基于区块链的微电网电力交易匹配机制

邓明辉[1],唐郑熠[1,2,3],黄 达[1],胡文瑜[1,2,3]
(1. 福建工程学院 计算机科学与数学学院,福建 福州 350118;
2. 湖南工商大学 移动商务智能湖南省重点实验室,湖南 长沙 410205;
3. 福建工程学院 福建省大数据挖掘与应用技术重点实验室,福建 福州 350118)

摘要:针对分布式微电网新能源电力交易问题,基于主体的历史交易完成比提出一种适用于交易的匹配策略。将匹配度量化为对实体信用与电力售价的考察,并借助区块链实现信用数据的有效共享与周期评估。当消费者在进行购电行为收到不同生产者的电价信息时,可从区块链账本中得知该生产者的交易信用值,并筛选出合适的交易方。算例分析表明:所提策略能够有效量化信用,结合售电价格匹配到最适合的交易方。

关键词:区块链;电力交易;新能源;匹配策略;分布式
中图分类号:TM 73 **文献标志码**:A DOI:10.16081/j.epae.202107017

0 引言

随着太阳能、风能、生物质能等新能源的发展及广泛应用,新能源以微电网形式高渗透率地接入配电网中,使得配电网的能源结构发生了质的变化。配电网可以向微电网的负荷提供电能,也可以从微电网的新能源接收电能,配电网由原先的单向潮流变为双向潮流,能源结构更加复杂。同时风能和太阳能受地理位置、天气条件等客观因素影响,发电具有间歇性和随机性等特点,致使配电网的能源分布具有更大的不确定性[1]。从能源利用的角度看,负荷类型的多样化导致配电网支撑下的微电网结构和潮流均发生了明显变化,需要良好的新能源交易和管理机制来实现分布式能源的有效消纳[2]。一种有效的实时电网电价机制是根据产消者的电力生产和需求情况,合理给出新能源发电的实时电价,以最大限度地满足消费主体需求,达到利益的最大化和生态的动态平衡[3]。我国现有的电力交易主要通过集中式交易中心完成,这虽然有利于保障电力交易的安全性,但集中式电力交易中心在市场机制、交易清算和交易管理等诸多领域还需进一步发展完善。另外,目前集中式电力交易主要进行年度、季度、月度等中长期电力交易,几乎不承担分时电力交易,而新能源由于自身发电的不确定性,更关注于短期电力交易,这在集中式电力交易中心难以实现[4]。文献[5]分析现有基于区块链技术的电力市场交易系统的优势与不足。区块链技术本质上是一种去中心化、公开透明的分布式数据库,在支持交易记录、实现互不信任的多方合作等方面具有独特的优势[6]。基于多方间的交易,信任是最常见的问题之一,其具有主观性、模糊性和不确定性,依赖于过往的行为并随时间变化,交易买卖双方彼此的态度受过去行为认识影响。社会关系中的信任评价可以按照以下方式进行:主体可以根据客体的历史表现直接给出信任评价,参照客体的贡献评分值实现自己的交易意愿[7]。文献[8]开发一种基于许可区块链的住宅能源交易系统RETS(Residential Energy Trading Systems),在该机制下参与交易的消费主体可以考虑自身偏好的投标策略,避免了单一模式下的被动性,另外该机制的执行过程高效简洁,可以实现合理配置资源的目的。文献[9]指出分布式可交易能源可以促进电力系统的供需平衡,提出面向源网荷可直接交易互动的去中心化扁平交易体系,通过设置有效的激励政策来引导交易的产生,并指出实现系统所需的核心技术,其中明确指出区块链技术是实现去中心化的基础。文献[10]在假设多个微电网主体是彼此非合作的情况下,提出非合作博弈下的多微电网电能交易一般模式,同时将配电网的职能定义为提供综合辅助服务,在交易过程中征收服务费,完善了交易机制。文献[11]将交易分成2种博弈,一方面是售电方之间的价格竞争,另一方面则是购电方之间对售电方进行选择的竞争,再分别进行建模,并提出2种迭代算法来实现博弈,使得每个博弈都存在一个均衡状态,进一步完善了交易模型。文献[12-15]分别从电网的优化控制、电力调度、共识机制选择和电力交易优化方面进行探讨。微电网电能生产者与消费者间、产消者(既产生电能也购买电能)间、产消者与消费者间存在广泛的交易合作,但由于微电网中交易双方的匿名性与未知性,如何确保交易能够顺利达成、实现各自利益的最大化是个

收稿日期:2020-10-27;**修回日期**:2021-05-24
基金项目:福建省自然科学基金资助项目(2020J01877);湖南省重点实验室开放研究基金资助项目(2015TP1002);国家重点研发计划子课题(2018YFC1201103)
Project supported by the Natural Science Foundation of Fujian Province(2020J01877),the Open Fund of Key Laboratory of Hunan Province(2015TP1002) and the Sub-project of National Key R&D Program of China(2018YFC1201103)

有待解决的问题。

解决合作问题的前提是为各电力生产者和产消者建立匹配机制，然而微电网中参与者成员各异，各供电方的产电能力也不同，这使得现有的交易安全无法统筹兼顾。本文采用基于区块链的微电网电力交易匹配方法，在不依赖于可信第三方与额外信任假设的完全分布式微电网中，确保交易安全，降低交易风险，促进配电网中新能源产电的实时利用。本文的主要贡献有以下2个方面。

1)针对分布式微电网中新能源电力属性与信任特征各异导致难以建立通用的信用管理方法的问题，本文提出各主体信任的建立与管理、信任数据全网共享的机制。该方法不依赖于任何可信第三方和额外信任假设，信任的建立与管理完全依赖于各主体的历史动态与共同维护。

2)针对微电网主体的电力需求，本文提出分布式微电网中各主体间的交易匹配机制，将匹配度量化为信用和价格。依据微电网各主体的发电能力差异和供电稳定性的特点对消费者报价后，消费者结合信用值并根据不同供电能力主体的匹配度筛选合适的交易匹配对象。

1 基于区块链的网络模型

1.1 通信网络模型

基于区块链的通信网络模型的拓扑结构如图1所示，其组成元素为：监管机构，包括分布式新能源交易联盟以及负责传输电力、保障交易的电网公司；电力公司，分为新能源发电和常规能源发电，新能源包括风能、太阳能等，常规能源包括水力发电、火力发电等；电力消费方，主要指充电桩、居民用户、工厂等。

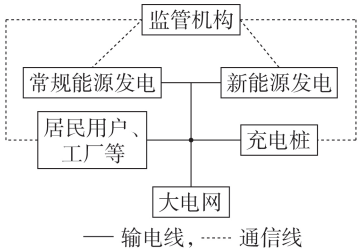


图1 电力交易的输电信息线路

Fig.1 Transmission information lines for power transaction

所有参与方构成电力交易的主体，各交易主体与运行区块链节点的智能设备一一对应，每个节点的智能设备代表该节点的账户地址，通过智能设备记录的电量变化来表示交易信息，在电力交割阶段结束时，智能设备可通过通信网络反馈发用电数据以触发交易结算。

1.2 初始化信息

为了能够方便响应分布式微电网交易所DME(Distributed Microgrid Exchange)中各主体间的交易，电网公司、信息中心等相关部门需明确所有参与者的真实身份，且参与者的交易数据存在一定的隐私性，不应被DME外的主体随意读取，因此，本文选择联盟链作为实现方案。

为了清晰地知道每个节点的真实身份，分发公钥和对应的私钥，将这些明文数据通过区块链直接上链，这些数据能方便其他参与方直观了解相应节点的身份信息。电力公司身份信息为I(IDname、address、phone、type)，消费主体身份信息为J(IDname、address、phone)。其中IDname、address、phone、type分别表示营业账号、公司地址、公司电话、能源类型，这是明确的公开数据，其真实性可以通过联盟链中作为监管节点的政府相关部门等权威节点确认，监管节点同时负责微电网电力交易联盟中新成员加入的身份认证，防止假冒身份者进入微电网电力交易中，交易交割阶段每个区块都记录一个主体达成的交易。实现步骤如图2所示，图中n_{sum}为参与方数量。

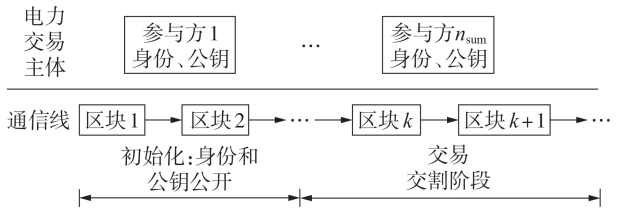


图2 区块链信息初始化

Fig.2 Initialization of block chain information

2 匹配评估

2.1 信用表现

信任指标是对主体可靠性的量化评估，由于单一的周期行为只能反映主体的片面特征，为了更好地评估主体的整体表现，本文提出一个能够体现主体长期和近期表现的指标体系，具体定义如下。

电力公司的信用与和消费者的电力交易事务相关，由售电额度的级别度量。信用是唯一标识发电公司在下个交易周期中受消费者信任程度的值，分为长期信用和短期信用，分别记为C_L、C_S。

定义1 交易记录。电力公司主体的交易记录$\kappa=(k_{ia},p_{ia},G)$。其中，k_{ia}为电力公司节点i达成交易的次数；p_{ia}为交易完成比；$G=<(1,p_{i1}),(2,p_{i2}),\cdots,(a_{iT},p_{ia_{iT}})>$是一个队列，包含最近$a_{iT}$次电力交易的交易完成比，$a_{iT}$为电力公司节点$i$在第$T$个交易周期中的有效电力交易数，$(a,p_{ia})(a=1,2,\cdots,a_{iT})$表示电力公司主体在第$a$次交易后的交易完成比是$p_{ia}$。

短期信用计算公式为：

$$C_S(i,T)=\frac{\sum_{a=1}^{a_{iT}}\min(p_a,1)}{a_{iT}} \tag{1}$$

式中：短期信用$C_S(i,T)$是通过平均最近一个交易

周期中的电力交易得到的，是对节点 i 在最近 a_{iT} 笔交易中发电行为的评估，这里 $C_S(i,T)\in[0,1]$；$p_a=E_{ia}/e_{ia}$，E_{ia} 为节点 i 进行第 a 次交易的实际交易电量，e_{ia} 为节点 i 进行第 a 次交易的合同申报电量。将主体与交易记录的对应关系表示为映射 $f_\kappa: I\rightarrow\{\kappa\}$。将主体 i 的表现记录表示为 $f_\kappa(i)$。

由于新能源电力公司供电易受到环境的影响，因此需要一个衡量电力公司长期供电稳定性的指标函数。

定义 2　长期表现记录。电力公司主体的长期表现记录 $\omega=(T_{idi},C_{idi},\alpha,F)$。其中，$T_{idi}$ 为电力公司主体进行交易的周期标记；C_{idi} 为初始信用值；α 为历史因子；$F=<(T_1,C_{i1}),(T_2,C_{i2}),\cdots,(T_{d_T},C_{id_T})>$ 是一个队列，包含最近 d_T 个电力交易周期信用值的变化，$(T_d,C_{id})(d=1,2,\cdots,d_T)$ 表示电力公司节点 i 在第 T_d 个交易周期后其信用值变化为 C_{id}。

长期信用 $C_L(i,T)$ 是主体在电力交易事件中的表现度量值的累积，其计算公式为：

$$C_L(i,T)=\alpha C_L(i,T-1)+(1-\alpha)C_S(i,T) \tag{2}$$

式中：$C_L(i,T)$ 是通过将 $C_S(i,T)$ 与旧的信用值 $C_L(i,T-1)$ 进行聚合计算得到的，这里 $C_L(i,T)$，$C_S(i,T)$，$\alpha\in[0,1]$，对于不诚信的节点，$C_L(i,T)$ 值偏小，反之偏大，α 为节点过去电力交易事件的给定权值，α 值决定了长期信用值的积累和下降速度，即其值越低，旧的信用值被遗忘的速度越快，受过去行为的影响就越小，反之亦然，为了提高电力公司的有效性，α 应大于 $1-\alpha$，因为一个公司的信用不能只看其短期内的积极性，还要保证能长期供电的稳定性。

将主体与交易记录的对应关系表示为映射 $f_\omega: I\rightarrow\{\omega\}$。将主体 i 的表现记录表示为 $f_\omega(i)$。

2.2　价格匹配

每个电力公司根据自身的投资、发展需求，给出在第 T 个交易周期中能源发电的电力报价 $P(i,T)$。文献[3]提出一种基于新能源供需关系的新能源定价机制，合理的电价可平衡电力交易中电力公司和消费者的利益，电力公司的电力报价 $P(i,T)\in[0,1]$。

基于节点在上一个时间周期中的交易行为给出对应的匹配度。匹配度的计算公式为：

$$\frac{1}{M(i,T)}=\frac{1}{C_L(i,T-1)}+P(i,T) \tag{3}$$

式中：$M(i,T)$ 为消费者对电力公司 i 在第 T 个交易周期匹配度的综合打分，可知 $M(i,T)$ 等于 $C_L(i,T-1)$ 和 $1/P(i,T)$ 的调和平均值。将主体与匹配度的对应关系表示为映射 $f_M: I\rightarrow\{M\}$。将主体 i 的表现记录表示为 $f_M(i)$。

消费主体在微电网中购电时，不仅要考虑购电成本，还要考虑交易方供电能力的稳定性。消费者在收到生产者反馈的电力报价后，从本地区块中获取该生产者的长期信任值，并利用式(3)的调和平均公式计算得到的交易匹配值筛选出合适的交易生产者。匹配值越大，表示该电量交易完成度和购电价格两方面的综合满意度越高，交易消费者更能够信任该生产者达成该笔交易的能力。

3　电力交易交割策略

在微电网电力交易的区块链交易过程中，以区块链的方式促成并完整地记录电力交易过程，这主要是通过智能合约实现的。智能合约是交易平台的核心代码，是满足消费者交易需求的数字匹配规则。本文设计的智能合同主要包括发布交易请求、交易价格匹配、缴纳保证金和交易结算 3 个功能模块。其中发布交易请求和交易价格匹配模块为交易阶段，缴纳保证金和交易结算为交割阶段。

3.1　发布交易请求

微电网的所有电力交易参与方时刻监听微电网通信网络的区块链信息。消费主体提交拟交易电量，用自身的私钥加密再经 Hash 算法产生电力交易需求信息摘要后，将加密的摘要与电力交易需求信息加入区块链中，并通过微电网通信网络向微电网的所有电力交易参与方广播包含该电力交易需求的区块链信息。

定义 3　申报信息。申报信息 $s=\left(j,t,e,j_{sig}\left(t\|e\right)\right)$。其中，$j$ 为消费主体的身份标识，在入网时颁发，且不可改变；t 为时间凭证，由消费主体向认证机构申请，是消费主体在申报发出时所处的时间点证明；e 为申报电量，由消费主体自主发起；$j_{sig}\left(t\|e\right)$ 为消费主体对交易发起时间和申报电量的数字签名。

消费者发布自身的申报信息到区块链网络中，每个电力公司接收包含最新交易请求的区块链信息，并根据自身的发电情况判断是否接受该电力交易。如果不接受，则忽略该交易。如果有交易意向，则对消费主体申报的电量进行检测，然后根据发布电力申报信息的参与方公钥解密发布方的 Hash 摘要，并与收到的电力交易需求信息的 Hash 计算值进行比较验证。当 2 个信息摘要的数值一致时，则可判断该区块链信息没有被伪造或篡改，是发布方发出的真实电力交易请求；反之，则丢弃该区块链信息。验证通过后电力公司用自身的私钥加密有交易意向的区块链信息并发给该电力交易需求的发布方。

定义 4　回复信息。回复信息 $r=\left(i,t^c,p,i_{sig}\left(t^c\|p\|s\right)\right)$。其中，$i$ 为电力公司的身份标识，在入网时颁发，且不可改变；t^c 为时间凭证，由电力公司主体向认证机构申请，是电力公司主体在回复信息时所处的时间点证明；p 为电力报价，由电力公司主体自主发起；$i_{sig}\left(t^c\|p\|s\right)$ 为电力公司主体对申报信息回复时间

和电量的数字签名。

电力公司广播自身的回复信息到区块链网络中，将包含同一申报信息s的回复集合记为$R=\{r_1, r_2, \cdots, r_n\}$，其中$r_g$($g$=1，2，…，$n$，$n$为回复信息总条数)表示收到的第$g$条回复信息。

3.2 交易价格匹配

消费主体接收所有的电力交易意向信息，并根据各产消者的历史信用值和售卖的实时电价，筛选出最有可能达成电力交易意向的电力公司，达成电力交易协议。若消费主体对所有的电力交易意向信息不满意或没有收到对该次交易的返回信息，则终止该次所发起的电力交易意向。交易价格匹配算法见附录A算法1。

3.3 缴纳保证金和交易结算

初步达成电力交易意向的电力交易供需双方，监管机构对生产方进行均衡保证金和交易结算。在电力交易双方约定的交易信息保密范围内，双方可以将自身完成交易的证明尽可能地记录到区块链中，在出现交易纠纷时为自身尽力履行电力交易提供证明。

在每个时段各节点都会从智能设备中读取其在该时段中注入微电网的新能源量或消耗的电能量的信息。在该时段结束时，发电方智能设备反馈发电量，购电方智能设备反馈用电量，结合两者电量情况触发最终结算，其他节点收到信息后将所有信息集中处理，这样能有效避免购电方在收到电能量后不提交交易完成的信息。交易完成后矿工从交易池中打包交易信息并存储到区块链中。

交易交割流程如图3所示。

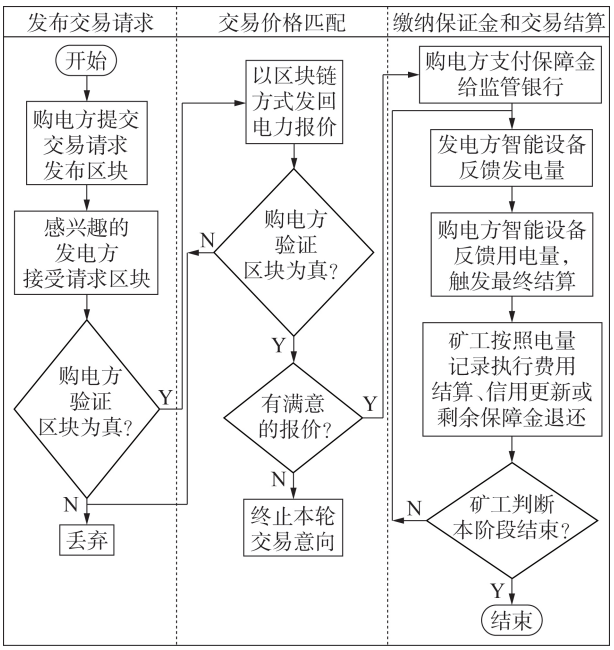


图3 交易交割流程图

Fig.3 Flowchart of transaction closing

4 区块链系统

4.1 记账权

为了保证数据的全局一致性，每个区块只能由唯一的节点生成，即记账节点。本文使用工作量证明POW(Proof Of Work)机制来分配记账权，每个记账节点需要对发电公司的交易情况计算出对应的信用值。区块链系统整体框架图见附录A图A1。

4.2 块头结构

定义5 区块链。区块链$\phi=(B_o, f_p)$。其中，$B_o=\{b\}$为区块集合，区块b包含块头和块体2个部分，分别记为b_{header}、b_{body}。映射$f_p: B_o \rightarrow B'_o$是区块的前向链接关系，$f_p(B_o)=B'_o$表示区块$B'_o$是$B_o$的直接前驱。

块头结构见附录A表A1。

4.3 块体结构

区块的块体是一棵以叶子节点为交易依据的Merkle树，称为交易树。对构成树结构用节点集合Q和节点连接集合$C=\left\{(m_1, m_2)\,\middle|\, m_1, m_2 \in Q\right\}$描述，定义谓词TranTree($Q$,$C$)，当TranTree($Q$,$C$)为真时，满足：$\exists$唯一的$v \in Q$，$\neg\exists(m_1, r) \in C$；$\forall m_2 \in Q \wedge m_2 \neq v$，$\exists$唯一的$(m_1, m_2) \in C$。

块体交易信息见附录A表A2。

定义6 交易树。交易树$\Psi_\chi=(Q_h \cup \chi^T, C)$。其中，$Q_h$为Hash值节点集合，$\chi^T$为交易依据集合，叶子节点都是交易节点。

$C=\left\{(m_1, m_2)\,\middle|\, m_1 \in Q_h, m_2 \in Q_h \cup \chi^T\right\}$是各个节点之间的连接，并且$\chi^T$满足：$\forall m_1 \in Q_h$，有且只有$m_2$，$m_3 \in Q_h \cup \chi^T$，$(m_1, m_2), (m_1, m_3) \in C \wedge m_1 = h\left(m_2 \| m_3\right)$；TranTree$(Q_h \cup \chi^T, C)$=true。$h\left(m_2 \| m_3\right)$表示对$m_2$和$m_3$的连接结果取Hash值。对交易依据集合$\chi^T$中交易依据$\chi$进行Hash运算时，将其转换为二进制串。将由交易依据集合χ^T创建Merkle树的过程记为χ^T_{st}，将交易树Ψ_χ的根节点记为$\Psi_{\chi root}$。由于任何一个叶子节点被篡改都会自下而上直至根节点引起一连串Hash值的变化，致使Merkle_root发生变化，并导致块头的Hash值发生变化，最终使整个区块链断裂，使用Merkle树存储交易可以保证交易依据很难被篡改。

4.4 共识阶段

基于自身算力，矿工在挖到区块后会从打包区块的交易中收取一定比例的奖励。一个周期中所有N个挖矿矿工构成出块序列Q_{block}，共识过程使所有区块链节点的数据保持一致，包含区块生成和区块验证2个部分。

对由同一电力公司主体i达成的交易集合S验证交易完成比p_{in}。为了保证区块的有效性，规定每个区块最少包含p^S_{in}个交易依据。区块生成算法见附录A算法2。

记账节点从消息池中取出未上链的消息，组织

为交易集合 S 进行交易完成比 p_{in} 验证，形成等量的交易依据 χ。由交易依据集合 χ^T 生成块体，即交易树 Ψ_χ，将交易树 Ψ_χ 的根 Hash 值记为 h。时间戳则是向认证服务器申请获得的。

矿工节点 i 在生成区块 b 之后，将区块消息（i，b，$i_{sig}(b)$）（$i_{sig}(b)$ 为电力公司对区块 b 的数字签名）在网络中广播。收到区块消息的序列节点首先验证 $j_{sig}(b)$（$j_{sig}(b)$ 为消费主体对区块 b 的数字签名）是否合法，区块合法性验证的内容包括区块高度是否合法、块体所含交易的发生时间是否在所属周期范围内、块体所含交易签名是否合法。全局一致性验证算法见附录 A 算法 3。

统计收到的 h 值与自身的 h 值相同的数量 Z，将自身的 h 值记为 H_{ver}，记当前出块节点广播的 Hash 值为 H_{block}。其余 $N-1$ 个矿工对 H_{block} 进行验证投票，若 $H_{block}=H_{ver}=h$，则投赞成，并发给监管节点，否则反对。统计赞成票数 Z，在监管节点收到大于 $N/2$ 的矿工赞成出块信息时，则出块成功，广播全网将区块连接到本地账本末尾区块，否则惩罚该出块挖矿节点，将其从挖矿序列 Q_{block} 剔除，剩余矿工重复该操作。共识流程如图 4 所示。

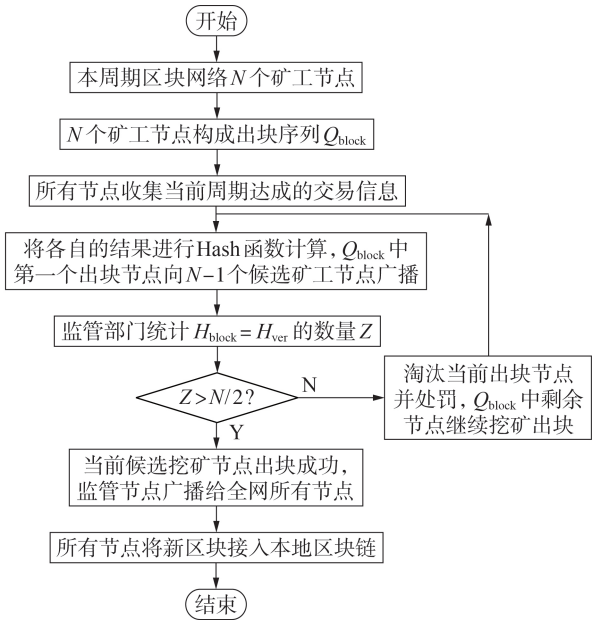


图 4　共识流程图

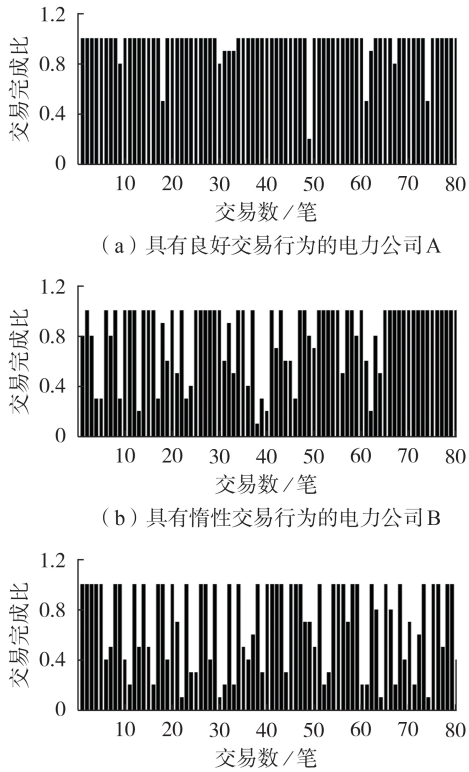
Fig.4　Consensus flowchart

块体中的交易消息验证通过后需将其从消息池中移除，避免重复打包。若区块通过了合法性验证，但不是链接到末尾区块，则视为无效区块，不予上链。

5　算例仿真

5.1　信任分析

电力公司的初始信用值和初始交易额都设置为 0，并规定：若其实际发电量不小于合同协议量，则该次交易完成比为 1；若其实际发电量小于合同协议量，则该次交易完成比为交易完成比。图 5 为 3 个电力公司分别达成 80 次电力交易的交易完成比分布情况的直方图。



（a）具有良好交易行为的电力公司 A

（b）具有惰性交易行为的电力公司 B

（c）具有消极交易行为的电力公司 C

图 5　基于节点交易行为的交易完成比

Fig.5　Transaction completion ratio based on node transaction behavior

由图 5 可知：电力公司 A 的行为较为稳定，绝大多数交易表现是合格的；电力公司 B 以惰性的交易表现居多，但在一段较短的时间内进行了大量的合格交易；电力公司 C 的交易行为一直处于消极状态，对交易的态度时好时坏，交易表现长期处于不合格状态。

每个交易周期取 8 笔交易作为信任指标的计算点，共进行 10 个交易周期，α 取值 0.7。图 6 为 3 个电力公司信用值的变化情况。由图中可以看出：电力公司 A 的信用值指标最好；电力公司 B 前期由于恶

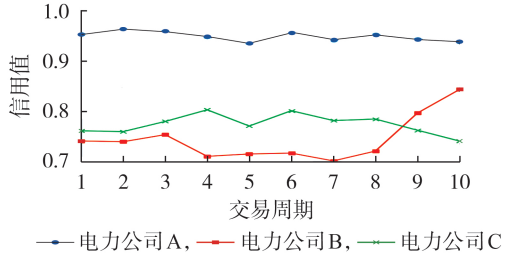


图 6　基于不同电量交易的信用值变化

Fig.6　Change of trust value based on different electricity quantity transaction

意交易行为与电力公司C的信用值接近，在后2个交易周期由于良好的交易记录其信用值有了一定的回升，但因为历史信用的劣迹仍达不到电力公司A的信用值。信用值作为累积型的评估指标，从侧面反映了总量上主体的表现。

5.2 匹配度分析

图7为基于电价的交易匹配变化情况。其中电力公司A、B、C在10个交易周期的平均信用值分别为0.94、0.74、0.77。可以看出，基于同样的价格，信用良好的电力公司A的匹配度在任意同等价格下都远高于B和C，这说明良好的交易行为更有利于与消费者达成合同。随着价格的上涨，交易匹配度出现了明显的下降，在同一匹配度0.6下，电力公司B、C的电价分别为0.32、0.35元／(kW·h)，而电力公司A的电价为0.63元／(kW·h)，几乎是前两者的2倍，因此电力公司A有明显的匹配优势。电力公司B和C的匹配度曲线相近，这说明在长期的劣质交易后即使在近期有良好的交易记录，电力公司主体的匹配度也不会立刻得到大幅提升。

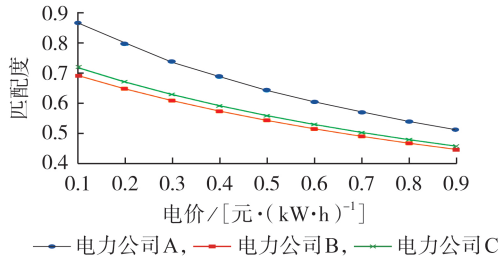


图7 基于电价的匹配度

Fig.7 Matching degree based on electricity price

匹配度随$C_L(i,T-1)$和$P(i,T)$的变化情况见图8，图中$M'(i,T)=C_L(i,T-1)/\sqrt{C_L^2(i,T-1)+P^2(i,T)}$为基准方法的结果。由图可见，相比$M'(i,T)$，$M(i,T)$的取值曲面更加平滑，即不会因单个变量的小范围变化而造成匹配度的剧烈波动。

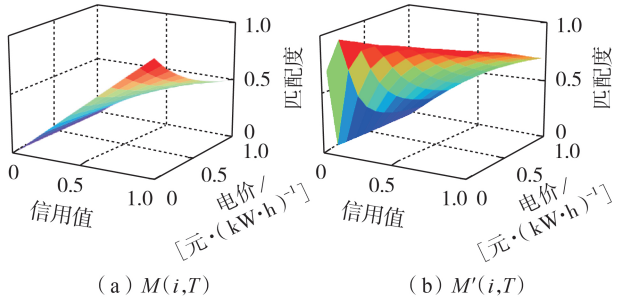


图8 匹配度随$C_L(i,T-1)$和$P(i,T)$变化情况

Fig.8 Change condition of matching degree along with $C_L(i,T-1)$ and $P(i,T)$

5.3 安全性分析

在此DME中由于POW机制，矿工挖矿需要耗用时间、设备与电力作为担保成本，一些节点的算力有限，而高算力的节点主要是一些电能的生产者。若这些参与者消耗巨大的电量来挖矿进行分叉攻击谋取利益，则在电力交易中有点得不偿失，因为矿工的出块奖励是块中达成的交易金的一定比例(5%左右)，当以虚假信息出块时，经4.4节的验证过程知$Z<N/2$，因此得不到出块奖励。

当少数恶意节点联合造假时，有可能会使区块链出现分叉的现象，此时可以采用双向的确认机制，防止网络故障区块链硬分叉，见附录A图A2。由监管节点统一该周期的合法区块记账节点的认可数，根据多则胜出的原则，将2个区块合并到统一的区块链中。在正常网络下，选取节点B作为区块生成节点，另外的4个节点A_1—A_4为普通节点。在故障网络下，节点D为区块生成节点，节点C_1和C_2为普通的主节点。从图中可以看出，正常网络中的节点B获得区块生成的赞同票数为4，而在故障网络中的节点D获得的票数为2，因此节点D生成的区块为不合法的区块，需要将该区块丢弃，并将节点B生成的区块内容同步到主区块链中。

基于区块链的交易，将挖矿难度设置为5，区块链交易记录图见附录A图A3。电力公司address1与用户address2达成50 kW·h的电力交易，交易Tran_ID转化为Hash值0x00000220492945F8，方便区块记录存储。挖矿奖励为100，电力公司address3耗时14.352 744 s挖矿成功后不会立刻收到奖励，而是在待处理交易池中产生一些新的交易并在下一次挖矿成功后此次挖矿奖励才会真正地到账户上，这样有利于提高节点参与区块链运维的积极性。

6 结论

在微电网交易的应用场景中，针对不依赖于可信第三方与额外信任假设难以在纯分布式微电网中进行信任管理与交易的问题，本文借助区块链与匹配机制设计了适用于微电网交易主体信任评价的方法，以实现对分布式微电网中主体的信任管理。基于主体的历史交易完成比，对每个电力售卖者进行信用评分，通过信用-价格匹配机制，在电力交易过程中结合给出的售电价格，使用户和电力公司在相互之间没有信任的前提下匹配到最适合的交易对象，完成电力交易。

附录见本刊网络版(http://www.epae.cn)。

参考文献：

[1] 朱文广，熊宁，钟士元，等. 基于区块链的配电网电力交易方法[J]. 电力系统保护与控制，2018，46(24)：165-172.
ZHU Wenguang，XIONG Ning，ZHONG Shiyuan，et al. Power trading method for distribution network based on block chain[J]. Power System Protection and Control，2018，46(24)：165-172.

[2] 龚钢军，张心语，张哲宁，等. 计及大用户负荷管理的可再生能

源消纳[J]. 电网技术,2020,44(8):2922-2932.
GONG Gangjun,ZHANG Xinyu,ZHANG Zhening,et al. Renewable energy consumption based on large consumer load management[J]. Power System Technology,2020,44(8):2922-2932.
[3] 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[J]. 浙江师范大学学报(自然科学版),2019,42(3):248-253.
CHEN Zhongyu,LÜ Liqun,LIN Feilong. Design and optimization of power pricing in the blockchain-based smart grid[J]. Journal of Zhejiang Normal University(Natural Sciences),2019,42(3):248-253.
[4] 张志伟,陈丹,杨爽,等. 基于区块链技术的配电网电力交易方法研究[J]. 自动化与仪器仪表,2020(8):205-209.
ZHANG Zhiwei,CHEN Dan,YANG Shuang,et al. Research on power trading method of distribution network based on block chain technology[J]. Automation & Instrumentation,2020(8):205-209.
[5] 徐嘉辉,马立新. 区块链技术在分布式能源交易中的应用[J]. 电力自动化设备,2020,40(8):17-22,30.
XU Jiahui,MA Lixin. Application of blockchain technology in distributed energy transaction[J]. Electric Power Automation Equipment,2020,40(8):17-22,30.
[6] 郭上铜,王瑞锦,张凤荔. 区块链技术原理与应用综述[J]. 计算机科学,2021,48(2):271-281.
GUO Shangtong,WANG Ruijin,ZHANG Fengli. Summary of principle and application of blockchain[J]. Computer Science,2021,48(2):271-281.
[7] 任彦冰,李兴华,刘海,等. 基于区块链的分布式物联网信任管理方法研究[J]. 计算机研究与发展,2018,55(7):1462-1478.
REN Yanbing,LI Xinghua,LIU Hai,et al. Blockchain-based trust management framework for distributed Internet of Things[J]. Journal of Computer Research and Development,2018,55(7):1462-1478.
[8] SAXENA S,FARAG H E Z,BROOKSON A,et al. A permissioned blockchain system to reduce peak demand in residential communities via energy trading:a real-world case study[J]. IEEE Access,2020,9:5517-5530.
[9] 陈启鑫,王克道,陈思捷,等. 面向分布式主体的可交易能源系统:体系架构、机制设计与关键技术[J]. 电力系统自动化,2018,42(3):1-7,31.
CHEN Qixin,WANG Kedao,CHEN Sijie,et al. Transactive energy system for distributed agents:architecture,mechanism design and key technologies[J]. Automation of Electric Power Systems,2018,42(3):1-7,31.
[10] 赵银波,高红均,王仲,等. 考虑用户电能替代的商业园区运营商多能交易博弈优化决策[J]. 电网技术,2021,45(4):1320-1331.
ZHAO Yinbo,GAO Hongjun,WANG Zhong,et al. Multi-energy trading game optimization decision-making of business park operators considering user electric energy substitution[J]. Power Grid Technology,2021,45(4):320-1331.
[11] PAUDEL A,CHAUDHARI K,LONG C,et al. Peer-to-peer energy trading in a prosumer-based community microgrid:a game-theoretic model[J]. IEEE Transactions on Industrial Electronics,2019,66(8):6087-6097.
[12] WANG W,LIU L,LIU J Z,et al. Energy management and optimization of vehicle-to-grid systems for wind power integration[J]. CSEE Journal of Power and Energy Systems,2020,7(1):172-180.
[13] 陟晶,张高航,邵冲,等. 含大规模风电及光热电站的电力系统优化调度方法[J]. 电力工程技术,2021,40(1):79-85.
ZHI Jing,ZHANG Gaohang,SHAO Chong,et al. Optimal dispatching method for power system with large scale wind power and concentrated solar power plant[J]. Electric Power Engineering Technology,2021,40(1):79-85.
[14] 方响,马笛,侯伟宏,等. 分布式新能源接入下的区块链共识机制研究[J]. 浙江电力,2019,38(7):1-6.
FANG Xiang,MA Di,HOU Weihong,et al. Research on the blockchain consensus mechanism for distributed renewable energy access[J]. Zhejiang Electric Power,2019,38(7):1-6.
[15] OGAWA D,KOBAYASHI K,YAMASHITA Y. Blockchain-based optimization of energy management systems with demand response[C]//2020 IEEE 9th Global Conference on Consumer Electronics(GCCE). Kobe,Japan:IEEE,2020:58-59.

作者简介:


邓明辉

邓明辉(1996—),男,湖北孝感人,硕士研究生,主要研究方向为能源区块链(**E-mail**:837022475@qq.com);

唐郑熠(1984—),男,福建福州人,副教授,博士,通信作者,主要研究方向为区块链技术、形式化方法、数据挖掘(**E-mail**:tangzy84@126.com);

黄　达(1997—),男,安徽巢湖人,硕士研究生,主要研究方向为能源区块链(**E-mail**:1250434127@qq.com)。

(**编辑**　王锦秀)

Power transaction matching mechanism of microgrid based on block chain

DENG Minghui[1],TANG Zhengyi[1,2,3],HUANG Da[1],HU Wenyu[1,2,3]

(1. School of Computer Science and Mathematics,Fujian University of Technology,Fuzhou 350118,China;
2. Key Laboratory of Hunan Province for Mobile Business Intelligence,Hunan University of Technology and Business,Changsha 410205,China;3. Fujian Provincial Key Laboratory of Big Data Mining and Applications,Fuzhou 350118,China)

Abstract:Aiming at power transaction problem of renewable energy in microgrid,a matching strategy suitable for transaction is proposed based on historical transaction completion degree. The matching degree is quantified into the investigation of entity credit and power selling price,and the block chain is used to realize effective sharing and cycle assessment of credit data. When the consumer receives power price information of different producers when buying power,he can know the producers' transaction credit from block chain account book and select suitable transaction party. Example analysis shows that the proposed strategy can effectively quantify credit,and match the most suitable transaction party combing with power selling price.

Key words:block chain;power transaction;renewable energy;matching strategy;distributed

附录 A：

算法 1 交易价格匹配。

Input：s

Output：$f_M(r)$ or null

$R = \{r_1, \quad r_2, \cdots, r_n\}$

For all $r \in R$ Then

If $s.t \in \omega.T \wedge r.t^c \in \omega.T$ Then

$f_M(r)$ =cal_M(r.$f_\omega(C_l)$，$r.p$)

End If

End For

Return $f_M(R)$

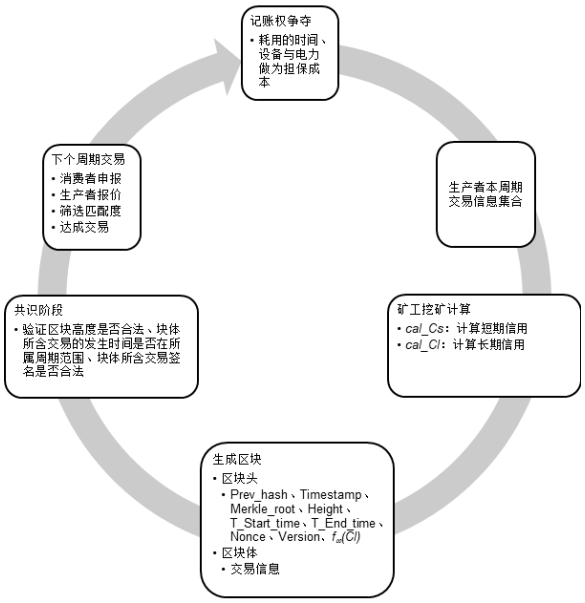


图 A1 区块链系统整体框架图

Fig.A1 Diagram of overall block chain system framework

表 A1 区块的块头结构

Table A1 Bulk structure of a block

元素	说明
Prev_hash	父区块的块头 Hash 值
Timestamp	区块生成时间
Merkle_root	块体中的 Merkle 树的树根
Height	区块在链中的位序
T_Start_time	交易周期开始时间
T_End_time	交易周期结束时间
Nonce	随机数
Version	版本号

表 A2 交易信息

Table A2 Transaction information

元素	说明
Tran_ID	交易账单
Tran_from	电力供给公司
Tran_to	消费主体
Tran_C	电力公司信用
Tran_p	交易售价
Tran_E	交易额度
Tran_e	申报额度

算法 2 区块生成。

Input：电力公司节点 i 的交易集群 S

Output：A block b or null

Height = n

Get Timestamp from certificate server

Get the last block b'：Pre_hash := $h(b')$

$\chi^{T} := \varnothing$

Get $S^{T} = \{S_1, S_2 \ldots\}$ from transaction pool:

For each $S \in S^{T}$ Then

  $\chi = (p_{in}, S)$

  $\chi^{T} := \chi^{T} \cup \{\chi\}$

  If $p_{in}.t <$ T_Start_time Then

    T_Start_time := $p_{in}.t$

  End If

  If $p_{in}.t >$ T_End_time Then

    T_End_time := $p_{in}.t$

  End If

End For

$f_{\kappa}(C_s)$=cal_Cs(p_{in}^{S})

$f_{\omega}(C_{l})$=cal_Cl($f_{\kappa}(C_s)$，$\omega.\alpha$)

Ψ_{χ} := χ_{st}^{T}

Merkle_root := $\Psi_{\chi root}$

b_{header} := (Pre_hash，Timestamp，Merkle_root，Height，T_Start_time，T_End_time，Nonce，Version)

body(b) := Ψ_{χ}

Return b

算法 3 全局一致性验证算法。

Input：节点的交易列表

A block b

Output：valid or invalid

For each χ in b_{body}:

For each s in $\chi.S$:

If $s.t < b_{header}$.T_Start_time

$\vee$ $s.t > b_{header}$.T_End_time Then

Return invalid

End If

If $r.i_{sig}(t^{c} \| p \| s)$ is illegal Then

Return invalid

End If

Remove s from transaction pool

End For

End For

Get the last block b'

If b_{header}.Pre_Hash $\neq h(b')$

Return invalid

End

If b_{header}.Height $\neq b'_{header}$.Height + 1

Return invalid

End

Return valid

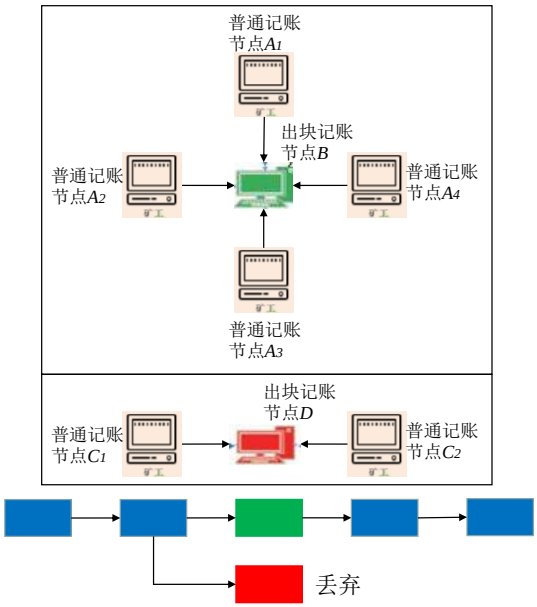


图 A2 防止网络故障区块链硬分叉

Fig.A2 Preventing block chain hard bifurcation for network failure

```
<__main__.Transaction object at 0x0000022049294 5F8>
{"from_address": "address1", "to_address": "address2", "amount": 50}
挖到区块:00000234e814f2a5a4dd98bf879fa88d2a4d6ee74b8b6c36c4b99de664c75f43, 耗时: 14.352744秒
address1   -50
address2   50
address3   0
挖到区块:00000c818745bc79d2af566b023a4267e7979ccf6d39267c822487d806b6cc73, 耗时: 12.525125秒
address1   -50
address2   50
address3   100
```

图 A3 区块链交易记录

Fig.A3 Block chain transaction records