

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

王健¹, 周念成¹, 王强钢¹, 王鹏²

- (1. 输配电装备及系统安全与新技术国家重点实验室(重庆大学), 重庆市 沙坪坝区 400044;
2. 新加坡南洋理工大学电机与电子工程学院, 新加坡 639798)

Electricity Direct Transaction Mode and Strategy in Microgrid Based on Blockchain and Continuous Double Auction Mechanism

WANG Jian¹, ZHOU Niancheng¹, WANG Qianggang¹, WANG Peng²

- (1. State Key Laboratory of Power Transmission Equipment & System Security and New Technology (Chongqing University),
Shapingba District, Chongqing 400044, China; 2. School of Electrical & Electronic Engineering,
Nanyang Technological University, Singapore 639798)

ABSTRACT: In order to realize power directly transaction between distributed generations (DG) and loads in microgrid, this paper proposed an electricity transaction mode and strategy in microgrid based on blockchain and continuous double auction (CDA). Firstly, the buyer and seller shall first complete the transaction matching through CDA. Considering the frequent price fluctuation in CDA market, this paper proposed an adaptive aggressiveness strategy, which enabled the trader to adjust the quotation timely according to the market changes. Then DGs and consumers exchanged trading power digital certificate and expenditure on the blockchain system, and the consumers' interests were guaranteed by multi-signature if DG defaults. Digital certification of electricity energy assets was replaced by the sequence number with specific tags in the transaction script, and the size of digital certification could be adjusted according to transaction energy quantity. Finally, the feasibility of market mechanism through specific microgrid case and settlement process was also given.

KEY WORDS: microgrid direct transaction; blockchain; continuous double auction; adaptive aggressiveness strategy; asset digital certification

摘要: 为实现微电网内部分布式电源(distributed generation, DG)与用户电量直接交易, 该文提出基于区块链和连续双向拍卖机制的微电网电力交易模式及报价策略。买卖双方首先

通过连续双向拍卖机制完成交易匹配, 考虑到连续拍卖市场中价格波动频繁, 提出自适应进取性交易策略, 使得交易方能够根据市场变化及时调整报价; 然后 DG 和用户通过区块链系统实现交易电能数字证明和费用的交换, 并且通过多重签名机制保证 DG 违约时用户的利益; 在电能资产数字证明中, 通过对交易脚本中的序列号添加特定标记来代替交易电量, 并且根据交易电量不同动态调整数字证明大小。最后, 该文通过具体微电网案例验证交易机制的可行性, 并给出微电网交易结算流程。

关键词: 微电网直接交易; 区块链; 连续双向拍卖; 自适应进取性策略; 资产数字证明

0 引言

随着电力市场化改革的推进, 微电网或拥有 DG 的用户作为售电主体被允许参与电力市场交易^[1-2]。2017 年 10 月国家能源局发布了《关于开展分布式发电市场化交易试点的通知》, 明确 DG 市场化交易机制, 允许 DG 与电力用户进行电量直接交易, 并根据接入电压等级向电网公司适当缴纳“过网费”^[3]。DG 与用户之间的电力交易具有分散化、小规模的特点, 并且供需关系呈现类似证券市场上多买多卖的局面。然而 DG 和用户之间还没有搭建起价值流通的渠道, 大多数 DG 还是只能借助上网获得电价补贴, 无法进行直接的交易。微电网市场交易的关键是建立安全、低成本以及信息透明的交易模式。传统通过中心化机构对交易进行管理模式存在以下 3 个问题^[4]: 1) 交易中心运行成本

基金项目: 国家自然科学基金项目(51577018); 重庆市基础科学与前沿技术研究专项(cstc2015cyjBX0033)。

Project Supported by National Natural Science Foundation of China (51577018); Chongqing Research Program of Basic Research and Frontier Technology (cstc2015cyjBX0033).

高, 这些成本将直接转移给交易方; 2) 交易中心和交易方之间存在信任问题, 交易中心难以保证交易信息的公平、透明和有效性; 3) 存在交易数据被篡改风险, 直接威胁交易数据的安全和交易方的利益。因此亟需新的技术应用于微电网交易^[5]。

与此同时, 区块链技术通过运用非对称加密、数字签名、工作量证明等机制实现了点对点交易。区块链是一种按照时间顺序将数据区块依次相连的链式数据结构, 并通过密码学原理保证了数据的不可篡改和伪造^[6]。基于区块链的交易模式无需承担交易机构的运行管理成本, 而分布式数据库存储方式也降低了购买服务器的成本, 并且能够保证交易数据的透明和安全^[7]。工信部在《中国区块链技术和应用发展白皮书(2016)》中指出区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域, 并且有能力引发新一轮的技术创新和产业变革^[8]。区块链的出现为微电网内部电量直接交易提供了可行的途径。

目前区块链技术在电力领域中的研究及应用尚处于起步阶段, 但是已有初步成果。文献[9-10]探讨了区块链技术在电力领域中可能应用场景, 包括计量认证、市场交易、组织协同、能源金融和辅助服务等, 但没有提出具体的实施方案; 文献[5]提出了基于区块链技术的电力交易和阻塞管理方法, 但是该方法依然依赖于中心机构, 并没有实现完全的去中心化; 文献[11-12]分别提出了基于区块链的自动需求响应系统关键问题和需求侧资源交易方案; 文献[4,13-14]则分别提出了区块链技术在用户直购电、去中心化配电网交易以及基于虚拟电厂的虚拟电力资源交易的应用方法, 但是忽视了与区块链技术配套的市场交易机制。而具体到微电网交易领域, 文献[15]研究基于多重签名和区块链的分布式能源交易模式, 但该方法只是将电能作为一般性商品, 没有严格的市场机制并且缺少灵活的价格方案, 也没有违约赔偿机制; 美国纽约新创事业 LO3 Energy 与西门子公司合作开发基于区块链的微电网交易平台 TransActive Grid^[16], 为布鲁克林地区的用户之间提供光伏发电交易结算服务, 并且设计了集合竞价的机制, 但是没有为交易双方提供合适的报价策略模型和通过区块链进行直接结算的方法。文献[17]指出由于集合市场机制只能在固定时间段内报价, 待到某一个固定时刻才根据市场报价确定统一出清价, 因此该机制不够灵活, 不能及时根据市场价格变化调整报价策略。而在连

续双向拍卖机制下, 买卖双方可以实时的对报价进行调整, 能够灵活的根据市场均衡价格变化调整报价, 具有更高的效率。

连续双向拍卖市场的交易具有复杂性、动态性、随机性等特点^[18], 因此在这样复杂的市场环境中, 选取合适的交易策略具有很高的难度。目前连续双向拍卖市场中的交易策略主要有零信息策略(zero intelligence, ZI), 增强零信息策略(zero intelligence plus, ZIP)和自适应进取性策略(adaptive aggressiveness strategy, AA strategy)^[19-21]。ZI 策略在给定的价格区间内随意报价, 而不考虑市场中的交易, 这造成市场中交易者的收益偏低; ZIP 策略在报价时考虑市场成交价和失败价格, 进而调整自身报价; AA 策略则是交易者根据市场成交价格、价格波动等信息, 并通过学习机制自动调整报价。文献[21]比较了 3 种交易策略, 结果表示 AA 策略在市场效率、交易收益等多项指标优于其他策略。

本文将区块链和连续双向拍卖机制相结合应用于微电网的内部电量交易中, 可以实现 DG 和用户安全、自主的点对点交易。该模式下买卖双方根据 AA 策略向连续双向拍卖市场提交报价, 并根据交易结果对报价不断调整。在完成市场匹配之后, 买卖双方根据匹配交易结果通过区块链完成售电量数字证明和交易费用的结算, 实现微电网内电量直接交易。最后通过算例分析微电网交易原理和结算过程。

1 区块链原理及 UTXO 模型

1.1 区块链基本原理

区块链由一串基于密码学原理产生的数据块组成, 每个区块由区块头和区块体组成^[22], 如图 1 所示。区块体负责记录前一段时间内的所有交易信息, 区块链的大部分功能由区块头实现。区块头包含了上一个区块的哈希值, 该值是对前一个区块的区块头进行哈希函数计算得到, 区块之间由该哈希值依次连接构成区块链。区块体和区块头之前通过 Merkle 根联系, Merkle 根是交易 Merkle 树的根节点, 能够帮助区块链网络中各节点快速验证交易的存在性和正确性。

区块链网络是一个点对点(peer to peer, P2P)网络, 各节点之间无需经过任何中心化的第三方直接进行交易。区块链网络中所有节点地位对等, 都能够对区块中数据进行验证。区块链网络通过非对称加密技术、数字签名、共识机制等保障交易数据安全。

全,同时有效避免双重支付。

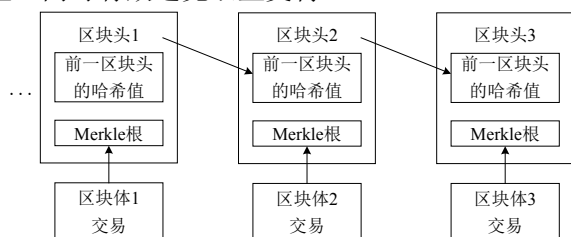


图1 区块链基本结构

Fig. 1 Blockchain structure

区块链去中心化的特点与微电网中 DG 和负荷分布式的分布特点天然对应,并且微电网的阻塞管理一般存在跨区域交易中,对于本文研究的微电网内部交易可忽略阻塞管理问题。因而区块链中 P2P 的交易方式恰好适应了微电网直接电能交易的要求。区块链中数据不可篡改、高度透明和可追溯的特性又进一步保障微电网交易的安全性和可靠性。

1.2 UTXO 模型

交易是区块链最核心的内容,传统的线上交易通过银行、支付宝等第三方实现,而区块链中的交易基于未消费输出模型(unspent transaction out, UTXO)模型,每一笔交易都包含输入和输出,输入交代了交易对象的来源必须是先前的交易中未曾使用的某个交易输出,输出则是将交易对象转移到新的地址。UTXO 模型使得区块链中的节点能够追踪任意一笔交易对象来源,判断支出方是否有权将其花费。

交易脚本是运行在区块链系统工作控制语言,根据支付给对象的不同,可以分为支付给公钥的哈希值(pay to public key hash, P2PKH)脚本和支付给脚本哈希值(pay to script hash, P2SH)脚本^[23]。P2PKH 脚本是最常见的一种交易脚本,目前比特币网络中大部分交易都是以 P2PKH 的方式进行的,在交易过程中,发送方将自己的 UTXO 使用输出脚本进行锁定,锁定在接收方的地址上(即接收方公钥哈希值),接收方通过输入脚本进行解锁,证明自己是这个地址的主人,各节点才认可这笔交易。以下是 P2PKH 的输入脚本(scriptSig)和输出脚本(scriptPubKey):

```

{scriptSig: < sig > < pubKey >;
 scriptPubKey: OP_DUP OP_HASH160<pubKey (1)
 Hash> OP_EQUALVERIFY OP_CHECKSIG;

```

式中: <sig>表示签名; <pubKey>表示公钥。

区块链中脚本的执行基于堆栈语言,并且采用数据指令和工作码指令进行计算。数据指令的作用

是把数据推到堆栈的最上面;工作码指令则通常是用堆栈顶部的数据作为输入值,用来计算一个函数。上述脚本中输入脚本指令和输出脚本中 <pubKeyHash>指令属于数据指令,其余输出脚本指令属于工作码指令。数据指令的作用是把数据堆到堆栈的顶部,工作码指令则是用堆栈顶部的数据作为一个输入值,计算一个函数。脚本执行过程如图2所示。

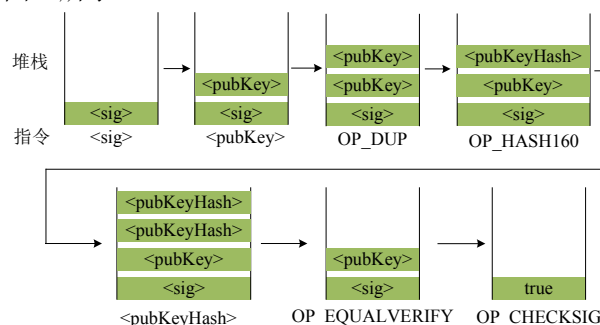


图2 脚本执行过程

Fig. 2 Script execution process

1) 数据指令<sig>和<pubKey>分别存入堆栈中,复制指令 OP_DUP 对堆栈顶层的公钥进行复制,并置于堆栈的最上层;

2) 利用 OP_HASH160 指令取堆栈顶层数据,并进行两次哈希计算。当该指令执行后,堆栈顶部的公钥变为公钥的哈希值,计算公式如下:

$$\text{pubKeyhash} = \text{RIPEMD160}(\text{SHA256}(\text{pubKey})) \quad (2)$$

式中:SHA256 和 RIPEMD160 分别是将数据转化为 256 位和 160 位的哈希函数。

3) 执行<pubKeyHash>数据指令,置于堆栈的最顶层;

4) 执行 OP_EQUALVERIFY 指令,如果发送方输出脚本中的公钥哈希值与接收方输入脚本中公钥哈希值相等,则移除堆栈顶部的两个数据,并执行下一个指令,否则返回一个失败信号,并停止执行。

5) OP_CHECKSIG 指令对堆栈中剩下的公钥和私钥验证,证明该公钥与接收方的私钥匹配,接收方获得该资产的所有权。

P2SH 允许发送方将交易发送到一个脚本哈希值,在处理多重签名交易时,发送方不需要输入多个公钥。P2SH 脚本结构如下所示:

```

{sigScript: < sig > [sig] [sig...] < redeemScript >
 pubkeyScript: OP_HASH160
 < redeemScriptHash > OP_EQUAL

```

式中:redeemScript 称为赎回脚本,接收方通过赎

回脚本和签名来获得资产的使用权；*redeemScript Hash* 为赎回脚本的哈希值，计算方法与式(2)类似。

当采用多重签名时，赎回脚本为：

$$\begin{cases} \text{redeemScript} = \text{OP_m} < \text{pubKeyA} > \\ < \text{pubKeyB} > < \text{pubKeyC} \dots > \text{OP_n} \\ \text{OP_CHECKMULTISIG} \end{cases} \quad (4)$$

该多重签名脚本表示 n 个公钥中至少有 m 个对应的数字签名，这笔交易才算成功。P2SH 脚本一方面让发送方的支付工作简单化，接收方只需要告诉支付方一个哈希值即可；另一方面采用 P2SH 的输出脚本很小，有利于区块链中的节点追踪未被消费的输出脚本。

2 连续双向拍卖机制

市场交易机制规定市场交易主体、交易时间、价格机制以及市场信息披露方式等内容。本文提出的微电网电力市场允许拥有 DG 的生产消费者、独立 DG 运营商和普通用户通过连续双向拍卖机制参与市场交易。考虑到可再生能源出力和负荷预测准确度，交易周期假设为 1h。连续双向拍卖是指在市场参与者以多对多形式存在的情况下，买卖双方在交易周期内可以随时提交报价，一旦价格匹配即可成交的交易形式。在连续双向拍卖机制中，买卖双方按照“价格优先，时间优先”的原则进行排序，买方价格从高到低排序，而卖方价格从低到高排序，价格相同的情况下，按提交报价时间前后排序。

连续双向拍卖机制下买卖双方匹配过程如图 3 所示，买方最高报价称为最优买价，卖方最低报价称为最优卖价。当最优买价大于等于最优卖价时，即可发生交易，在匹配过程中，报价最高的买方与报价最低的卖方进行匹配，成交价为二者平均价。依次类推，直到最优买价低于最优卖价，此时称为

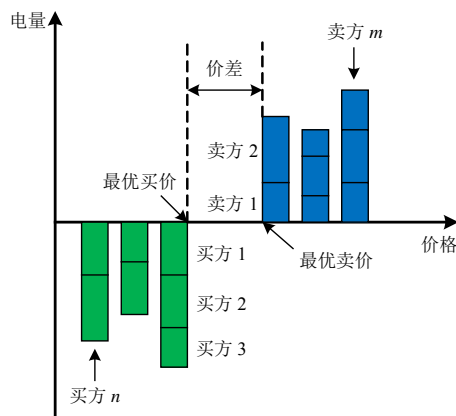


图 3 连续双向拍卖机制匹配过程

Fig. 3 Matching process of continuous double auction

完成一轮交易，每轮交易中至少存在一笔交易。在交易过程中，市场参与方可以查看最优买价、最优卖价以及成交价，然后根据市场信息运用报价策略不断调整自身报价进行下一轮交易，直到市场中的交易电量全部匹配完成或者交易时间截止。如果市场中买卖双方交易截止时，还未完成匹配，则向大电网购电或售电。

3 基于区块链和连续双向拍卖机制的微电网交易模式及策略

3.1 总体架构

微电网电力交易通过连续双向拍卖市场实现买卖双方电量和价格匹配，并通过区块链技术实现交易结算，总体架构如图 4 所示。微电网电力市场中存在多个 DG 和用户，在每个交易周期内，DG 和用户分别向连续双向拍卖市场提交报价和交易电量，市场根据双方报价自动进行匹配。在匹配过程中，市场不断对外公布交易信息，包括成交价、当前最优卖价、最优买价信息，以及未完成匹配的 DG 和用户通过代理系统依据一定的报价策略调整报价。而完成匹配的交易双方通过区块链进行结算，DG 通过区块链向与其交易的用户转移电量数字证明，而用户通过区块链向与其交易的 DG 转移购电费用。待全网中各节点确认后，即可认为买卖双方交易成功。交易过程中，交易双方通过公有链进行交易，仍然可以采用工作量证明机制对交易进行确认并记录到区块中。

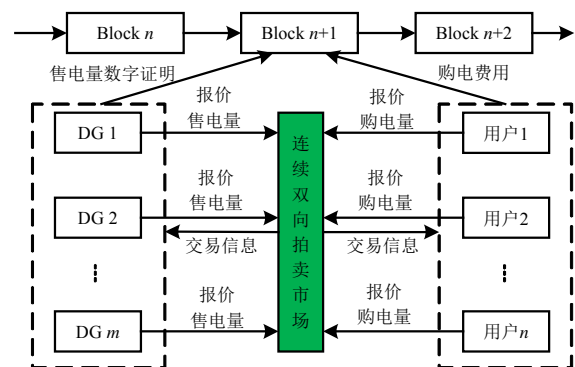


图 4 微电网电力交易总体架构

Fig. 4 Overall architecture of microgrid electricity transactions

3.2 微电网电力市场中 AA 交易策略

AA 策略通过短期和长期学习机制根据市场信息自动调整报价，然后通过多代理系统自动向市场提交报价。AA 策略主要由竞争性均衡价格估计、进取性模型、近期和远期自适应学习组成。

1) 竞争性均衡价格估计。

市场竞争性均衡指的是以完全竞争为特征的市场或经济中供给和需求的平衡。由于微电网电力市场中存在多个 DG 和用户, 并且双方都没有力量(支配性地)影响市场, 使得交易价格逐渐趋向于竞争性均衡价格。市场中均衡价格无法提前获取, 但可以通过计算最近 n 笔历史交易的成交价加权移动平均数估计均衡价格, 即:

$$p' = \sum_{i=m-n}^n (\omega_i \cdot p_i) \quad (5)$$

式中: p_i 表示第 i 笔交易的成交价; ω_i 表示第 i 笔交易的权重, 根据序关系分析法^[24]求解。

2) 进取性模型。

进取性反映了市场主体参与市场竞争意愿强烈程度。如果用户(或 DG)竞价成功意愿强烈, 则其会主动提高(或降低)目标报价, 相反则会主动降低(或提高)目标报价, 但会增加收益。根据用户购电估价(即可承受的最高购电价格)和 DG 成本与均衡价格估计值关系, 分为内缘买方或卖方和外缘买方或卖方。当用户购电估价高于均衡价格时, 该用户即为内缘买方, 否则为外缘买方; 当 DG 成本低于均衡价格时, 该 DG 即为内缘卖方, 否则为外缘卖方。

进取度 r 是反映进取性强烈程度的参数, r 为 $[-1, 1]$ 的实数, r 越接近于 1, 则市场主体竞价的愿望越强烈, r 越接近于 -1, 则市场主体竞价的愿望越消极, r 等于 0 时表明市场主体对交易持中立的态度。内缘交易方和外缘交易方目标价格与进取度变化规律^[21]如图 5 所示。

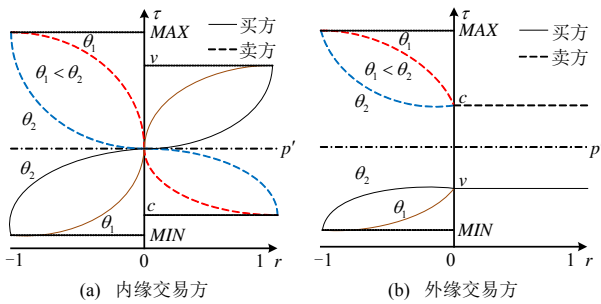


图5 目标价格与进取度关系曲线

Fig. 5 Relationship of target price and aggressiveness degree

从图 5 可以看出, 随着进取度不断接近于 1, 用户的目标价格不断增加, 而 DG 的目标价格不断提高, 从而增加成交的概率。应当注意到, 对于外缘买方来说, 由于最高限价低于均衡价格, 即使当进取度大于 0, 目标价格也不能高于均衡价格, 因此将其设为常数, 即最高限价 v 。类似的, 外缘卖方在进取度大于 0 时, 目标价格为成本 c 。此外,

目标报价曲线变化规律还受到参数 θ 影响, 当 θ 越小时, $r=0$ 附近的目标报价变化较快, 反之则变化较慢。 θ 取值受市场价格波动影响, 当市场价格波动幅度较大时, 代理通过减小 θ 使得目标价格快速收敛到均衡价格附近; 当市场价格波动幅度较小时, 则收敛速度可适当减慢。

不同用户和 DG 的目标价格可分别表示为

$$\tau_{in,b} = \begin{cases} (p' - MIN)(1 - \frac{e^{-r\theta} - 1}{e^\theta - 1}) + MIN, & r \in (-1, 0) \\ p' + (v - p') \frac{e^{r\theta} - 1}{e^\theta - 1}, & r \in (0, 1) \end{cases} \quad (6)$$

$$\tau_{in,s} = \begin{cases} p' + (MAX - p') \frac{e^{-r\theta} - 1}{e^\theta - 1}, & r \in (-1, 0) \\ c + (p' - c)(1 - \frac{e^{r\theta} - 1}{e^\theta - 1}), & r \in (0, 1) \end{cases} \quad (7)$$

$$\tau_{ex,b} = \begin{cases} (v - MIN)(1 - \frac{e^{-r\theta} - 1}{e^\theta - 1}) + MIN, & r \in (-1, 0) \\ v, & r \in (0, 1) \end{cases} \quad (8)$$

$$\tau_{ex,s} = \begin{cases} c + (MAX - c)(\frac{e^{-r\theta} - 1}{e^\theta - 1}), & r \in (-1, 0) \\ c, & r \in (0, 1) \end{cases} \quad (9)$$

式中: $\tau_{in,b}$ 、 $\tau_{in,s}$ 、 $\tau_{ex,b}$ 和 $\tau_{ex,s}$ 分别为内缘买方、内缘卖方、外缘买方和外缘卖方目标报价; v 、 c 分别是用户和 DG 的购电估价和成本; MIN 、 MAX 分别是市场规定最低购电价和最高售电价格。

3) 自适应学习过程。

自适应学习过程是交易双方根据市场信息调整进取度 r 以及参数 θ , 分别通过短期学习和长期学习调整。

短期学习可表示为

$$\begin{cases} r(t+1) = r(t) + \beta_1 [\delta(t) - r(t)] \\ \delta(t) = (1 + \lambda) r_{shout}(t) \\ \lambda = \{-0.05, 0.05\} \end{cases} \quad (10)$$

式中: $r(t)$ 表示 t 轮交易的进取度; $\delta(t)$ 为 t 轮交易理想进取度, 表示用户报价位于最优买价附近或 DG 报价位于最优卖价附近对应的进取度; $r_{shout}(t)$ 表示 t 轮交易最优报价对应的进取度, 当该代理 t 轮交易中未成交时, t 轮交易最优报价为成交价, 当该代理为用户(或 DG)并在 t 轮交易成交, 则最优报价为 t 轮购电价(或售电价); λ 为理想进度因子, 当 $\lambda = -0.05$, 表示该代理通过减小进取度, 提高自身收益, 当 $\lambda = 0.05$, 表示该代理通过增加进取度, 提高交易成功概率; $\beta_1 \in (0, 1)$ 表示短期学习速度。

当用户的目标价格大于成交价或上一轮购电价(如果交易成功)时,用户代理需要减小进取度,否则增加进取度;当 DG 的目标价格小于成交价或上一轮售电价(如果交易成功)时,DG 代理需要减小进取度,否则增加进取度。

长期学习可表示为

$$\begin{cases} \theta(t+1) = \theta(t) + \beta_2[\theta'(\alpha) - \theta(t)] \\ \alpha = \frac{\sqrt{\frac{1}{n} \sum_{i=m-n+1}^n (p_i - p')^2}}{p'} \end{cases} \quad (11)$$

式中: α 为近期轮 n 笔交易成交价标准差的归一化值,反映了市场价格波动情况; $\beta_2 \in (0,1)$ 为远期学习速度; $\theta'(\alpha)$ 是一个关于 α 的函数,可以通过市场历史成交价格波动情况找到最优的 $\theta(t+1)$, 函数关系式可表示为

$$\theta'(\alpha) = (\theta_{\max} - \theta_{\min}) \left(1 - \frac{\alpha - \alpha_{\min}}{\alpha_{\max} - \alpha_{\min}}\right)^{2\left(\frac{\alpha - \alpha_{\min}}{\alpha_{\max} - \alpha_{\min}} - 1\right)} + \theta_{\min} \quad (12)$$

式中: θ_{\min} 和 θ_{\max} 分别为 θ 的限值; α_{\min} 和 α_{\max} 分别为 α 的最小值和最大值。

4) 报价策略。

如果交易双方报价完全遵循目标报价,没有根据当前市场信息进行价格调整,有可能造成电力市场中不发生任何交易。因此在每一轮交易成交之前,交易双方根据当前最优买价、最优卖价信息,逐渐调整报价直到交易成功。

用户报价策略如下式所示:

$$p_b(t) = \begin{cases} p_{Obid}(t) + \eta[\min\{v_i, p_{Oask}(t)\} - p_{Obid}(t)], t=1 \\ p_{Obid}(t) + \eta[\tau_b(t) - p_{Obid}(t)], t \geq 2 \end{cases} \quad (13)$$

式中: $\eta \in (0,1]$ 表示用户报价增加率; $p_{Obid}(t)$ 和 $p_{Oask}(t)$ 分别为 t 轮交易中最优买价和最优卖价。在第 1 轮交易中,由于市场中没有成交价信息,因此无法根据市场信息确定目标报价,用户只能根据当前市场中最优买价、最优买价信息适当增加自身报价;在随后的交易中,如果市场中买卖双方还未成交,则用户根据目标报价和当前最优卖价,适当增加自身报价。

DG 报价策略:

$$p_s(t) = \begin{cases} p_{Oask}(t) - \eta[p_{Oask}(t) - \max\{c_j, p_{Obid}(t)\}], t=1 \\ p_{Oask}(t) - \eta[p_{Oask}(t) - \tau_s(t)], t \geq 2 \end{cases} \quad (14)$$

DG 报价策略具体原理可参考用户报价策略,

此处不再赘述。

5) 平衡机制。

考虑到负荷和 DG 出力预测不可能完全准确,在微电网市场交易关闭后,由于预测误差引起的电能缺额或多余部分,负荷和 DG 分别与大电网交易结算。

对于负荷来说,当负荷实际消耗电能小于交易电量时,则不对其退款补偿,相当于多余的电量由电源出售给电网;当负荷实际消耗电能多于交易电量时,则负荷需要从电网购电以弥补自身过多电能消耗。即考虑预测误差时负荷实际支出 F_{actual} 为

$$F_{\text{actual}} = \begin{cases} \bar{p}_b \cdot W, \Delta W < 0 \\ \bar{p}_b \cdot W + p_{b_grid} \cdot \Delta W, \Delta W > 0 \end{cases} \quad (15)$$

式中: \bar{p}_b 为市场交易平均购电价; W 为总购电量; ΔW 为负荷预测误差, $\Delta W < 0$ 表示负荷实际消耗电能小于预测值, $\Delta W > 0$ 表示负荷实际消耗电能大于预测值; p_{b_grid} 为向电网购电价格。

当负荷预测完全准确时,市场交易等量电能的期望支出 F_E 为

$$F_E = \bar{p}_b \cdot (W + \Delta W) \quad (16)$$

对于 DG 来说,当 DG 实际发出电量多余交易电量时,则其自身与电网交易多余电量;而当 DG 实际发出电量小于交易电量时,则需要从电网购买差额电量以弥补自身出力不足。即考虑预测误差时 DG 实际收益 G_{actual} 为

$$G_{\text{actual}} = \begin{cases} \bar{p}_s \cdot Q + p_{b_grid} \cdot \Delta Q, \Delta Q < 0 \\ \bar{p}_s \cdot Q + p_{s_grid} \cdot \Delta Q, \Delta Q > 0 \end{cases} \quad (17)$$

式中: \bar{p}_s 为市场交易平均售电价; Q 为总售电量; ΔQ 为 DG 预测误差, $\Delta Q < 0$ 表示 DG 实际发出电能小于预测值, $\Delta Q > 0$ 表示 DG 实际发出电能大于预测值; p_{s_grid} 为向电网售电价格。

当 DG 出力预测完全准确时,市场交易等量电能的期望收益 G_E 为

$$G_E = \bar{p}_s \cdot (Q + \Delta Q) \quad (18)$$

3.3 微电网交易结算原理

微电网中用户与 DG 完成交易匹配之后,通过区块链完成购电费用以及售电量数字证明的交换。本文微电网的交易结算基于比特币协议,用户通过比特币与 DG 进行交易,而 DG 利用代币制度实现电能资产的转移。所谓代币实际上是电力能源在区块链系统中的证明,用以表示交易电能数量。在物理世界中,用户向能源销售商支付一定的物理货

币, 签署协议或者获得 IC 卡来证明对一定量能源的所有权。由于区块链网络中的交易对象只能是比特币, 为了实现物理资产在区块链网络中的交易, 可通过对比特币添加标记从而与普通的比特币区分, 作为物理资产的数字证明, 这种特定的比特币叫彩色币(colored coins)^[25]。彩色币本身就是比特币, 其利用少量的比特币实现电能资产在区块链上的数字记录, 并且存储和转移不需要通过第三方, 可以利用已经存在的比特币基础, 因此彩色币可以为现实世界中难以通过传统方法去中心化的事物铺平道路。

DG 通过将彩色币嵌入区块链网络当中, 用于区块链中点对点交易。DG 向用户转移与交易电量成正比的彩色币, 而用户转移相应的交易费用。DG 在收到用户支付的比特币之后, 可能不向用户转移代币或者由于系统故障等因素不能向用户供电, 造成用户损失。为了避免这一弊端, 本文引入保证金和违约机制, 用户和 DG 采用多重签名分别将交易费用和保证金支付给赎回脚本。多重签名交易只有双方共同签名才能生效, 并且在交易双方发生分歧时, 通过第三方仲裁保证双方的利益。由于仲裁方只在买卖双方发生分歧时才会介入, 因此并不影响去中心化电量直接交易的本质。通过多重签名机制结算的具体过程如下:

1) 发行彩色币: 在完成匹配之后, DG 在区块链网络中发行一个与自身交易电量成正比的彩色币, 作为交易脚本中输入的来源;

2) 转移比特币: DG 向用户发送一个包含 DG、用户以及第三方公钥的赎回脚本, 与该 DG 达成交易的用户创建一个普通比特币转移交易, 输入: 上一笔交易未花费的输出, 输出: 将该笔交易转移到赎回脚本中, 并附上数字签名; 同理, DG 也向该赎回脚本创建一个普通比特币转移交易, 作为交易保证金, 假设保证金为交易费用的 20%。

3) 转移彩色币: DG 在用户完成比特币转移之后, 创建一个交易, 输入: 指向(1)发行的彩色币, 输出: 将彩色币转移到用户公钥, 并附上数字签名, 此时即认为双方交易达成。

由于 DG 要想获得该赎回脚本地址中比特币的使用权, 需要三方中任意两方签名, 这样能够保证在 DG 违约时, 用户能够通过第三方仲裁保证合法的权益。

3.4 电能资产的数字证明

通过设定交易输入脚本中的序列号对该交易

的比特币进行标记是一种生成彩色币常用的方法^[26]。序列号(*Sequence_N*)是输入脚本中 32 位的字符, 将最后 6 位作为交易类型标签 *Tag_Tx*。定义 *Tag_Tx*=110011 为彩色币转移交易, *Tag_Tx*=100101 为彩色币发行交易, 十六进制值分别为 0x33 和 0x25, 除此之外为普通比特币交易。交易类型标签提取方法为

$$Tag_Tx = Sequence_N \& 0x3F \quad (19)$$

式中: & 表示按位与运算。当 *Tag_Tx*=0x25, 交易类型为彩色币发行交易; 当 *Tag_Tx*=0x33, 交易类型为彩色币转移交易; 如果两者都不是, 交易类型为普通比特币交易。

由于彩色币只作为电能交易的证明, 其实际比特币额度无需太高, 但是考虑到比特币交易规则对比特币最低交易额有一定要求, 并且可能改变。因此引入填充变量以满足要求, 如下所示:

$$Value = Padding + Ve \quad (20)$$

式中: *Value* 为输出脚本中比特币值; *Padding* 为填充变量; *Ve* 为彩色币实际值。

与交易类型标记方法类似, 填充变量值大小由序列号第 7 位到 12 位字符计算得到, 方法如下:

1) 提取序列号第 7 位至 12 位:

$$Padding_N = Sequence_N \& 0x0FC0 \quad (21)$$

2) 计算填充变量值:

$$Padding = 2^{Padding_N} \quad (22)$$

用户依据收到的比特币值以及输入脚本的序列号, 根据式(20)–(22)计算收到的彩色币数量, 以此作为购电量的证明, 由此完成电力能源资产的数字化。

卖方向买方转移彩色币过程中, 由此带来少量交易成本, 买方在支付比特币时应退回该部分的成本。即买方实际转移比特币数量为

$$C = p \cdot n + Paddiing \quad (23)$$

式中: *p* 为买卖双方成交价; *n* 为买卖双方交易量; *C* 为买方实际转移比特币数量。

4 应用场景分析

4.1 参数设置

假设某个微电网中存在 8 个用户和 6 个 DG, 各用户和 DG 的交易电量以及报价参数如表 1 所示。

4.2 微电网交易结果分析

根据前述交易策略及参数设定, 利用 MATLAB

表 1 用户和 DG 交易参数

Tab. 1 Transaction parameters of user's and DG's

类型	交易电量/Unit	MIN/Satoshi Unit ⁻¹	v/Satoshi Unit ⁻¹
用户 1	4	5000	15000
用户 2	2	5000	14000
用户 3	3	5000	13000
用户 4	5	5000	13000
用户 5	3	5000	17000
用户 6	3	5000	15000
用户 7	6	5000	14000
用户 8	2	5000	15000
类型	交易电量/Unit	c/Satoshi Unit ⁻¹	MAX/Satoshi Unit ⁻¹
DG 1	5	6000	16000
DG 2	5	4500	16000
DG 3	4	4000	16000
DG 4	7	5000	16000
DG 5	4	6500	16000
DG 6	5	8000	16000

注：Unit 为交易单元，1Unit=10kWh；Satoshi 为比特币最小单位，1BTC=10⁸Satoshi(微电网交易中也可以用其他数字货币代替)。

仿真分析，仿真程序在 CPU i5-7500，内存 8GB 的计算机上运行。在测试过程中，设定买卖双方报价时间为 0~1s 范围内随机数(连续双向拍卖市场中，交易双方通过代理自动报价，时间极短^[27])。成交价及成交量变化过程如图 6 所示。

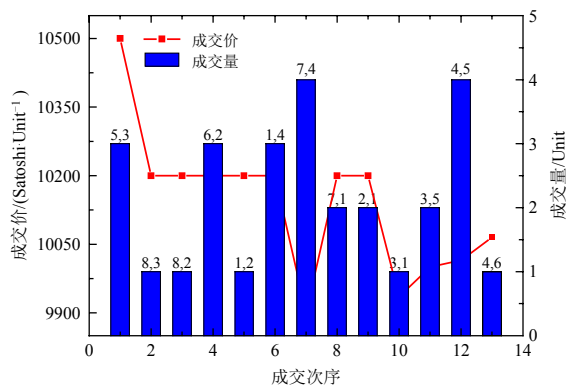


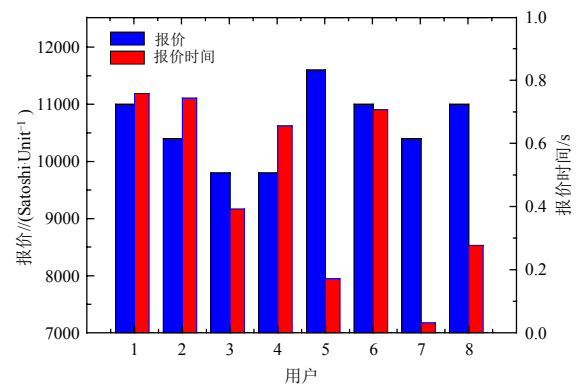
图 6 微电网交易成交价和成交量变化曲线

Fig. 6 Transaction price and volume curve in microgrid transaction

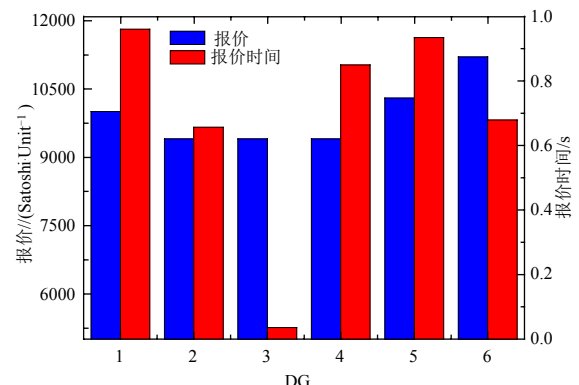
在整个交易周期中，交易双方总共完成了 13 笔交易，交易轮数为 5 轮。成交次序与交易轮次对应关系为(1-9, 1)、(10, 2)、(11, 3)、(12, 4)和(13, 5)。从图 6 可以看出，第 1 轮成交的有用户 5、用户 8、用户 6、用户 1、用户 7、用户 2 和 DG 3、DG 2、DG 4、DG 1(柱状图上方数字表示发生交易的用户和 DG 序号)。这是由于这些用户估价较高，在交易期间报价较高，而这些 DG 的成本较低，在交易期间报价较低，故而能够第 1 轮交易中成交。用户 4

估价最低和 DG 6 成本最高，因而直到最后 1 轮才完成交易。

交易过程中，买卖双方匹配的顺序受到自身报价和报价时间的影响，图 7 为第 1 轮用户和 DG 的报价以及报价时间。由图 7(a)可知，由于用户 5 估价最高，因此其报价也最高，相反用户 3 和用户 4 的报价最低。同理，DG 3 成本最低，因而报价最低。根据图 6 和图 7，虽然用户 6 和用户 8 第 1 轮报价相同，但是用户 8 报价时间早于用户 6 报价时间，因而用户 8 成交次序早于用户 6。同理 DG 2、DG 3 和 DG 4 报价相同，由于 DG 3 最早报价，因此 DG 3 最先匹配成功。



(a) 用户报价及报价时间



(b) DG报价及报价时间

图 7 用户和 DG 报价及报价时间

Fig. 7 Quotation and time of consumer and DG

为进一步分析交易过程中，市场参与方调整报价的过程。以用户 4 交易过程为例，每 1 轮交易均衡价格估计、短期学习和长期学习结果如图 8 所示。

从图 6 和图 8(a)、(b)可以看出，用户 4 在第 1 轮未发生交易，在第 2 轮交易时，根据第 1 轮均衡估计价格小于成交价得到 r_{shout} 为正，因此必须通过增加进取取值从而增大交易成功的概率，后续 3 轮竞价采取类似手段。并且从图 8(b)可以发现用户 4 在第 4 轮交易成功后，并没有调整自身的进取度，这与式(10)表达的含义一致。而由图 8(c)可以得到，

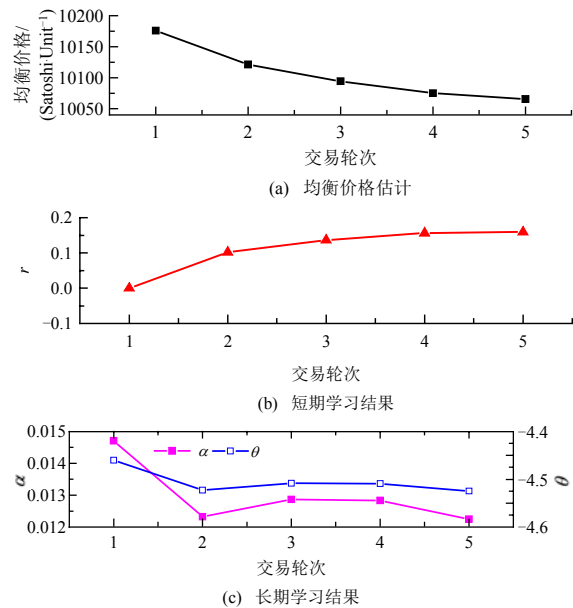


图 8 均衡价格估计、短期学习和长期学习结果

Fig. 8 Equilibrium price estimation, short-term learning and long-term learning outcomes

由于第 1 轮价格波动大于第 2 轮价格波动，所以第 2 轮 θ 的值应小于第 3 轮 θ 的值，这是因为价格波动越大，此时用户需要更加快速调整自身目标报价。

4.3 预测误差对用户支出和 DG 收益的影响

在实际中，负荷和 DG 出力预测必然存在误差。以负荷 1 和 DG 1 为例，不考虑预测误差时，平均交易价格分别为 $\bar{p}_b=10200\text{Satoshi/Unit}$ 和 $\bar{p}_s=10147\text{Satoshi/Unit}$ ，且 $p_{s_grid}=6000\text{Satoshi/Unit}$ ， $p_{b_grid}=18000\text{Satoshi/Unit}$ ，当预测误差分别为 $\pm 1\text{Unit}$ 时，则考虑预测误差时交易双方支出和收益如表 2 所示。

从表 2 可知，由于电网售电价格高于微电网市场成交价，而电网购电价格低于微电网市场成交价，当用户实际消耗电能少于预测值，由于不能退款，相当于在交易时多支出 $|\Delta W|\cdot\bar{p}_b=10200\text{ Satoshi}$ ；当用户实际消耗电能多于预测值，由于电网售电价格高于微电网市场成交价，则实际支出 F_{actual} 比市场交易期望支出 F_E 多 $|\Delta W|\cdot(p_{b_grid}-\bar{p}_b)=7800\text{Satoshi}$ 。当 DG 实际发电量少于预测值，则需要从电网购买电能弥补自身出力的不足，而电网售电价偏高，

表 2 考虑预测误差时用户支出和 DG 收益

Tab. 2 Expenditure and profits considering forecasting error

类型	$\Delta W/\text{Unit}$	$F_E/\text{Satoshi}$	$F_{\text{actual}}/\text{Satoshi}$	经济损失/Satoshi
用户	-1	30600	40800	10200
	1	51000	58800	7800
类型	$\Delta Q/\text{Unit}$	$G_E/\text{Satoshi}$	$G_{\text{actual}}/\text{Satoshi}$	经济损失/Satoshi
DG	-1	40588	32735	7853
	1	60882	56735	4147

因而造成自身收益减少了 $|\Delta Q|\cdot(p_{b_grid}-\bar{p}_s)=7853\text{Satoshi}$ ；当 DG 实际发电量多于预测值，由于电网购电价格偏低，多余的部分只能以较低的价格卖出，因此收益比市场交易期望收益低 $|\Delta Q|\cdot(\bar{p}_s-p_{b_grid})=4147\text{Satoshi}$ 。

为进一步分析预测误差大小对用户和 DG 支出收益的影响，图 9 为不同预测误差下用户和 DG 的经济损失。

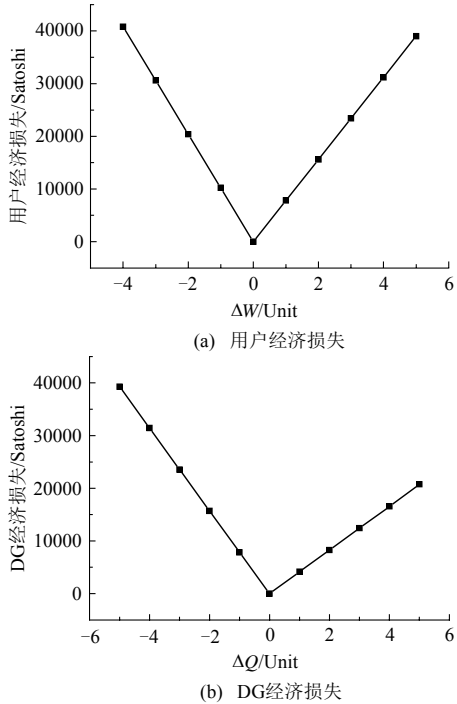


图 9 不同预测误差下用户和 DG 经济损失

Fig. 9 Economic loss of consumer and DG under different forecasting error

从图 9 可以看出，用户和 DG 的经济损失与预测误差的绝对值成正比，并结合式(15)—(18)和上文可得，用户经济损失变化曲线的斜率分别为 $10200\text{Satoshi/Unit}(\Delta W<0)$ 和 $7800\text{Satoshi/Unit}(\Delta W>0)$ ；DG 经济损失变化曲线的斜率分别为 $7853\text{Satoshi/Unit}(\Delta Q<0)$ 和 $4147\text{Satoshi/Unit}(\Delta Q>0)$ 。显然负荷和 DG 出力预测值比实际值偏小或偏大都会给交易方带来一定的经济损失，并且预测误差越大，经济损失也越大。因此，交易双方为了保障自身收益，必须提高负荷和 DG 出力预测的准确度。

4.4 微电网交易适应性及时效性分析

为了分析微电网中不同交易主体数量对交易策略适应性和时效性，以 4.1 节中交易主体数量为基准，当交易主体数量为基准 k 倍时，交易轮数和时间(程序计算时间加上交易随机设定时间)随 k 的变化规律如图 10 所示。

从图 10 可以看出，随着交易主体规模的增加，

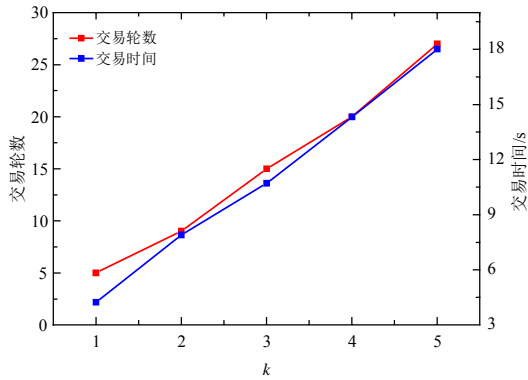


图 10 不同交易主体数量下交易轮数和时间变化规律

Fig. 10 variation of transaction round and time under different quantity of transaction parities

交易轮数和时间均增加。当 $k=1$ 时, 需要 5 轮完成交易匹配, 而当 $k=5$ 时, 交易轮数增加到 27 轮。尽管交易轮数显著增加, 但是交易时间仍是秒级, 主要是因为交易双方跟随交易市场交易信息, 通过程序自动调整报价, 因此交易时间很短。故可以认为本文的交易策略能够适应不同规模微电网交易, 并且交易时间完全满足 1h 前交易周期要求。

4.5 微电网交易结算流程分析

用户与 DG 完成匹配后, 基于交易的电量和价格, 通过区块链完成交易结算。以用户 5 与 DG 3 的交易为例, 成交电量为 3 Unit, 成交价为 10500Satoshi/Unit, 结算过程如下:

1) DG 3 创建发行彩色币交易。

匹配完成之后 DG 3(用 A 代替)创建一笔发行彩色币的交易, 设置序列号后六位交易类型标签为 $Tag_Tx=100101$ 。定义 100Satoshi 彩色币表示 1 Unit 电能。因此 DG 3 应发行 300Satoshi 彩色币, 而比特币系统目前最小交易额为 546Satoshi。由式(9)可知, 填充变量 $Padding \geq 246Satoshi$, 结合式(10)满足要求的最小填充变量 $Padding=256Satoshi$, 此时序列号第 7 位至 12 位为 $Padding_N=0x08=001000$, 故序列号可设置为 $Sequence_N=1000100101=0x225$, 输出比特币 $Value=556Satoshi$ 。根据以上结果, 彩色币发行交易如附录表 A1 所示。

2) 用户 5 创建多重签名转移交易。

用户 5(用 B 代替)在与 A 沟通好之后, 通过区块链网络向 A 发送一定数量的比特币。为保证自身的财产安全, B 要求必须使用多重签名, 并引入双方共同信任的第三方 C 作为担保人, 这笔交易必须有三人当中的两个人签名才能生效。A 向 B 发送一个多重签名脚本 $redeemScript=OP_2<pubKeyA><pubKeyB><pubKeyC>OP_3OP_CHECKMULTISIG$

以保证双方公钥都包含在里面, 然后将脚本哈希运算, 并将该哈希值编入到输出脚本中。用户 5 向该脚本哈希支付交易费用 31500Satoshi 和彩色币成本 556Satoshi, 即 32056Satoshi。转移交易如附录表 A2 所示。

同时, DG 3 也需要向该赎回脚本转移保证金 6300Satoshi, 转移过程与附录表 A2 类似。用户 5 支付完比特币之后, 如果 DG 3 违约, 并且用户 5 与 DG 3 在赔偿问题上不能达成一致, 此时双方找第三方 C 进行仲裁。假设仲裁方 C 判定 DG 3 需要向用户 5 支付 30%的退款, DG 3 收取 70%的比特币, 其违约保证金转移给用户 5。待双方认可后, 仲裁方 C 创建一笔双输入双输出的退款交易如附录 A 表 A3 所示。C 用自己的数字签名和 A、B 中任一数字签名验证用户 5 转移交易和 DG 3 保证金交易输出, 将地址 $Hash160(redeemScript)$ 的比特币分别转移给用户 5 和 DG 3 的公钥哈希值。

3) DG 2 创建彩色币转移交易。

DG 2 在看到用户 5 支付比特币之后, 创建彩色币转移交易, 向用户 5 支付 300 Satoshi 的彩色币。转移过程与发行过程类似, 只是在序列号上要添加彩色币转移交易标记。

买卖双方创建交易之后, 将交易单广播到区块链网络中, 网络中每个节点都会收到交易信息并纳入到一个区块中。公有链中, 每个节点通过工作量证明寻求对该区块的管理权, 最先完成的节点向全网广播该区块记录的交易。待网络中其他节点核对该区块记账的正确性之后, 将该区块添加到区块链中, 由此完成 DG 与用户直接交易结算。

4.6 交易模型比较分析

本文从社会福利^[28]和市场效率^[29]两个方面比较本文交易模型和传统交易模型的优劣。假设用户和 DG 的总购电量和售电量均为 50Unit, 用户购电估价 $v \sim U(8000, 16000)$, DG 成本 $c \sim U(4000, 10000)$ 。分别利用本文交易模型和文献[30]的交易模型进行 30 次仿真测试。社会福利和市场效率的测试结果如图 11 所示。

从图 11 可以看出, 本文提出的交易模型在社会福利和市场效率两个方面均优于文献[30]提出的交易模型。根据经济学原理, 当市场成交价格等于均衡价格时, 此时社会福利最大。本文提出的交易模型能够根据市场成交价估计市场均衡价格, 从而调整报价, 而文献[30]中的交易模型是基于暗标拍卖, 买卖双方无法根据市场价格调整报价, 买卖双

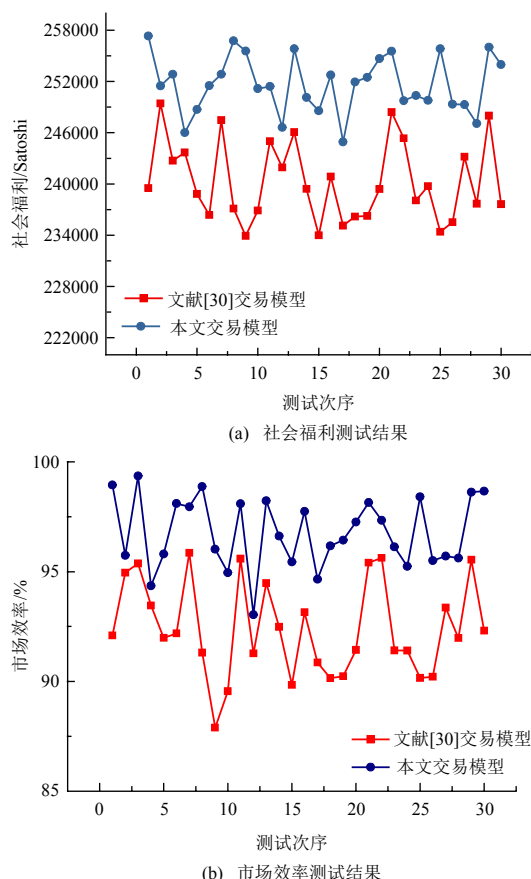


图 11 不同交易模型下的社会福利和市场效率

Fig. 11 Social welfare and market efficiency under different transaction models

方都是朝着自身收益最大化的报价,因此该交易模型的社会福利低于本文提出的交易模型。市场效率是实际社会福利与最大社会福利的比值,而本文测试数据样本为均匀分布随机数,每次测试的最大社会福利差别较小,因而本文交易模型的市场效率也优于文献[30]的交易模型,并且图 11(b)曲线的变化趋势与图 11(a)的变化趋势相似。

此外,传统交易模型依赖于第三方交易机构,而本文提出交易模型实现了用户和 DG 点对点交易(本文交易模型中的第三方只处理买卖双方争议,去中心化的性质没有改变),正好对应于微电网中电源和用户在空间上呈现分布式的特点。在传统交易模式下,交易数据存储于中心化服务器,交易数据不透明,面临被篡改风险,也不能够追溯。而区块链通过非对称加密技术、数据签名和共识机制保证了交易数据透明、不可篡改以及可追溯,很好地解决了以上问题。

5 结论

本文提出了基于区块链和连续双向拍卖机制的微电网内 DG 与用户直接电量交易模式及策略,

并通过微电网电力交易案例对所提方法进行验证。分析结果表明:1) 本文提出交易模型可用于微电网内部电力交易,在连续双向拍卖市场机制下,交易双方能够根据市场交易信息动态地调整报价,并且对于微电网交易具有很好的适应性;2) AA 交易策略能够自适应地跟踪市场信息,根据市场成交价和价格波动寻找最优报价;3) DG 与用户通过区块链实现了无需中心化机构参与的交易结算,并且多重签名机制能够保证买方的利益,避免卖方违约引起用户损失;4) 本文提出交易模型通过跟踪市场均衡价格调整报价,因而在社会福利和市场效率方面均优于传统的交易模型。该方法能够满足微电网分散式、小规模和低成本的交易需求,为新一轮电改下微电网电力市场建设提供参考。

参考文献

- [1] 中共中央国务院. 中共中央国务院关于进一步深化电力体制改革的若干意见(中发[2015]9号)[EB/OL]. [2015-03-15]. http://tgs.ndrc.gov.cn/zywj/201601/t20160129_773852.html.
CPC Central Committee and State Council. The CPC central committee and state council of the several opinions on further deepening the reform of electric power system[EB/OL]. [2015-03-15]. http://tgs.ndrc.gov.cn/zywj/201601/t20160129_773852.html(in Chinese).
- [2] 国家发展和改革委员会. 关于推进电力市场建设的实施意见[EB/OL]. [2015-11-30]. <http://www.gov.cn/xinwen/2015-11/30/5018221/files/87556b7e1f4f4aaab86ac7c99f5acf3f.pdf>.
National Development and Reform Commission. Suggestions on the implementation of the construction of electric power market[EB/OL]. [2015-11-30]. <http://www.gov.cn/xinwen/2015-11/30/5018221/files/87556b7e1f4f4aaab86ac7c99f5acf3f.pdf>(in Chinese).
- [3] 国家发展改革委, 国家能源局. 关于开展分布式发电市场化交易试点的通知[EB/OL]. [2017-10-31]. http://zfxgk.nea.gov.cn/auto87/201711/t20171113_3055.htm.
National Development and Reform Commission, National Energy Administration. Notice on the pilot of distributed generation market trading[EB/OL]. [2017-10-31]. http://zfxgk.nea.gov.cn/auto87/201711/t20171113_3055.htm(in Chinese).
- [4] 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, 37(13): 3682-3690.
Ping Jian, Chen Sijie, Zhang Ning, et al. Decentralized transactive mechanism in distribution network based on smart contract[J]. Proceedings of the CSEE, 2017, 37(13): 3682-3690.

- 3682-3690(in Chinese).
- [5] 邵雪, 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, 40(12): 3630-3638.
- Tai Xue, Sun Hongbin, Guo Qinglai. Electricity transactions and congestion management based on blockchain in energy internet[J]. Power System Technology, 2016, 40(12): 3630-3638(in Chinese).
- [6] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2009).<https://bitcoin.org/bitcoin.pdf>.
- [7] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
- Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese).
- [8] 工信部. 中国区块链技术和应用发展白皮书(2016)[EB/OL]. (2016-10-19). <http://www.useit.com.cn/thread-13618-1-1.html>.
- [9] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术: 研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4022.
- Zhang Ning, Wang Yi, Kang Chongqing, et al. Blockchain technique in the energy internet: preliminary research framework and typical applications[J]. Proceedings of the CSEE, 2016, 36(15): 4011-4022(in Chinese).
- [10] 李彬, 曹望璋, 祁兵, 等. 区块链技术在电力辅助服务领域的应用综述[J]. 电网技术, 2017, 41(3): 736-744.
- Li Bin, Cao Wangzhang, Qi Bing, et al. Overview of application of block chain technology in ancillary service market[J]. Power System Technology, 2017, 41(3): 736-744(in Chinese).
- [11] 李彬, 卢超, 曹望璋, 等. 基于区块链技术的自动需求响应系统应用初探[J]. 中国电机工程学报, 2017, 37(13): 3691-3702.
- Li Bin, Lu Chao, Cao Wangzhang, et al. A preliminary study of block chain based automated demand response system[J]. Proceedings of the CSEE, 2017, 37(13): 3691-3702(in Chinese).
- [12] 武庚, 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, 37(13): 3717-3728.
- Wu Geng, Zeng Bo, Li Ran, et al. Research on the application of blockchain in the integrated demand response resource transaction[J]. Proceedings of the CSEE, 2017, 37(13): 3717-3728(in Chinese).
- [13] 欧阳旭, 朱向前, 叶伦, 等. 区块链技术在用户直购电中的应用初探[J]. 中国电机工程学报, 2017, 37(13): 3737-3745.
- Ouyang Xu, Zhu Xiangqian, Ye Lun, et al. Preliminary applications of blockchain technique in large consumers direct power trading[J]. Proceedings of the CSEE, 2017, 37(13): 3737-3745(in Chinese).
- [14] 余维, 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(13): 3729-3736.
- She Wei, Hu Yue, Yang Xiaoyu, et al. Virtual power plant operation and scheduling model based on energy blockchain network[J]. Proceedings of the CSEE, 2017, 37(13): 3729-3736(in Chinese).
- [15] Aitzhan N Z, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[J]. IEEE Transactions on Dependable and Secure Computing, 2016, doi: 10.1109/TDSC.2016.2616861(in Press).
- [16] Mengelkamp E, Gärttner J, Rock K, et al. Designing microgrid energy markets: a case study: the Brooklyn Microgrid[J]. Applied Energy, 2018, 210: 870-880.
- [17] Vytelingum P, Cliff D, Jennings N R. Strategic bidding in continuous double auctions[J]. Artificial Intelligence, 2008, 172(14): 1700-1729.
- [18] 邵娜. 基于连续双向拍卖市场的报价策略选择研究[D]. 武汉: 华中科技大学, 2014.
- Shao Yuan. Bidding strategy choice in continuous double auction[D]. Wuhan: Huazhong University of Science and Technology, 2014(in Chinese).
- [19] Gode D K, Sunder S. Allocative efficiency of markets with zero-intelligence traders: market as a partial substitute for individual rationality[J]. Journal of Political Economy, 1993, 101(1): 119-137.
- [20] Walia V, Byde A, Cliff D. Evolving market design in zero-intelligence trader markets[C]//Proceedings of 2003 IEEE International Conference on E-Commerce. Newport Beach, CA, USA: IEEE, 2003: 157-164.
- [21] Vytelingum P. The structure and behaviour of the continuous double auction[D]. Southampton: University of Southampton, School of Electronics and Computer Science, 2006.
- [22] Bitcoins the hard way: using the raw bitcoin protocol [EB/OL]. (2014-02-23). <http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html>.
- [23] Bitcoin developer guide[EB/OL]. (2016-12-14). <https://bitcoin.org/en/developer-guide#block-chain-overview>.
- [24] 欧阳森, 石怡理. 改进熵权法及其在电能质量评估中的应用[J]. 电力系统自动化, 2013, 37(21): 156-159.
- Ouyang Sen, Shi Yili. A new improved entropy method and its application in power quality evaluation [J]. Automation of Electric Power Systems, 2013, 37(21): 156-159(in Chinese).
- [25] Colored coins[EB/OL]. (2015-11-02). https://en.bitcoin.it/wiki/Colored_Coins.

[26] EPOBC_simple[EB/OL]. (2015-05-12). https://github.com/chromaway/ngccbase/wiki/EPOBC_simple.

[27] Li Yuelei, Zhang Wei, Zhang Yongjie, et al. Calibration of the agent-based continuous double auction stock market by scaling analysis[J]. Information Sciences, 2014, 256: 46-56.

[28] 彭涛, 夏清, 江健健, 等. 区域电力市场交易模式的经济机理剖析[J]. 电力系统自动化, 2004, 28(7): 20-23, 29.
Peng Tao, Xia Qing, Jiang Jianjian, et al. Analysis of economic mechanism of two regional electricity market models[J]. Automation of Electric Power Systems, 2004, 28(7): 20-23, 29(in Chinese).

[29] Nicolaisen J, Petrov V, Tesfatsion L. Market power and efficiency in a computational electricity market with discriminatory double-auction pricing[J]. IEEE Transactions on Evolutionary Computation, 2001, 5(5): 504-523.

[30] 王秀丽, 周鹏, 王锡凡. 发/供电公司市场均衡及竞价策略[J]. 电力系统自动化, 2007, 31(6): 6-10.
Wang Xiuli, Zhou Peng, Wang Xifan. Market equilibrium and bidding strategies of generation/distribution companies[J]. Automation of Electric Power Systems, 2007, 31(6): 6-10(in Chinese).

附录 A

表 A1 彩色币发行交易

Tab. A1 Transaction of issuing colored coins

过程	脚本
输入	Prev_Tx hash1//前一笔交易哈希值 Vout: 0//前一笔未花费交易输出 scriptSig: <A sig>, <pubKeyA> //输入脚本 Sequence_N: 0x225 //序列号
	Value: 556 //输出比特币值
输出	scriptPubKey: OP_DUP OP_HASH160 <pubKeyAHash> OP_EQUALVERIFY OP_CHECKSIG //输出脚本
执行步骤	1) 获取上一笔未花费交易的哈希值 Prev_Tx hash1 和该笔交易的输出 Vout;
	2) 通过图 2 所示的堆栈语言执行脚本, 验证上一笔交易输出能否被花费;
	3) 如果脚本执行未通过, 交易终止, 否则进入步骤 4);
	4) 判断交易类型: Tag_Tx=Sequence_N&0x3F=0x25, 属于彩色币发行交易;
	5) 计算填充变量相关序列号位数: Padding_N=Sequence_N&0x0FC0=0x08=8;
	6) 计算填充变量大小 Padding=2 ⁸ =256;
	7) 将 556 Satoshi 比特币转移给 A 自身的公钥哈希值 pubKeyAHash;
	8) 判断彩色币数量 Ve=Value-Padding=300 Satoshi;
	9) 交易完毕。

表 A2 普通比特币转移交易

Tab. A2 Transaction of transferring Bitcoins

过程	脚本
输入	Prev_Tx hash2//前一笔交易哈希值 Vout: 0//前一笔交易输出

过程	脚本
输出	scriptSig: <B sig>, <pubKeyB> //输入脚本 Sequence_N: 0xFFFFFFFF //序列号 Value: 32056 //输出比特币值
	scriptPubKey: OP_HASH160 <Hash160(redeemScript)> OP_EQUAL //输出脚本
	1) 获取上一笔未花费交易的哈希值 Prev_Tx hash2 和该笔交易的输出 Vout;
执行步骤	2) 通过图 2 所示的堆栈语言执行脚本, 验证上一笔交易输出能否被花费;
	3) 如果脚本执行未通过, 交易终止, 否则进入步骤 4);
	4) 判断交易类型: Sequence_N=0xFFFFFFFF 属于普通比特币交易
	5) 将 32056 Satoshi 比特币转移给赎回脚本哈希值 Hash160(redeemScript);
	6) 交易完毕。

表 A3 仲裁退款交易

Tab. A3 Transaction of arbitration refund

过程	脚本
输入	Pre_Tx hash3 //用户 5 转移比特币交易的哈希值 Pre_Tx hash4 //DG 3 保证金交易的哈希值 Vout3: 0 //用户 5 转移比特币交易输出 Vout4: 0 //DG 3 保证金交易输出
	scriptSig: OP_0 <A sig or B sig> <C sig> <redeemScript> //多重签名输入脚本 Sequence_N: 0xFFFFFFFF //序列号
	{Value1: 22606 //输出到 DG 3 70% 交易费和彩色币成本 scriptPubKey: OP_DUP OP_HASH160 <pubKeyAHash> OP_EQUALVERIFY OP_CHECKSIG //输出脚本}
	{Value2: 15750 //输出到用户 5 30% 退款和保证金 scriptPubKey: OP_DUP OP_HASH160 <pubKeyBHash> OP_EQUALVERIFY OP_CHECKSIG //输出脚本}
执行步骤	1) 获取 B 转移到转移给 Hash160(redeemScript) 交易的哈希值 Prev_Tx hash3 和该笔交易的输出 Vout;
	2) 通过堆栈语言执行 P2SH 脚本, 根据多重签名输入脚本验证该交易输出能否被花费;
	3) 如果脚本执行未通过, 交易终止, 否则进入步骤 4);
	4) 判断交易类型: Sequence_N=0xFFFFFFFF 属于普通比特币交易
	5) 将 22606 Satoshi 比特币转移给 A 公钥哈希值 pubKeyAHash;
	6) 将 15750 Satoshi 比特币转移给 B 公钥哈希值 pubKeyBHash;
	7) 交易完毕。



王健

收稿日期: 2017-09-11。

作者简介:

王健(1993), 男, 博士研究生, 研究方向为电力系统优化运行、电力市场和数据挖掘, cqu_wj@cqu.edu.cn;

周念成(1969), 男, 教授, 博士生导师, 主要从事电力系统自动化和电能质量等方面的教学和研究, cee_nczhou@cqu.edu.cn。

(责任编辑 李泽荣)

Electricity Direct Transaction Mode and Strategy in Microgrid Based on Blockchain and Continuous Double Auction Mechanism

WANG Jian¹, ZHOU Niancheng¹, WANG Qianggang¹, WANG Peng²

(1. Chongqing University; 2. Nanyang Technological University)

KEY WORDS: microgrid direct transaction; blockchain; continuous double auction; adaptive aggressiveness strategy; asset digital certification

With the reform of electricity market, microgrid or distributed generations (DGs) are allowed to participate in electricity market transactions. The electricity transactions between DGs and consumers are characterized by decentralization and small scale, and the relationship of supply and demand presents a similar situation in the stock market. However, now most DGs can only sell power to grid, and cannot make direct transaction.

In order to realize the direct transaction between DGs and consumers in microgrid, a direct transaction method is proposed based on blockchain and continuous double auction (CDA). Firstly, DGs and consumers submit quotes and transaction volume to the CDA market respectively, and the market matches automatically according to the quotation of both parties. In the process of matching, the market publicizes the transaction information, and DGs and consumers constantly adjust the quotes according to adaptive aggressiveness strategy (AA strategy). AA strategy models of the buyer and seller are as follows:

$$p_b(t) = \begin{cases} p_{Obid}(t) + \eta[\min\{v_i, p_{Oask}(t)\} - p_{Obid}(t)], & t = 1 \\ p_{Obid}(t) + \eta[\tau_b(t) - p_{Obid}(t)], & t \geq 2 \end{cases} \quad (1)$$

$$p_s(t) = \begin{cases} p_{Oask}(t) - \eta[p_{Oask}(t) - \max\{c_j, p_{Obid}(t)\}], & t = 1 \\ p_{Oask}(t) - \eta[p_{Oask}(t) - \tau_s(t)], & t \geq 2 \end{cases} \quad (2)$$

Then, the quotes of the buyers are in high-to-low order, whereas the quotes of the sellers are in low-to-high order. When the outstanding bid price is greater than or equal to the outstanding ask price, the transaction can occur. In the matching process, the buyer with the outstanding bid price matches the outstanding ask price, and the transaction price is the average price of the two. And so on, until the outstanding bid price is below the outstanding ask price. The transaction parties settle through the blockchain after matching. DG transfers digital certificate of electricity energy to the consumer in blockchain system, the digital certification of electricity assets is replaced by the sequence number

with specific tags in the transaction script, and the size of digital certification can be adjusted according to transaction energy quantity. The consumer transfers bitcoins to DG through blockchain, and the consumer's benefit is guaranteed through the multi-signature mechanism. The blockchain transaction is based on the unspent transaction out model, which is implemented through the stack language, and the script execution process is shown in Fig. 1.

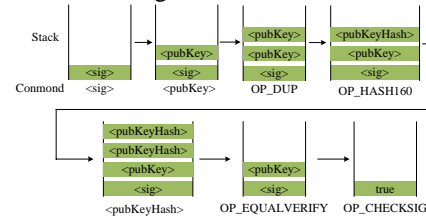


Fig. 1 Script execution process

The simulation results show that the transaction model can be used for the internal power transaction of microgrid. Under CDA mechanism, AA trading strategy can adaptively track the market information and find the optimal quotes according to transaction price and price fluctuations. The adaptive adjustment process is shown in Fig. 2. In addition, DGs and consumers realize the transaction settlement without centralized organization through blockchain, and the multi-signature mechanism can guarantee the interests of the consumer and avoid the loss caused by the DG's default.

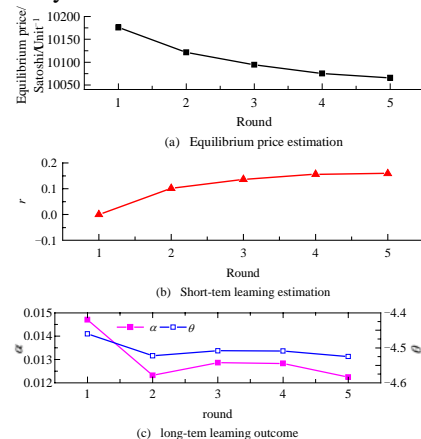


Fig. 2 Equilibrium price estimation, short-term learning and long-term learning outcomes