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.

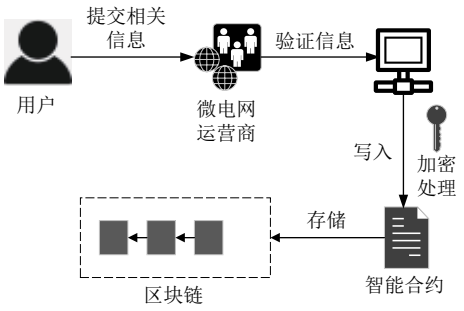

图 5 用户注册过程

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].

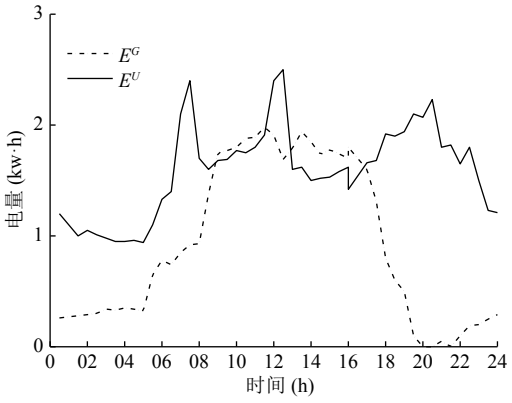

图 6 微电网内每 0.5 h 总出售/购买电量

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.

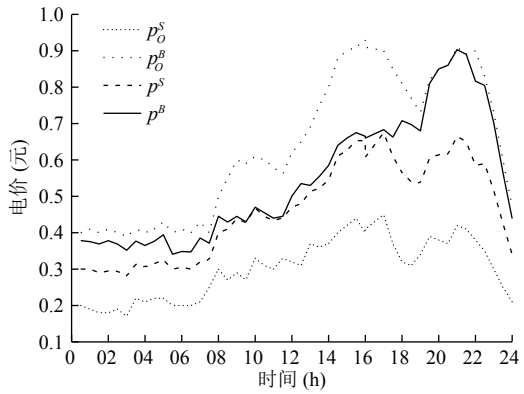

图 7 电价对比

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_{New}和C_{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_{New}和S_{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.

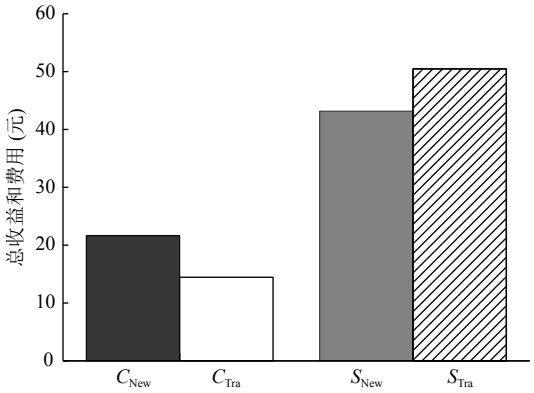

图 8 总收益和费用对比

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.