, 微电网运营商维护电网稳定运行同时对交易收取过网费. 假设每个用户均安装集成了区块链模块的双向智能电表, 从而将用户的出售/购买电量信息上传至区块链网络. 微电网运营商充当一个 signer 节点, 收集实时用电数据, 维护微电网运行. 金融机构也作为一个 signer 节点参与区块链网络, 每个用户都可以选择充当一个节点, 可由微电网社区内的所有用户选择出固定数目的授权节点. 整个微电网通过微电网运营商与外部的大电网相连接, 在内部电力不足时可向大电网购电, 内部电力富余时向大电网出售多余电量. 基于区块链的微电网电力交易机制的系统结构如图 2 所示.

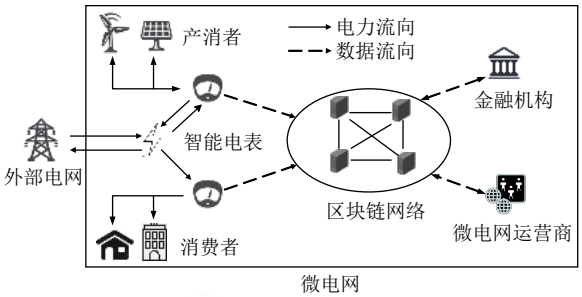


图 2 系统结构

当前许多交易机制未考虑到电力消费者用户无法很好地对自身用电情况进行预测, 因此无法提供未来一个交易周期内正确的购买电量使得当前许多已有交易机制有很大的局限性. 本文所采用的交易机制中消费者用户在交易时不需要提交购买报价和电量, 只需要向智能合约转移足够的能源代币. 智能合约周期性结算上一用电周期的电力交易费用. 每个用户的智能电表周期性将出售/购买电量数据上传至区块链, 通过上传的数据计算的上一周期实际交易电量. 以消费者为例, 根据上周期实际购买电量计算交易费用, 并从之前转移的能源代币中扣除相应的费用, 当能源代币不足后可控制智能电表进行断电. 对于产消而言需要准确预测自身的出售量, 智能合约在每个周期将上一周期发电所得利益以能源代币形式转移至产消者账户地址, 同时还进行惩罚激励, 对报量与实际量不一致进行惩罚, 以促进产消者合理报量. 每个用户在交易前都需提前转移一笔安全保证金至交易智能合约. 对于消费者来说此费用是为了避免该用户在智能合约所剩余的用于交易的能源代币数量不足以支付上一周期的实际用电量. 对于生产者来说, 奖惩激励会从保证金中扣除费用, 保证金的存在能督促其更好预测出售量, 提交合理发电量.

基于区块链的微电网电力交易机制分如下几个阶段:

1) 注册阶段: 用户通过微电网运营商注册, 取得区块链微电网电力交易资格.

2) 缴纳保证金阶段: 用户向金融机构兑换能源代币, 在缴纳一笔保证金后才能开始电力交易.

3) 预交易阶段: 电力产消者用户提交下一周期的预测出售量; 电力消费者用户预先缴纳电费, 在预付电费耗尽前可不用再次提交交易请求.

4) 交易结算阶段: 根据上一交易周期的微电网内部实际交易总电量和大电网上一周期的平均购/售电价格计算出上一周期的微电网内部购/售电价格, 再根据各个用户的实际交易电量计算各自的收益和支出.

5) 惩罚激励阶段: 根据产消者的预测出售电量与实际量的偏差进行相应的惩罚, 以经济惩罚激励产消者提高预报量准确度.

针对以上交易流程我们设计了两个智能合约来实现. 一个是用于发行能源代币的能源代币合约, 整个交易的资源转移通过能源代币进行, 该合约由金融机构发布. 用户在进行电力交易前需要通过金融机构兑换一定数量的能源代币, 具体的兑换规则可根据实际情况确定, 本文未对其进行探讨. 另一个是交易合约, 用户的电力交易都通过此合约自动执行.

### 2.2 智能合约

#### 2.2.1 能源代币合约

在比特币和以太坊中, 新代币的来源是通过挖矿

产生的铸币交易, 且代币的价值是波动的. 而在本地微电网电力交易中, 交易周期性进行, 而进行结算的代币应具有稳定的价值, 价值会变化的代币不利于与金融机构间的实时结算. 且在 PoA 共识机制中出块没有奖励, 代币的来源需要有权威机构来担保, 因此通过金融机构发行一种价值稳定的能源代币就变得很有意义, 用户通过金融机构兑换能源代币进行能源交易. 本文发行能源代币基于 ERC223[22], 这是一种代币设计标准. 目前普遍采用的标准是 ERC20, 但它还远有一个很大的缺陷使得不适用于本文的微电网电力交易机制. 在本文方案中用户需要将能源代币发送给交易合约, 而 ERC20 在将代币发送到智能合约时, 代币可能丢失, 在 ERC223 中解决了这一缺陷. 设计能源代币合约函数如图 3 所示, 调用 balanceof 函数可查询账户能源代币的数量, 通过 transfer 函数可将能源代币转移至另一账户地址. 金融机构发布能源代币智能合约, 参与用户按需通过金融机构购买能源代币参与微电网电力交易.

```
function totalSupply() constant returns (uint256 totalSupply)
function name() constant returns (string _name)
function symbol() constant returns (bytes32 _symbol)
function decimals() constant returns (uint8 _decimals)
function balanceOf(address _owner) constant returns (uint256 balance)
function transfer(address _to, uint _value) returns (bool)
function transfer(address _to, uint _value, bytes _data) returns (bool)
function tokenFallback(address _from, uint _value, bytes _data)
```

图 3 能源代币合约函数

### 2.2.2 交易合约

交易合约由微电网运营商发布, 微电网内的电力交易都通过该合约实现. 主要包含用户注册函数、保证金函数、出售报量函数、预付电费函数、实际交易电量函数、交易结算函数和惩罚激励函数 7 个核心函数, 具体的功能与相关设计在本文后面的 2.4 节详细介绍. 交易智能合约各函数互相协助完成电力交易的逻辑如图 4 所示.

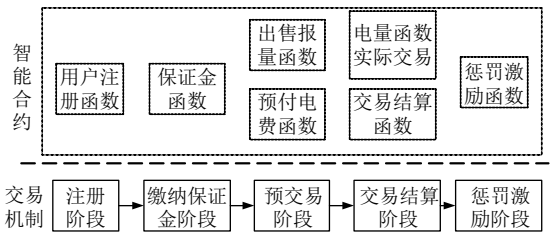


图 4 交易智能合约函数逻辑

## 2.3 定价机制

假设微电网有$m$个拥有分布式发电设备的产消者, $n$个消费者和 1 个微电网运营商. 产消者$i\in\{1,2,\cdots,m\}$, 产消者在发电量不满足自身用电需求时将变为消费者, 因此消费者数量最多可能为$m+n$, 消费者$j\in\{1,2,\cdots,m+n\}$. 用户一个交易周期内实际出售电量为$e_j^G$, 实际购买电量为$e_j^U$. 一个周期内的总实际出售电量为$E^G$, 实际总购买电量为$E^U$. 微电网电力富余时向大电网出售电力, 微电网电力不足时向大电网购买电量, 设该周期大电网的平均收购价为$p_o^S$, 平均售电价位$p_o^B$. 则微电网内的该时段产消者的电力出售价格$p^S$和消费者电力价格购买$p^B$应处于区间$\left[p_o^S,p_o^B\right]$, 考虑两种情况计算微电网内部电价$p^S$和$p^B$.

1) 当$E^G\geq E^U$时, 微电网内部电力富余, 向大电网出售电力总金额与消费者购电总金额之和应等于产消者的总收益.

$$\left(E^G-E^U\right)p_o^S+E^U p^B=E^G p^S \tag{1}$$

在本文模式下消费者和产消者与直接向大电网交易所获得的额外收益应相等, 即:

$$E^U\left(p_o^B-p^B\right)=E^G\left(p^S-p_o^S\right) \tag{2}$$

根据式 (1) 和式 (2) 可计算出:

$$p^S=p_o^S+E^U\left(p_o^B-p_o^S\right)/2E^G \tag{3}$$

$$p^B=\left(p_o^S+p_o^B\right)/2 \tag{4}$$

2) 当$E^G<E^U$时, 微电网内电力不足需向外部大电网购电, 这部分购电金额与产消者的售电总收益之和应为消费者的总支出, 即式 (5).

$$\left(E^U-E^G\right)p_o^B+E^G p^S=E^U p^B \tag{5}$$

根据式 (2) 和式 (5) 可计算出:

$$p^S=\left(p_o^S+p_o^B\right)/2 \tag{6}$$

$$p^B=p_o^B-E^G\left(p_o^B-p_o^S\right)/2E^U \tag{7}$$

## 2.4 交易机制

### 2.4.1 用户注册

在本文的交易模型中, 与传统比特币、以太坊中仅仅只转移资金的模式不同, 还涉及到电力资源的转移, 为确保交易者的身份真实有效, 用户在初次使用时需要提前进行向微电网运营商注册. 用户的相关信息应不被区块链网络中的其他用户所知, 为确保隐私性

使用 SHA256 算法[23] 对用户相关信息进行加密处理, 将所得的哈希值 *ID* 作为用户的唯一标识, 推断用户的相关信息将变得十分困难, 这在一定上保护了用户的隐私信息. 加密公式如式 (8) 所示.

$$SHA256(UserInfo) = ID \tag{8}$$

$UserInfo$中的信息包括用户的姓名、性别、现实世界中的地址、智能电表的编号、用户以太坊账户地址等. 由于 signer 的信息公开, 因此充当 signer 的用户的 signer 账户地址与用户的注册以太坊地址不相同. 避免根据相同账户地址推断出更多个人信息. 在验证用户提交的相关信息真实后, 微电网运营商将调用交易智能合约中的用户注册函数, 为用户创建用户信息结构体, 该函数只能由微电网运营商的账户地址触发, 其他用户无权写入用户信息, 结构体形式如下:

Struct User{
String ID;//用户相关身份信息唯一标识
address Address;//用户以太坊账户地址
}

用户注册过程如图 5 所示. 因用户身份信息模糊化的加密操作只在注册阶段进行一次, 在其后的阶段用户使用哈希值 *ID* 作为身份标识, 区块链节点仅需验证 *ID* 与结构体中的 Address 是否相对应, 所以对性能的影响极小.

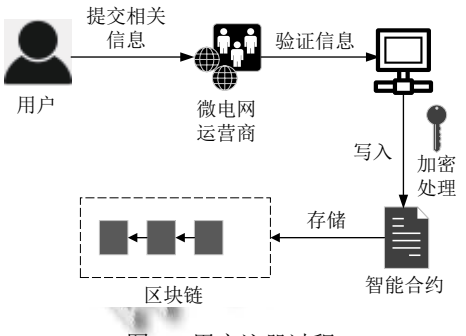


图 5 用户注册过程

### 2.4.2 保证金与预交易

用户缴纳保证金实质是转移一定数额的能源代币至交易智能合约账户. 产消者的保证金用来支付后面的惩罚阶段的惩罚金, 消费者的保证金是为了防止交易结算阶段出现剩余预付电费不足以支付上一周期实际用电电费. 成功缴纳保证金后智能合约将为其创建保证金结构体, 结构体的形式如下:

Struct Deposit{
address Address;//用户以太坊账户地址
uint256 DepositNum;//用户保证金数目
}

用户的保证金数额需达到相应的数额才可进行入预交易阶段.

在预交易阶段, 电力产消者通过发电报量函数提交下一周期的预测发电量, 电力消费者用户通过预付电费函数预先缴纳电费, 只要预付电费没有耗尽, 用户可以一直用电.

### 2.4.3 交易结算

用户智能电表的实时出售/购买电量数据通过实际发用电量函数上传至区块链网络, 发送的数据包括实时出售/购买电量、用户以太坊账户地址和用户私钥生成的数字签名. 通过验证数字签名确认此信息不是其他用户所发出[24].

每个周期结算上一周期的实际电力交易, 根据实际发用电量函数收集的用户实际出售/购买电量数据, 结算上周期产消者的收益和消费者的支出, 具体的流程如算法 1.

算法 1. 电力交易结算算法

1) 输入: $e_i^G$, $e_j^U$, $p_o^S$, $p_o^B$;
2) 输出: 产消者$i$的收益$C_i$, 消费者$j$的支付电费$S_j$;
3) 初始化$E^G$=0, $E^U$=0.
4) $E^G=\sum_{i=1}^{m} e_i^G$
5) $E^U=\sum_{j=1}^{m+n} e_j^U$
6) if $E^G \geq E^U$
7) 根据式 (3) 和式 (4) 计算$p^B$和$p^S$
8) else
9) 根据式 (6) 和式 (7) 计算$p^B$和$p^S$
10) end if
11) for $i$=1; $i \leq m$; $i$++ do
12) $C_i=p^B \times e_i^G$
13) end for
14) for $j$=1; $j \leq m+n$; $j$++ do
15) $S_j=p^S \times e_j^U$
16) end for

### 2.4.4 惩罚激励

智能合约根据产消者的预测出售电量与实际出售电量的偏差进行相应的惩罚激励, 产消者为了获得更大的经济利益会努力提高预测的准确度. 由于本文直接根据上一周期实际交易量进行结算, 预测偏差不会对实际交易产生影响, 因此提高准确度主要是为了微电网运营商能更准确获取实时的微电网内产消者的预

售电信息, 本文进行简单设计.

产消者$i$的预测出售电量为$e_i^p$, 则产消者$i$的偏差量为$\left|e_i^G-e_i^p\right|$, 所有产消者的总偏差量$E^D$如式 (9) 所示. 产消者$i$的惩罚激励值$R_i$如式 (10), 惩罚值与该交易周期外部电网的平均出售售电价$p_o^S$相关, $D$为惩罚系数, 由微电网运营商根据实际情况调整.

$$E^D=\sum_{i=1}^{m}\left|e_i^G-e_i^p\right| \tag{9}$$

$$R_i=\frac{e_i^G-e_i^p}{E^D}p_o^S D \tag{10}$$

## 3 分析与仿真实验

### 3.1 效率分析

我们将事务在被节点打包到区块广播至区块链网络, 被全网其他节点接收并验证合法性而达成共识的时间长短来作为效率的评估指标. PoW 的效率最低, 因为在广播区块前, 需要花费大量时间来计算一个复杂的数学难题. 与 PBFT 相比, 在 PoA 中 signer 节点在广播区块时只需一次通信, 而在 PBFT 中需要 3 次通信, 如图 6 所示. 假设节点数量为$N$ , 则 PoA 的通信规模为$N$, 而 PBFT 的通信规模为$N^3$, 因此在$N$的数量大于 16 个时, PBFT 的效率会大大降低[25].

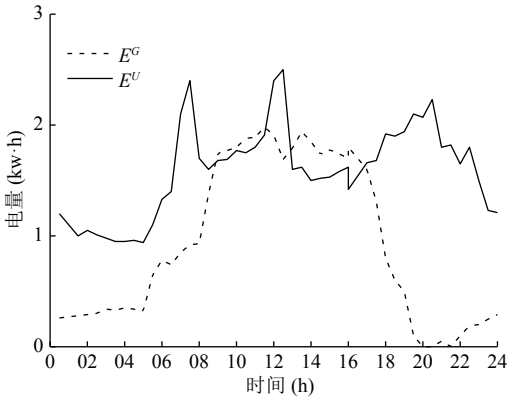


图 6 微电网内每 0.5 h 总出售/购买电量

### 3.2 安全性分析

(1) 身份隐私

用户的真实身份信息仅有微电网运营商所知, 在区块链网络中以用户经过加密处理的的哈希值 ID 作为唯一标识, 推断用户的相关信息将变得十分困难, 这在一定上保护了用户的身份隐私.

(2) 数据安全

电力数据分布式存储, 非对称加密技术以及数字签名技术的结合使得保证恶意节点恶意节点无法伪造交易数据, 去中心化的方式还能避免单点故障且交易过程也更加透明化.

(3) 恶意节点

联盟链的准入机制以及 signer 节点是由大家选举出来的有公信力的用户, 使得其作恶可能性大大降低. 即使存在恶意 signer, PoA 的机制也能保证区块链的安全. 其最多只能攻击 ((signer 总数量/2)+1) 个连续块中的 1 个, 期间可以由其他 signer 投票踢出该恶意 signer.

### 3.3 对比分析

本文与其它 4 种现有方案进行对比分析, 结果如表 1 所示. 本文考虑了用户身份隐私性, 用户真实信息仅有微电网运营商所知, 在交易过程中用户仅以哈希 ID 作为身份标识, 相比于文献 [11] 的方案隐私性有所增强. 在共识效率方面, 在 4.1 小节中已进行了相关分析, 本文采取 PoA 共识机制与其它 4 种方案的 PoW 和 PBFT 相比都具有优势. 表 1 中前两种方案的 PoW 机制需要较多的节点来防止少数节点作恶, 本文采用的联盟链和表 1 中的第 4 和第 5 两种方案都可使用较少的节点. 因此可看出, 本文方案适合解决微电网电力交易问题.

表 1 本文与其他方案对比

| 方案 | 共识机制 | 类型 | 隐私性 | 共识效率 | 节点需求 |
|---|---|---|---|---|---|
| 文献[11] | PoW | 公有链 | 差 | 低 | 多 |
| 文献[12] | PoW | 公有链 | 较强 | 低 | 多 |
| 文献[6] | PBFT | 联盟链 | 较强 | 较高 | 较多 |
| 文献[7] | PBFT | 联盟链 | 强 | 高 | 少 |
| 本文方案 | PoA | 联盟链 | 较强 | 高 | 少 |

### 3.4 微电网电力交易仿真实验

在实验过程中, 用 5 台机器作为联盟链中节点的载体, 将金融机构和微电网运营商设为初始授权节点, 负责打包生成新区块, 其余节点为普通节点. 使用 Solidity 在 Remix 上编写智能合约, 编译和调试后再部署在 PoA 联盟链上, 实验环境如表 2 所示. 本文的电力交易数据是文献 [26] 中所提供的电力数据集, 该数据集是 Discovergy GmbH 公司收集的 100 个纯能源消费者和 100 个能源产消者的智能电表的电表读数信息. 本文模拟了 5 个消费者和 5 个产消者在 1 天中的电力交易情

况, 设置一个交易周期为 30 分钟, 结合用电峰谷情况设置外部大电网每一周期平均电价[27].

表 2 实验环境

| 实验环境 | 详情 |
|---|---|
| CPU | Intel 酷睿i5 (2.8 GHz) |
| 系统 | Windows 7 |
| IDE | Remix |
| 语言 | Solidity |
| 编译环境 | JavaScript VM |
| 测试网络 | Rinkeby |

各交易周期整个微电网内部电力总出售量和总购买量的变化情况如图 6 所示. 可以看出出售量在白天多而晚上低, 这是因为光伏发电设备的发电量受光照强度的影响, 在缺乏充足光照条件时因此发电量主要来源于其他发电设备, 如风力发电机. 图 7 为各交易周期间的向外部电网平均出售电价$p_o^S$, 向外部电网平均购电价格$p_o^B$, 微电网内部产消者售电价格$p^S$和微电网内部消费者购电价格$p^B$的变化情况. 可以看出内部电价始终处于区间$\left[p_o^S, p_o^B\right]$内, 与直接向外部电网交易相比, 产消者与消费者都比获得更多经济利益. 在 0:00~8:00 是用电低谷期间, 相应的收/售电价都较低; 下午 14:00~17:00 和晚上 19:00~22:00 为用电高峰, 平均收/售电价都最高; 其余时间为正常用电时期, 电价均衡.

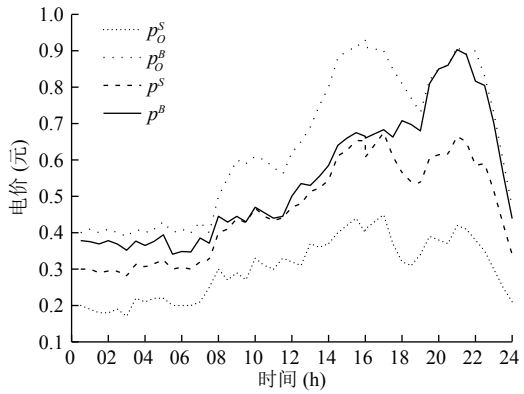


图 7 电价对比

图 8 为本文模式与传统电力交易模式下一天内的总售电收益和总购电费用对比. $C_{\text{New}}$和$C_{\text{Tra}}$分别表示所有产消者一天内在本文模式和传统模式下的总收益, $S_{\text{New}}$和$S_{\text{Tra}}$分别表示所有消费者一天内在本文模式和传统模式下的总电费. 可以看出在本文机制下, 在一天的时间内, 产消者增加了大约 7.19 元售电收益, 消费者减少了大约 7.30 元购电费用, 证明了本文模式的可行性.

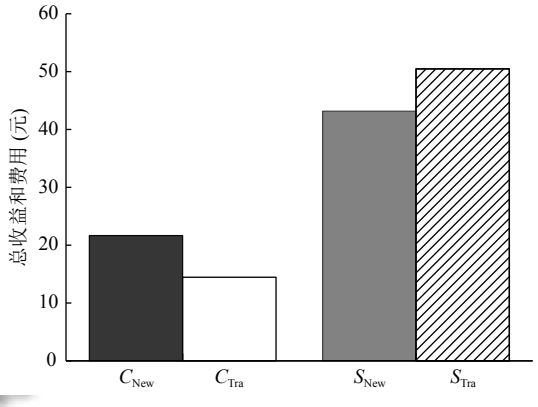


图 8 总收益和费用对比

## 4 总结

本文针对当前电力交易所存在的需要不断报价、效率不足和用户身份隐私的问题, 提出一个基于 PoA 联盟链的微电网无报价交易机制. 本文的交易机制对电力消费者用户更加友好, 用户只需预缴一笔电费即可通过智能合约自动完成每周期交易, 而无需不断进行电力拍卖报价. 与现有的几个方案做对比, 本文方案在共识效率、用户身份隐私性、节点需求方面都具有一定优势. 最后仿真模拟了一天内的 5 个产消者和 5 个消费者的电力交易, 实验表明本文模式与传统交易模式相比具有明显优势, 证明了本文方案的可行性.

## 参考文献

1 Zia MF, Elbouchikhi E, Benbouzid M. Microgrids energy management systems: A critical review on methods, solutions, and prospects. Applied Energy, 2018, 222: 1033–1055. [doi: 10.1016/j.apenergy.2018.04.103]

2 陈美福, 夏明超, 陈奇芳, 等. 主动配电网源-网-荷-储协调调度研究综述. 电力建设, 2018, 39(11): 109–118. [doi: 10.3969/j.issn.1000-7229.2018.11.013]

3 林俐, 许冰倩, 王皓怀. 典型分布式发电市场化交易机制分析与建议. 电力系统自动化, 2019, 43(4): 1–8. [doi: 10.7500/AEPS20180829001]

4 郭欣沅, 董思晴, 黄文涛, 等. 区块链技术在电力行业物资合同管理中的应用. 计算机系统应用, 2019, 28(7): 65–71. [doi: 10.15888/j.cnki.csa.006968]

5 Lu X, Guan ZT, Zhou X, *et al*. A secure and efficient renewable energy trading scheme based on blockchain in smart grid. Proceedings of 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Zhangjiajie, China. 2019. 1839–1844.

6 Sugiyama E, Marmiroli M. Blockchain-based bilateral energy transaction platform. Proceedings of 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). Bucharest, Romania. 2019. 1–5.

7 王惠洲, 于艾清. 基于联盟区块链技术的 V2V 电力交易研究. 现代电力, 2019, 36(3): 34–41. [doi: 10.3969/j.issn.1007-2322.2019.03.006]

8 Andoni M, Robu V, Flynn D, *et al*. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 2019, 100: 143–174. [doi: 10.1016/j.rser.2018.10.014]

9 Wang NY, Zhou X, Lu X, *et al*. When energy trading meets blockchain in electrical power system: The state of the art. Applied Sciences, 2019, 9(8): 1561. [doi: 10.3390/app9081561]

10 Mengelkamp E, Gärttner J, Rock K, *et al*. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied Energy, 2018, 210: 870–880. [doi: 10.1016/j.apenergy.2017.06.054]

11 王健, 周念成, 王强钢, 等. 基于区块链和连续双向拍卖机制的微电网直接交易模式及策略. 中国电机工程学报, 2018, 38(17): 5072–5084.

12 韩冬, 张程正浩, 孙伟卿, 等. 基于区块链技术的智能配售电交易平台架构设计. 电力系统自动化, 2019, 43(7): 89–96. [doi: 10.7500/AEPS20181225009]

13 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

14 张俊, 高文忠, 张应晨, 等. 运行于区块链上的智能分布式电力能源系统: 需求、概念、方法以及展望. 自动化学报, 2017, 43(9): 1544–1554.

15 付烁, 徐海霞, 李佩丽, 等. 数字货币的匿名性研究. 计算机学报, 2019, 42(5): 1045–1062. [doi: 10.11897/SP.J.1016.2019.01045]

16 Wang JP, Wang H. Monoxide: Scale out blockchain with asynchronous consensus zones. Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19). Boston, MA, USA. 2019. 95–112.

17 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望. 自动化学报, 2018, 44(11): 2011–2022.

18 Lamport L, Shostak R, Pease M. The Byzantine generals problem. Concurrency: The Works of Leslie Lamport. New York, NY, USA. 2019. 203–226.

19 Cao B, Zhang ZH, Feng DQ, *et al*. Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks, 2020. [doi: 10.1016/j.dcan.2019.12.001]

20 Samuel O, Javaid N, Awais M, *et al*. A blockchain model for fair data sharing in deregulated smart grids. Proceedings of 2019 IEEE Global Communications Conference (GLOBCOM). Waikoloa, HI, USA. 2019. 127–138.

21 Dinh TTA, Liu R, Zhang MH, *et al*. Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(7): 1366–1385. [doi: 10.1109/TKDE.2017.2781227]

22 Mulders M. A comparison between ERC20, ERC223, and ERC777 token standard. https://www.Cointelligence.com/content/comparison-erc20-erc223-new-ethereum-erc777-token-standard.-Title from the screen.

23 乔蕊, 曹琰, 王清贤. 基于联盟链的物联网动态数据溯源机制. 软件学报, 2019, 30(6): 1614–1631. [doi: 10.13328/j.cnki.jos.005739]

24 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望. 自动化学报, 2019, 45(1): 206–225.

25 Dinh TTA, Wang J, Chen G, *et al*. Blockbench: A framework for analyzing private blockchains. Proceedings of the 2017 ACM International Conference on Management of Data. New York, NY, USA. 2017. 1085–1100.

26 Kostmann M, Härdle WK. Forecasting in blockchain-based local energy markets. Energies, 2019, 12(14): 2718. [doi: 10.3390/en12142718]

27 陈中育, 吕立群, 林飞龙. 基于区块链的微电网定价机制设计与优化. 浙江师范大学学报 (自然科学版), 2019, 42(3): 248–253.