doi: 10.7690/bgzdh.2025.01.014

基于区块链的电力交易隐私保护

范　琨[1]，刘　俊[2]，杨　猛[2]，肖坤军[2]
（1. 江西电力交易中心有限公司市场（技术）部，南昌 330000；
2. 四川中电启明星信息技术有限公司能源交易事业部，成都 610000）

摘要：为解决连续双拍卖区块链成本高、速度慢和缺乏隐私保护的问题，提出一种结合基于联盟区块链和连续双拍卖的微电网直接交易隐私保护方案。参与电力交易的用户在监管中心注册，从而获得交易匹配的匿名和匿名交易证书；在消费者和生产者通过连续双拍卖机制进行匹配后，消费者确认生产者发送的账户和电费的真实性，并创建交易记录；电力生产商向本地聚合器发送电费和交易记录并进行加密，将其打包成块向每个聚合器节点广播验证。实验结果表明：所提方案具有较低的计算开销和能量消耗，为电力交易智能化、安全化应用提供一定借鉴。

关键词：电力系统；电力交易；区块链；匿名；隐私保护
中图分类号：TM737　　**文献标志码：**A

Privacy Protection of Power Transaction Based on Blockchain

Fan Kun[1], Liu Jun[2], Yang Meng[2], Xiao Kunjun[2]
(1. *Market* (*Technology*) *Department of Jiangxi Power Trading Center Co*., *Ltd*., *Nanchang* 330000, *China*;
2. *Energy Trading Department of Sichuan Zhongdian Qiming Information Technology Co*., *Ltd*., *Chengdu* 610000, *China*)

Abstract: In order to solve the problems of high cost, slow speed and lack of privacy protection of continuous double auction block chain, a privacy protection scheme for microgrid direct transaction based on alliance block chain and continuous double auction is proposed. After the consumer and the producer are matched through a continuous double-auction mechanism, the consumer confirms the authenticity of the account and the electricity charge sent by the producer and creates a transaction record; Electricity producers send electricity bills and transaction records to local aggregators, encrypt them, and package them into blocks to broadcast verification to each aggregator node. The experimental results show that the proposed scheme has lower computational overhead and energy consumption, and provides a reference for the intelligent and secure application of electricity trading.

Keywords: power system; power transaction; blockchain; anonymity; privacy protection

0　引言

随着通信、计算机、物联网、网络[1-3]等技术兴起，微电网迎来了飞速发展时期。微电网是一个基于分布式发电技术的模块化分散供电网络，与终端用户电能质量管理和能源梯级利用密切相关。由于分布式电源具有存储容量小、便于远距离传输等特点，传统的集中式供电调度方法增加了系统的复杂性，导致微电网的低效率和高成本。

随着微电网开发建设的逐步深入，相邻微电网之间可以形成微电网群；同时，市场机制的完善为微电网参与电力市场竞价交易提供了机遇。分布式电源和用户可以在微电网能源市场上通过竞价完成交易匹配；因此，有必要在分布式电源和客户之间建立一个直接、开放的电力交易信息流系统[4]。这样，微电网中的用户不仅能以更低的价格购买本地电力，电力供应商能以更高的价格出售多余的电力，还可提高分布式电源的资源利用率。微电网中的各种实体需要在分布式环境中进行测量、交互、控制和决策，然而这些实体作为分布式参与节点很难实现互信。区块链作为一种新兴的分布式和去中心化技术，是解决此类问题的一个很好研究方向。

目前，关于如何将区块链技术应用于电力交易已成为研究热点。文献[5]设计了基于区块链技术的电力数据资产化及交易系统，实现了电力数据交易业务的安全、透明、可追溯、不可篡改。文献[6]研究产消者通过有机朗肯循环系统进行分布式多能源交易的机制。文献[7]提出了基于区块链的电力市场交易系统功能设计与实现方法。然而，在能量有限的微电网中建立区块链的成本太高，需要考虑节点共识一致性造成计算成本高以及能量消耗过大等问题。此外，电力交易常采用连续双拍卖机制，这将导致竞拍者身份及竞拍信息遭受隐私泄露风险；因此，拍卖过程中的隐私保护问题也是另一个需要关注的重点。

收稿日期：2024-07-05；**修回日期：**2024-08-05
第一作者：范　琨（1976—），男，湖南人，硕士。

为解决连续双拍卖区块链成本高、速度慢和缺乏隐私保护的问题，笔者提出基于联盟区块链结合连续双拍卖的微电网直接交易隐私保护方案，从而降低交易成本，提高交易效率，实现连续双拍卖中的身份隐私包含。

1 隐私保护方案设计

1.1 微电网电力交易工作过程

笔者提出一种基于联盟区块链和连续双拍卖机制的微电网电力直接交易模型。电力交易过程中涉及的实体包括电力生产商和电力消费者。电力生产商和电力消费者在交易周期内通过连续双拍卖机制不断调整报价，从而完成交易匹配。交易结算通过区块链的共识流程进行，从而实现微电网内用户的直接交易。

微电网直接电力交易过程如图 1 所示。该过程由 3 部分组成：1) 用户注册以生成交易证书；2) 用户通过连续双拍卖机制完成电力交易匹配；3) 联盟区块链本地聚合节点完成共识。

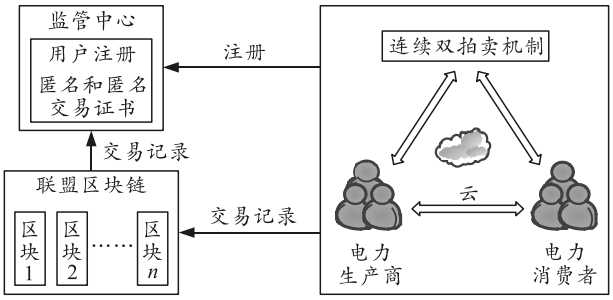

图 1 微电网直接电力交易过程

上图中电力交易工作过程为：首先，参与电力交易的用户在监管中心注册，从而获得交易匹配的匿名和匿名交易证书；其次，在消费者和生产者通过连续双拍卖机制进行匹配后，消费者确认生产者发送的账户和电费的真实性，并创建交易记录；最后，电力生产商向本地聚合器发送电费和交易记录，该聚合器对交易记录进行加密，并将其打包成块，向每个聚合器节点广播验证。需注意：在联盟区块链协商一致之后，将会生成一个新的区块并加入联盟区块链。联盟区块链中的交易记录不可篡改，并且对于用户节点具有高度透明查询权限。

1.2 隐私保护机制

隐私保护方案的基本系统架构基于微电网设计，系统共包含 4 类实体：微电网用户(U_i)、注册管理中心(registration management，RM)、市场管理中心(market management，MM)和跟踪中心(trace center，TC)。用户生成 RM 中的匿名和 MM 中的匿名对应的匿名证书。用户只需要匿名和匿名证书即可参与后续拍卖，而不需要真实的用户身份信息，从而实现公平拍卖。TC 用于在必要时跟踪用户的真实身份。隐私保护方案系统架构如图 2 所示。

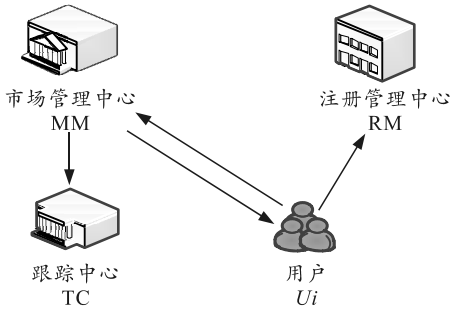

图 2 隐私保护方案系统架构

隐私保护的基本实施过程如下：

步骤 1 参与拍卖的用户首先注册，并使用公平盲签名通过 RM 验证用户身份后生成相应的匿名；

步骤 2 用户向 MM 申请匿名证书；

步骤 3 MM 生成用户参与电力拍卖所需的匿名证书；

步骤 4 TC 作为受信任的第三方，其私钥通过使用门限秘密共享技术[8]单独保存，从而确保在此过程中没有可信机构能够生成用户真实身份和匿名之间的对应关系。同时，还可以使用密钥恢复来实现中途退出的用户的可追溯性。

2 隐私保护实施过程

根据前述知识，TC 的私钥通过(t, n)门限秘密共享技术单独存储，不易受到攻击，从而实现了系统的鲁棒性。同时，用户匿名和交易证书通过公平盲签名进行验证。在生成过程中，用户和 RM、MM 在 2 个方向上进行身份验证，从而实现隐私保护的匿名性、不可伪造性和不可否认性。此外，TC 私钥的恢复主要通过(t, n)门限秘密共享技术，然后 TC 跟踪用户的真实身份，从而实现隐患保护的可追溯性。接下来，对隐私保护实施过程进行详细介绍。

2.1 系统初始化和参数设置

在参与电力交易之前，加入联盟区块链的节点连接到本地聚合器，并将其帐户发送给本地聚合器。本地聚合节点存储完整的区块链交易数据，从而便于用户查询和验证交易。然而，参与电力交易的普通节点存储部分数据且由每个块头组成的哈希链形式，从而有效减少总数据存储和总存储开销。另一方面，该过程降低了加入节点的性能要求，从而促

进更多节点加入联盟区块链。

隐私保护过程中系统初始化和参数设置如下：首先，用户通过 RSA 算法生成的公钥(N_u, e_u)和私钥 d_u。其次，由 RM 通过 RSA 算法生成的公钥(N_{RM}, e_{RM})和私钥 d_{RM}。接着，MM 通过 RSA 算法生成公钥(N_{MM}, e_{MM})和私钥 d_{MM}。TC 通过 RSA 算法生成公钥(N_{TC}, e_{TC})和私钥 d_{TC}。进一步，RM、MM 和 TC 的公钥发布在 MM 上，RM 和 MM 的私钥自行保管。

2.2　私钥分发

通过 RSA 算法生成 TC 私钥后，可根据(t, n)门限秘密共享计算将私钥分别存储在 n 个参与者中。私钥分发过程如下：

步骤 1 共享每个参与者拥有的子私钥。为提高效率，选择的共享份额是递增的，同时确保每个参与者的共享份额不相同。

步骤 2 使用拉格朗日插值构造 n 阶多项式 $F(x)$：

$$F(x)=d_{TC}+a_1x+a_2x^2+a_3x^3+\cdots+a_{n-1}x^{n-1}。\quad(1)$$

式中：d_{TC} 为初始获得的私钥；$a_i(i=1, 2, \cdots, n-1)$为多项式的系数。

步骤 3 通过将每个参与者获得的共享信息和私钥信息代入多项式计算结果，从而获得每个参与者获取的子私钥的内容。

2.3　匿名和匿名证书生成

在此阶段，用户通过生成匿名和匿名证书匿名参与电能拍卖过程，具体执行过程如图 3 所示。

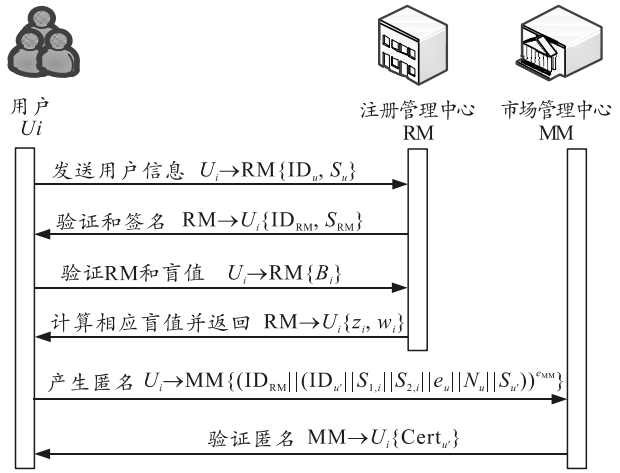

图 3　用户通过生成匿名和匿名证书匿名参与电能拍卖执行过程

该执行过程分为以下 6 个步骤：

步骤 1 用户向 RM 发送第 i 个用户的标识身份 ID_u 和签名 S_u：

$$U_i\rightarrow \mathrm{RM}\{\mathrm{ID}_u, S_u\}；\quad(2)$$

$$S_u=\mathrm{ID}_{\mathrm{RM}}^{d_u} \bmod N_u。\quad(3)$$

式中：$\mathrm{ID}_{\mathrm{RM}}^{d_u}$ 为由 RM 分配的用户身份 ID；N_u 为通过 RSA 算法生成的公钥；d_u 为私钥；mod 为余运算符。

步骤 2 RM 验证用户签名，如果认证成功，则同意生成匿名，并向用户发送 ID_{RM} 和签名 S_{RM}：

$$\mathrm{RM}\rightarrow U_i\{\mathrm{ID}_{\mathrm{RM}}, S_{\mathrm{RM}}\}；\quad(4)$$

$$S_{\mathrm{RM}}=\left[(\mathrm{ID}_{\mathrm{RM}}\|\mathrm{ID}_u\|t_s)^{d_{\mathrm{RM}}} \bmod N_{\mathrm{RM}}\right]^{e_u} \bmod N_u。\quad(5)$$

式中：N_{RM} 为 RM 通过 RSA 算法生成的公钥；d_{RM} 为私钥；t_s 为时间戳。

步骤 3 在接收到消息后，用户使用私钥解密，然后使用 RM 的公钥验证其 RM 签名。同时选择随机正整数 x_i，y_i 并计算盲签名值 B_i：

$$U_i\rightarrow \mathrm{RM}\{B_i\}；\quad(6)$$

$$B_i=y_i^{e_{\mathrm{RM}}}x_i。\quad(7)$$

步骤 4 当接收到盲签名值 B_i 后，RM 计算 z_i 和 w_i：

$$\mathrm{RM}\rightarrow U_i\{z_i, w_i\}；\quad(8)$$

$$z_i=\left(y_i^{e_{\mathrm{RM}}}x_i\bullet(i\|\mathrm{ID}_u\|t_s)\right)^{d_{\mathrm{RM}}}；\quad(9)$$

$$w_i=\left((i\|\mathrm{ID}_u\|t_s)^{e_{\mathrm{TC}}}\right)^{d_{\mathrm{RM}}}。\quad(10)$$

式中 TC 通过 RSA 算法生成公钥(N_{TC}, e_{TC})和私钥 d_{TC}。

步骤 5 产生匿名，产生过程如下：

$$U_i\rightarrow \mathrm{MM}\left\{\left(\mathrm{ID}_{\mathrm{RM}}\|\left(\mathrm{ID}_{u'}\|s_{1,i}\|s_{2,i}\|e_u\|N_u\|S_{u'}\right)\right)^{e_{\mathrm{MM}}}\right\}；\quad(11)$$

$$s_{1,i}=z_i/y_i；\quad(12)$$

$$s_{2,i}=s_{1,i}^{e_{\mathrm{TC}}}/w_i；\quad(13)$$

$$\mathrm{ID}_{u'}=x_i\bullet(i\|\mathrm{ID}_u\|t_s)x_i^{e_{\mathrm{TC}}}。\quad(14)$$

式中：$S_{u'}$ 为具有临时私钥 $d_{u'}$ 的用户 u 的交易签名；$\mathrm{ID}_{u'}$ 为用户 u 的匿名；$x_i^{e_{TC}}$ 为 TC 中产生的随机正整数。

步骤 6 验证匿名，验证过程如下：

$$\mathrm{MM}\rightarrow U_i\{\mathrm{Cert}_{u'}\}；\quad(15)$$

$$s_{1,i}^{e_{\mathrm{RM}}}=(z_i/y_i)^{e_{\mathrm{RM}}}=\left(x_i\bullet(i\|\mathrm{ID}_u\|t_s)_{\mathrm{RM}}^{d}\right)^{e_{\mathrm{RM}}}=x_i\bullet(i\|\mathrm{ID}_u\|t_s)；\quad(16)$$

$$s_{2,i}^{e_{\mathrm{RM}}}=\left(s_{1,i}^{e_{\mathrm{TC}}}/w_i\right)^{e_{\mathrm{RM}}}=\left((z_i/y_i)^{e_{\mathrm{TC}}}/w_i\right)^{e_{\mathrm{RM}}}=\left(\left(x_i^{d_{\mathrm{RM}}}\right)^{e_{\mathrm{TC}}}\right)^{e_{\mathrm{RM}}}=x_i^{e_{\mathrm{TC}}}。\quad(17)$$

式中 Cert 为追踪中心。

2.4 连续双拍卖交易机制

当用户完成匿名及匿名证书生成后，可基于匿名实现连续双拍卖电力交易。笔者设计的交易机制描述如下：

首先，用户 u 完成注册并获得交易证书。在交易周期内，用户提交竞价信息，匿名证书 C_u 和交易数字签名 $S_{u'}(o)$。其中，o 为电力交易信息，定义如下：

$$o=\{\mathrm{ID}_{u'}, m, t_s, v_{u'}\}。\tag{18}$$

式中：m 为竞标标签；t_s 为时间戳；$v_{u'}$ 为交易电量。需注意：正的交易电量表示卖方，负的交易电量则表示买方。

其次，根据交易规则判断投标价格是否符合市场要求。如果满足要求，将接受投标人的价格；否则，将要求投标人重新提交标书。一旦买方的价格高于卖方的价格，买方的最高价格与卖方的最低价格匹配。同样，交易价格为双方的平均价格。同时，发布市场交易信息，包括交易价格、交易数量和未完成交易的出价信息。

当提交一轮报价后，用户重新选择随机数以生成相应的盲签名值和匿名。然后将其发送给 MM，从而获得下一轮拍卖竞标的新匿名证书。重复开始新的交易配对，直到交易周期结束。

2.5 联盟区块链

参与电力交易的用户匹配后，供电用户将其账户信息和电费单发送给电力用户，电力用户确认账户的真实性并创建交易记录。然后，电力用户将电力成本和交易记录发送给本地聚合器。本地聚合器加密交易记录并将其打包成块，并广播到每个聚合器节点，从而执行联盟区块链的协商一致过程。现有共识算法中，工作量证明(proof of work，POW)是最安全的公共区块链中的共识算法，然而其效率太低，无法满足用户的实时需求，且计算资源耗费太多。权益证明(proof of stake，POS)和股权授权证明(delegated proof of stake，DPO)相对于 POW 减少了计算资源消耗，但存在过度集中的问题。

为此，笔者基于实用拜占庭容错算法(practical byzantine fault tolerance，PBFT)设计了一种联盟区块链，从而为本地聚合节点实现共识过程。令 n 为联盟区块链中参与共识的本地聚合节点总数，f 为允许失败的节点数。图 4 所示为联盟区块链共识过程。

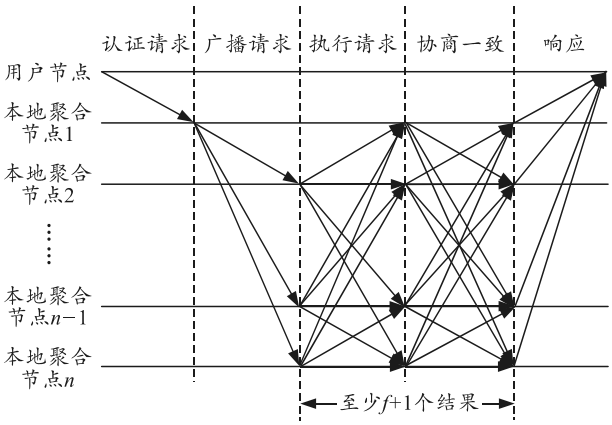

图 4 联盟区块链共识过程

首先，用户节点向本地聚合节点发送认证请求以调用服务操作。其次，本地聚合节点将广播请求发送到其他本地聚集器节点。接着，所有本地聚合节点执行请求并将结果发送给用户节点，用户节点至少等待来自不同本地聚合器结点的 f+1 个结果。如果结果相同，则为请求的最终结果。在通过协商一致过程将交易记录添加到联盟区块链后，所有记录都存储在区块链中，从而便于用户查询和跟踪。

2.6 门限秘密共享

当中标买方未支付与中标相同金额的货币，或卖方未向买方支付与中标金额相同金额的电力时，跟踪中心 TC 可以通过(t, n)门限秘密共享方法恢复密钥以获得私钥。在私钥恢复阶段，令参与者的集合为 $A=\{P_1, P_2, \cdots, P_n\}$。假定有 t 个参与者参与恢复私钥，则恢复密钥过程描述如下：

步骤 1 在参与私钥恢复的 t 个参与者中，每个参与者必须获得有关私钥的信息。

步骤 2 每个参与者使用其子私钥共享来计算子私钥内容。计算结果将传递给私钥生成器或调用恢复私钥的另一参与者。

步骤 3 当恢复私钥时，使用拉格朗日插值法计算每个参与者的子私钥。

3 案例分析

对所提基于联盟区块链和连续双拍卖的微电网直接交易隐私保护模型进行仿真与测试，从而评估系统数据处理和共享的效率。测试时总共部署了 7 台虚拟机从而模拟网络节点。测试硬件配置：服务器 10 块 Intel(R) Xeon(R)金牌 6136 CPU，3.00 GHz，内存 64 G，硬盘 2 T；虚拟机 Intel(R) Xeon(R)金牌 6136 CPU，3.00 GHz 1 块，内存 8 G，硬盘 20 G。

软件环境如下：操作系统均为 ubuntu18.04，Hyperledger Fabric 版本 V1.4.0。

3.1　安全性分形

笔者基于是否存在所提隐私保护模型对虚拟节点数据处理和共享安全性进行分析。试验时分别对无隐私保护虚拟节点网络和有隐私保护虚拟节点网络进行网络攻击，攻击方式包括：消息篡改、拒绝服务攻击(denial of service，DOS)、身份伪造。同时，每种攻击执行 1 000 次，以成功攻击率为指标对比不同机制性能。表 1 为系统安全性分析说明。

表 1　系统安全性分析说明　　%

实验	消息篡改	DOS	身份伪造
无隐私保护	39.6	29.2	13.9
有隐私保护	0.3	0.5	0.2

从上表可以看出：加入所提隐私保护模型后，虚拟节点网络安全性大大提升。试验结果验证了所提模型对网络安全具有一定保护作用。

3.2　性能分析

基于计算开销测试来评估系统性能。需注意，测试时忽略了一次性计算开销阶段的测试，例如系统构建和注册阶段。表 2 为系统测试情况说明，测试时共包含 6 种计算指标。

表 2　系统测试情况说明

实验	说明
1	RSA 算法加密数据
2	RSA 算法解密数据
3	用户数据签名
4	生成转换密钥和数据共享密钥
5	基于门限秘密共享转换数据共享密钥
6	验证数字签名

测试时，分别使用不同大小的未加密电力交易数据文件(文件 1、文件 2 和文件 3 分别为 64 KB、256 KB 和 1 MB)对每个操作进行 1 000 次，最终试验结果的计算开销平均值统计如表 3 所示。

表 3　计算开销平均值统计结果　　ms

实验	文件 1	文件 2	文件 3	均值
1	396	1 592	6 352	2 870.0
2	418	1 455	35 889	15 487.3
3	5	4	4	4.3
4	3	7	26	12.0
5	2	2	2	2.0
6	39	40	45	41.3

从上表可以看出，加解密计算消耗随着未加密数据文件的大小而增加。其中，RSA 算法加密和解密数据平均计算开销为 2 870 ms 和 15 487.3 ms。RSA 加密算法加密时间很短，基本可以忽略不计；但是，RSA 解密时间与解密文件的大小呈现线性增长趋势。考虑到电力数据动态交易时时间有限，除极特殊情况，交易数据量不会太大(小于 64 KB)；因此，加解密时间均在可接受范围(400 ms 左右)。

此外，区块链中数字签名与共享的计算开销与电力数据文件的大小没有明显的关系。其中，用户数据签名平均计算开销为 4.3 ms，生成转换密钥和数据共享密钥平均计算开销为 12 ms，基于门限秘密共享转换数据共享密钥平均计算开销为 2 ms，验证数字签名平均计算开销为 41.3 ms。仿真结果验证了所提方案具有较低的计算开销，可大大降低网络的计算成本。

3.3　交叉对比分析

为验证所提联盟区块链性能，对传统区块链和联盟区块链能量消耗进行对比。图 5 为传统区块链和联盟区块链能量消耗对比结果。

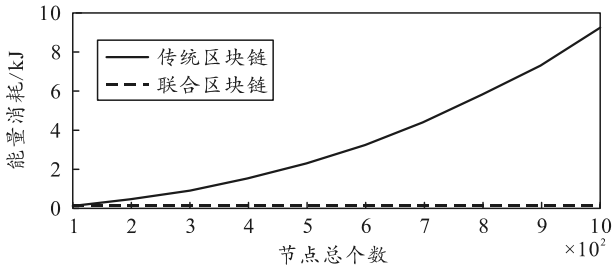

图 5　传统区块链和联盟区块链能量消耗对比结果

上图中，随着联盟区块链和区块链中节点总数的增加，联盟区块链中共识能量消耗约 9.6 kJ，且不受汇聚节点总数的影响。相比之下，传统区块链需要整个网络的总节点达成一致；因此，随着广播和验证消耗中节点个数的增加，其能量消耗急剧增加。同时，试验结果还表明，所提隐私保护模型下的虚拟节点网络可按照更低的运行成本保障网络顺利执行。实验结果验证了所提模型的可行性和有效性。

4　结论

笔者建立一种基于联盟区块链的电力交易隐私保护方案。该方案结合电力供应商和电力消费者连续双拍卖交易机制和联盟区块链共识机制，具备电力交易匿名性、可追溯性、健壮性等优点，从而解决连续双拍卖区块链成本高、速度慢和缺乏隐私保护的问题。该方案为电力交易管理及智能隐私保护提供了一定借鉴。未来，可对模型参数的优化配置和规模进行研究，进一步降低系统计算消耗。

（下转第 109 页）