计算机科学
COMPUTER SCIENCE

基于区块链的可靠电力数据调度方案

马军伟, 潘秀魁, 王玉琪, 巫健, 杜锋

引用本文

马军伟, 潘秀魁, 王玉琪, 巫健, 杜锋. 基于区块链的可靠电力数据调度方案[J]. 计算机科学, 2024, 51(11A): 231100178-8.

MA Junwei, PAN Xiukui, WANG Yuqi, WU Jian, DU Feng. Reliable Power Data Scheduling Scheme Based on Blockchain [J]. Computer Science, 2024, 51(11A): 231100178-8.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231100178

基于区块链的可靠电力数据调度方案

马军伟[1]　潘秀魁[2]　王玉琪[2]　巫　健[1]　杜　锋[1]
1 国网山西省电力公司　太原 030021
2 国网区块链科技(北京)有限公司　北京 100053

摘　要　智能物联网的高速发展使得电网中的电力信息资源能够实现高效聚合。区块链技术的不可篡改性、透明性、高可用性,使得共享信息变得更加安全和高效。随着能源电力市场的开放,负荷调控、优化配置等需求日益迫切。在信息收集阶段可以通过电网中的智能设备收集电力数据,但在电力数据调度阶段存在信息共享壁垒、虚假信息威胁等问题,严重影响调度效益。为此,设计一种基于区块链的可靠电力数据调度方案。该方案利用区块链实现调度信息共享,链下设计适用于电力调度场景的智能终端设备准入机制,将调度风险规避在链下;设计基于数据可靠性评估的电力数据发布方法及基于效益理论的多策略调度模型,保障上链数据的可靠性,实现数据调度风险的可控;设计基于动静态评价结合的信任更新计算方法,实现用户调度行为量化上链。通过对调度成功率、系统总收益等指标进行仿真实验,验证了该方案的有效性。

关键词:智能物联网;负荷调控;区块链;多策略调度;效益理论
中图分类号　TP391

Reliable Power Data Scheduling Scheme Based on Blockchain

MA Junwei[1],PAN Xiukui[2],WANG Yuqi[2],WU Jian[1] and DU Feng[1]
1 State Grid Shanxi Electric Power Company,Taiyuan 030021,China
2 State Grid Blockchain Technology(Beijing) Co.,Beijing 100053,China

Abstract　The rapid development of the intelligent Internet of Things(IoT) has enabled efficient aggregation of electrical information resources in the power grid. The immutability,transparency,and high availability of blockchain technology enhance the security and efficiency of shared information. With the opening of the energy and electricity market,the demand for power resource integration,load regulation,and optimized allocation has become increasingly urgent. During the information gathering stage,electricity data can be collected through intelligent devices in the power grid. However,in the stage of electricity data dispatch,there are barriers to information sharing and threats of false information,which seriously affect dispatch efficiency. In this paper,a reliable power data dispatch scheme based on blockchain is proposed. The scheme utilizes blockchain to achieve information sharing in dispatching,and off-chain design for intelligent terminal device access mechanisms applicable to electricity dispatch scenarios. It designs a power data publication method based on data reliability assessment and a multi-strategy dispatch model based on utility theory to ensure the reliability of on-chain data and achieve controllable data dispatch risks. Furthermore,it designs a trust update calculation method based on dynamic and static evaluation combination to quantify user dispatching behaviors on the blockchain. The effectiveness of the proposed scheme is validated through simulation experiments on dispatch success rate,total system revenue,and other indicators.

Keywords　Smart Internet of things,Load regulation,Blockchain,Multi-strategy scheduling,Utility theory

1　引言

随着新能源的发展,电力资源日趋多元化。积极调整能源结构,大力发展新能源建设,优化电力资源配置,提升电力资源利用效率是大势所趋[1]。同时,国家为了适应市场化需求,建立了新的开放型能源电力市场,众多的电力资源个体户开始涌现。个体户的加入[2],为电力资源配置增加了更多的灵活性。新的市场结构下,设计与开放型市场相匹配的新的资源配置优化方案是必要的[3]。

由于能源电力市场的逐步开放,出现了越来越多的小型电力资源户(下称个体户)与公司化的资源户(下称公司户)。资源用户的多元化使得在调度方面不仅存在信息壁垒,也存在诸多安全隐患。由于信息无法及时共享,电力信息传输过程中存在数据篡改和信息泄露风险[4-5]。数据本身的语义的可靠性问题,都会导致调度效益的下降。如何兼顾安全与效益,是需要解决的一大问题。

智能物联网和区块链技术的结合,为这些问题提供了新的解决方案。智能物联网技术通过终端传感器、设备和互联网连接了整个电网系统,实现了实时监测、数据收集和分析[6]。电网运营商能够更好地了解电力系统的运行状况,快

基金项目:国网山西省电力公司科技项目(52051C220004)
This work was supported by the State Grid Shanxi Electric Power Company Technology Project(52051C220004).
通信作者:马军伟(junweima@foxmail.com)

速响应故障，提高能源利用效率，并支持智能化的电能管理[7]。电网中智能终端通过对收集的数据进行加密，降低了数据篡改和信息泄露风险，但数据本身的语义的可靠性没有得到保证。随着区块链技术的发展，考虑将能源市场与区块链技术相结合的理念也相继被提出[8-9]。区块链技术的去中心化、公开透明的特点，能够很好地解决信息共享壁垒的问题，促进能源电力市场各方的信息互通，推动能源电力的按需调配[10]。依托于区块链技术，电力资源共享变得更加方便快捷，有效地助力了能源电力资源的配置优化。但区块链技术也不是万能的，针对链上共享信息的安全及可靠性问题，便变得束手无策。

在智能物联网得到了快速发展的大场景下，保障共享信息安全性的研究有很多。例如文献[11]中提出的 SPINS 协议，实现了通信的机密性、完整性、新鲜性及点到点的消息认证，但其认证涉及的多轮交互复杂性，使得其不适用于对吞吐量要求高的实时交互场景；文献[12]中使用同态加密和 PBFT 解决了数据安全和隐私问题，但未考虑用户效益和系统风险的影响；文献[13]提出了一个两阶段调度算法，考虑了电动汽车和新能源用户的个体电力成本的最优调度，但未考虑安全性；文献[14]中提出的一种新的具有合理效率的消息认证方案，满足智能电网实际实施和部署的安全性和轻量级要求，但无法保障调度信息的可靠性，且认证仅在准入阶段生效，未对后续行为进行监督约束；文献[15]中提出的可证明安全且匿名的智能电网消息认证方案，为智能电网提供了相互认证和密钥建立，但认证的复杂性导致其不适合分布式的电力调度交互场景。

综上所述，针对保障共享信息的安全，现有研究多采用加密或认证的方式，缺乏对信息本身语义可靠性的保证。本文针对此问题，设计融合零信任的基于调度行为分析的信任评估机制，通过对电力数据的可靠性进行评估，规避虚假数据发布风险，结合用户发布行为评分，依据动静结合的信任更新算法，满足电力数据的可靠性需求；为解决信息可靠性和调度效益兼顾问题，设计基于效益理论的多策略调度模型，通过在个体户调度过程中基于效益理论，实现用户调度的风险与信任量化，结合系统当前风险状态和用户的效益值，进行综合考量，保障安全性的同时极大化调度效益。

2 背景知识

2.1 区块链与智能合约

区块链技术融合了密码学、智能合约、分布式存储、拜占庭容错(BFT)和共识算法、点对点网络等一系列技术，使区块链拥有去中心化、不可篡改、公开透明和可追溯性[16]的特征。区块链的这些特点使其能够很好地应用于能源电力场景，保证能源电力场景下的数据可信[17-18]。智能合约部署在链上，使得不可信实体间的可信交互变得可行[19]，无需经由第三方权威机构，解决了中心化的信任机制问题[20]，能够很好地应用于电力数据调度场景，对调度数据进行自动可靠的评估。

2.2 效益理论及零信任

效益理论通过效益函数和期望效益函数，对参与交互的用户进行收益和风险的评估，指导决策[21]。在安全领域存在诸多导致风险的因素，如实体自身漏洞、运行环境潜在的威胁等，评估风险和信任的目的是保障系统的调度安全性和运行经济性[22]。效益理论的函数[23]如下：

$$U_i=\frac{1}{\theta}(B-C)^{\theta} \tag{1}$$

$$\theta=\begin{cases}1<\theta\leqslant 2, & \text{风险追求}\\ 1, & \text{风险中立}\\ 0<\theta<1, & \text{风险规避}\end{cases} \tag{2}$$

其中，B 表示行为预期收益，C 表示行为潜在成本，θ 为当前风险态度，U_i 表示用户 i 的正向收益。

通过对电力用户进行风险和收益分析，供决策中心选择最佳的调度方式，能够同时兼顾安全与效益。“永不信任、持续验证”是零信任的根本思想[24]。对零信任网络而言，不存在特权用户，加入网络的一切实体都是不可信的[25]。将零信任的理念应用于电网数据调度场景，能够很好地保障调度系统的安全性。

3 可靠电力数据调度方案

本文提出基于区块链的可靠电力数据调度方案，方案主要包含 4 个阶段，分别为准入阶段、电力数据发布阶段、调度决策阶段与信任更新阶段，如图 1 所示。针对准入阶段，设计了基于 RSA 与 PKI 的准入机制，保障用户的入网安全；针对电力数据发布阶段，设计了电力数据可靠性评估方法，将数据安全风险规避在链下；针对调度决策阶段，设计了基于效益理论的多策略调度方案，通过风险评估和效益计算保障调度决策的可靠；针对信任更新阶段，设计了基于动静态评价结合的信任更新计算方法，通过对调度用户参与整个调度过程的行为评价来计算用户信任，通过信任奖惩约束用户调度行为。

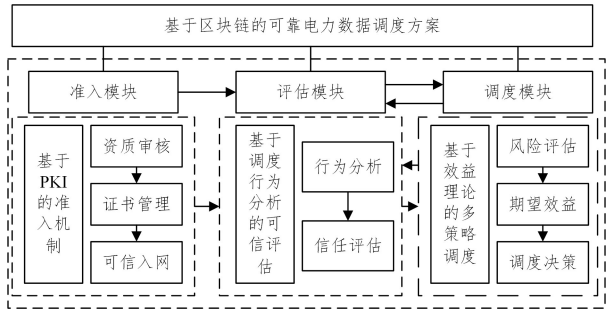

图 1 整体方案设计

Fig. 1 Overall scheme design

3.1 基于 RSA 与 PKI 的智能终端准入机制

PKI 技术是处理身份认证问题的有效解决方案[26-27]，电力资源调度用户在入网之前，将与 PKI 系统进行交互。如图 2 所示，用户首先通过智能终端提交电力资格材料供 PKI 系统审核，审核通过后颁发准入证书。用户携带证书发起入网请求，准入合约将会校验证书合法性，检验通过方可允许用户加入网络。

为保证安全性，准入过程采用基于中国剩余定理优化的 RSA 加密算法加密[28-31]。准入过程设计如下：

1)用户 i 本地生成资格审核信息序列 $Info_i$，其中包含用户 i 的发用电资质、位置、设备等信息。

2)由用户 i 随机生成 1024 位的大素数 p 和 q，并计算：

$$\phi(n)=(p-1)*(q-1) \tag{3}$$

其中，$n=p*q$。

3)选取固定长度且满足 $GCD[e,\phi(n)]=1$ 的长整数 e 为公钥。

4）用户 i 根据 $(e*d) \bmod \phi(n)=1$ 计算出私钥 d。

5）用户 i 用使用私钥 d 加密数据，得到密文 $CInfo_i=(Info_i)^e \bmod (n)$。

6）用户 i 将密文 $CInfo_i$ 发送给准入系统认证服务器。

7）认证服务器收到密文数据之后，根据式(4)设置 m_1，m_2，…，m_k 的值。

$$GCD(m_i,m_j)=1 \tag{4}$$

其中，$i,j=1,2,\cdots,k$，且 $i\neq j$。

8）认证服务器对于整数 a_1，a_2，…，a_k 可得到同余方程组：

$$X\equiv a_1 \bmod m_1, X\equiv a_2 \bmod m_2,\cdots, X\equiv a_k \bmod m_k \tag{5}$$

9）$[m_1,m_2,\cdots,m_k]$ 有唯一解，认证服务器根据中国剩余定理得到解为：

$$X\equiv(a_1M_1y_1+a_2M_2y_2+a_kM_ky_k) \bmod N \tag{6}$$

其中，$N=\prod_{i=1}^{k}n_i$，$M_i=\frac{N}{m_i}$，$y_i=M_i \bmod m_i$。

10）认证服务器收到数据之后，根据计算得到的解进行私钥计算，得到 p 和 q。

$$d*p=d \bmod (p-1) \tag{7}$$

$$d*q=d \bmod (e(q-1)), q_{\text{inv}}=q^{-1} \bmod p \tag{8}$$

11）根据计算得到的 p 和 q，对用户 i 发来的密文序列 $CInfo_i$ 进行如下解密。

$$m_1=c^{(d*p)} \bmod p, m_2=c^{(d*p)} \bmod q \tag{9}$$

$$h=q_{\text{inv}}(m_1-m_2) \bmod p \tag{10}$$

$$Info_i=m_2+(h*q) \bmod (p*q) \tag{11}$$

12）最终认证服务器得到用户发来的认证数据 $Info_i$。

13）认证服务器将认证数据 $Info_i$ 发送给 PKI 系统中的 RA 进行数据可靠性核验。核验通过后，RA 颁发给用户 i 准入证书。

14）用户 i 携带准入证书再次发起入网请求，通过认证服务器核验便可成功加入网络，由此实现了调度用户的安全准入。

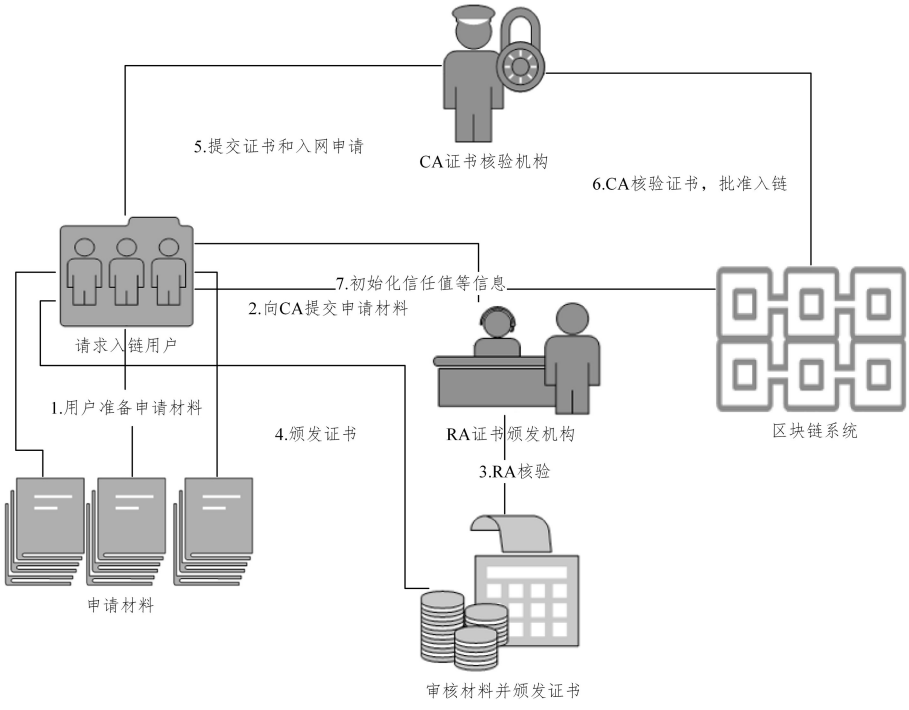

图 2　准入流程

Fig. 2　Admission process

3.2　基于数据可靠性评估的电力数据发布方法

准入成功的用户，便可通过已经准入的智能终端上传本地调度资源信息。系统根据发电规模及安全属性指标，将参与调度用户分为公司户和个体户。用户需首先获取本地调度资源信息并提出上链申请，系统会对上链申请信息进行审核，保证上链数据的可靠性。对上链信息的审核主要采用数据可靠性审核的方法，对用户提交的调度信息包进行各指标的审核。审核指标如下：

1）需求电量和供给电量字段的差值不能超过最大值的 50%；

2）个体户的需求电量和供给电量不能超过电量上限；

3）公司户的需求电量和供给电量不能低于电量下限；

4）信任值不能低于最低信任阈值要求；

5）时间戳不能超过当前时间的未来 2 h；

6）设备 id 字段与系统存储的一致。

具体审核过程由链上智能合约自动完成，无第三方参与。数据可靠性审核的具体设计如式(12)－式(17)所示，数据可靠性审核的结果为评分结果以及是否满足上链安全要求，满足上链需求的予以上链，否则将不准上链。评分结果是数据可靠性审核的量化分值，衡量信息的可靠程度。评分幅度表示违反可靠性指标的评分增减程度。

$$|L_i-P_i| \leqslant \max(L_i,P_i)*0.5 \tag{12}$$

其中，评分幅度为：$|L_i-P_i|/\text{sum}(L_i+P_i)$。

$$L_i \leqslant S_s; P_i \leqslant S_s \tag{13}$$

其中，评分幅度为：$\frac{1}{S_s-L_i}$，$\frac{1}{S_s-P_i}$。

$$D_i \leqslant d \tag{14}$$

其中，评分幅度为：$\frac{D_i-d}{D_i+d}$。

$$T_i-CT \leqslant 2h \tag{15}$$

其中，评分幅度为：$\frac{T_i-CT}{CT}$。

$$LS_i=\begin{cases}\mu, & R_i=T\\ -\mu, & R_i=F\end{cases} \tag{16}$$

$$R_i=\begin{cases}T, & DI_i=LI_i\\ F, & DI_i\neq LI_i\end{cases} \tag{17}$$

其中，$i\in[1,n]$标识用户，L_i表示用户i需求电量，P_i表示用户i当前供给电量，S_s表示供给电量上限；D_i表示用户i信任值，d表示信任阈值；T_i表示用户i发布数据时间戳，CT表示系统当前时间；μ是调度结果影响因子；DI_i表示用户i当前设备id，LI_i表示用户i注册设备id，R_i为用户i行为分析结果；1表示通过，0表示不通过，$I(i)$表示用户全集，$I(j)$表示调度全集。

$$Score_{i,j}=\frac{L_i-P_i}{\mathrm{sum}(L_i+P_i)}*(\max(L_i,P_i)*0.05-|L_i-P_i|)+\tau*PD \tag{18}$$

其中，$i\in I(i)$，$j\in I(j)$。

$$PD=\frac{2S_s-(L_i+P_i)}{(S_s-L_i)*(S_s-P_i)}+\frac{D_i-d}{D_i+d}+\frac{T_i-CT}{CT} \tag{19}$$

其中，$Score_{i,j}$表示用户i的第j次调度行为评分，τ是约束权重因子。

针对发布数据的可靠性审核评分之后，会得到审核结果R_i和可靠性评分值$Score_{i,j}$。系统依据R_i确定数据是否准许上链。可靠性评分值将参与调度结束之后用户信任的更新计算。

对于链上的可靠电力数据，系统需要根据当前的风险状态采用合理的调度方案。

3.3 基于效益理论的多策略调度模型

系统将当前状态衡量为不同的风险等级θ，并根据不同的风险等级选用不同的调度策略，当风险状态表现为风险追求时，选用开放型调度策略，当风险状态表现为风险避免时，选用保守型调度策略。

风险等级θ的衡量视系统的供需情况而定，与公司户TP_{com}的总供电量与全网电力需求量Ad有关，即：

$$\theta=\begin{cases}1+\dfrac{Ad-TP_{\mathrm{com}}}{Ad}, & TP_{\mathrm{com}}<Ad\\ 1, & TP_{\mathrm{com}}=Ad\\ \dfrac{TP_{\mathrm{com}}-Ad}{Ad}, & TP_{\mathrm{com}}>Ad\end{cases} \tag{20}$$

当$TP_{\mathrm{com}}>Ad$时，系统风险状态为风险追求；当$TP_{\mathrm{com}}=Ad$时，系统风险状态为风险中立；当$TP_{\mathrm{com}}<Ad$时，系统风险状态为风险避免。

根据系统当前的风险等级，采用效益理论模型进行分析，衡量用户参与调度的潜在风险及收益。衡量方法如下所示：

$$EU_i=Td_i*U_i-(1-Td_i)*U_i \tag{21}$$

$$B_i=\beta*P_i \tag{22}$$

$$C_i=P_i*(1-Score_{i,j}) \tag{23}$$

其中，Td_i表示用户i的当前信任值；P_i表示用户i的当前电量；EU_i为用户i的效益值，该效益值与用户i的潜在风险、收益和信任度有关。β为收益与电量的相关系数。

由式(21)－式(23)，可得：

$$\begin{aligned}E_i&=B_i-C_i\\&=P_i-P_i*(1-Score_{i,j})\\&=P_i*Score_{i,j}\end{aligned} \tag{24}$$

$$EU_i=Td_i*\theta*(P_i*Score_{i,j})^{\frac{1}{\theta}}-(1-Td_i)*\theta*(P_i*Score_{i,j})^{\frac{1}{\theta}} \tag{25}$$

其中，E_i表示收益期望。用户i的效益值和系统风险状态、用户i的信任值、供给电量及行为评分有关。调度系统根据用户效益值EU_i进行排序，按照系统需求择优调度。系统根据决策结果签署智能合约，在调度周期内由链上智能合约自动执行调度。

3.4 基于动静态评价结合的信任更新计算方法

当调度结束后，调度系统会根据调度执行结果，更新参与用户的信任值。用户i的当前信任值Td_i的更新主要根据用户i的静态评价和动态评价得到，即：

$$Td_i=\beta_1*Se_i+\beta_2*De_i \tag{26}$$

其中，Se_i表示静态评价，是通过用户i的历史调度行为和调度参与度来对计算。De_i表示动态评价，是通过系统对用户i的调度行为进行评价。β_1和β_2分别表示相应评价的权重系数。

用户i的静态评价Se_i是根据用户i在调度过程中的行为来进行计算的，可以表示为：

$$Se_i=\gamma_1*Hbf_i+\gamma_2*Hpf_i \tag{27}$$

其中，Hbf_i是用户i在调度过程中的历史行为因子，Hpf_i是用户i在调度过程中的历史参与度因子，γ_1和γ_2是相应权重。历史行为因子Hbf_i表示用户i的历史调度行为对信任值的影响程度，可以表示为：

$$Hbf_i=\frac{\varphi_1*Ht_i+\varphi_2*Mt_i}{Tn_i} \tag{28}$$

$$\varphi_1+\varphi_2=1 \tag{29}$$

$$Tn_i=Ht_i+Mt_i \tag{30}$$

其中，Ht_i表示用户i的调度行为诚信次数。Mt_i表示用户i的调度行为恶意的次数。φ_1和φ_2是对应权重，Tn_i表示用户i参与调度次数。诚信次数越多，信任值增加幅度越大。

用户i的调度参与程度Tp_i可以描述为：

$$Tp_i=\frac{Tn_i}{TT} \tag{31}$$

其中，TT表示为周期内所有用户的调度总次数，Tn_i表示用户i参与调度的次数。用户i的动态评价描述为系统评价，可以表示为：

$$De_i=\begin{cases}\dfrac{\sum_{j}^{n}\dfrac{\sum_{m=1}^{l}f(m)*De_{ij}^{m}}{Tn_i}}{n}, & Tn_i\neq 0\\ 0, & Tn_i=0\end{cases} \tag{32}$$

其中，j表示当前周期，n表示微电网系统调度周期总数，l表示调度总次数，m表示第m次调度，De_{ij}^{m}表示第m次调度完成后系统对用户i的调度行为评价，$f(m)$为时间衰减函数，表示为：

$$f(m)=\mu^{1-m}(0<\mu<1,1\leqslant m\leqslant Tn_i) \tag{33}$$

其中，$f(m)$表示调度次数与调度时间的距离，距离调度时间越远，时间衰减越严重，动态评价占比越小。基于设计的信任更新算法，根据用户历史调度行为进行信任更新，用户的恶意调度行为将会影响后序的调度，保障了微电网调度环境的可靠。

调度结束之后，通过对用户信任值的更新，将用户行为量化为信任，实现了对调度用户的约束作用，为系统整体的可靠调度保驾护航。

4 实验分析

4.1 实验环境

仿真环境为：Inter © Corei7_10700CPU @2.97 GHz＋Win10＋Remix＋solidity0.7.0-0.9.0＋Meta Mask。

4.1.1 实验的相关假设

1）假设个体用户的规模上限为 100 kWh；公司用户的规模下限为 100 kWh，上限为 200 kWh；

2）假设允许信息上链的信任阈值为 0.5，信任值最高为 1，默认初始化信任值为 0.25；

3）假设调度影响因子为 0.03，调度成功与否对下次调度的信任值影响为±0.03；

4）假设收益与电量的相关系数为 1，信任权重因子为 0.6；

5）假设用户能轻易通过智能设备获取到本地的负荷电力信息；

6）为验证方案有效性，假设信任值以明文的形式存储；

7）假设参与资源调度的用户已经完成准入环节。

4.1.2 算法设计

本方案中的相关算法设计流程如图 3 所示。

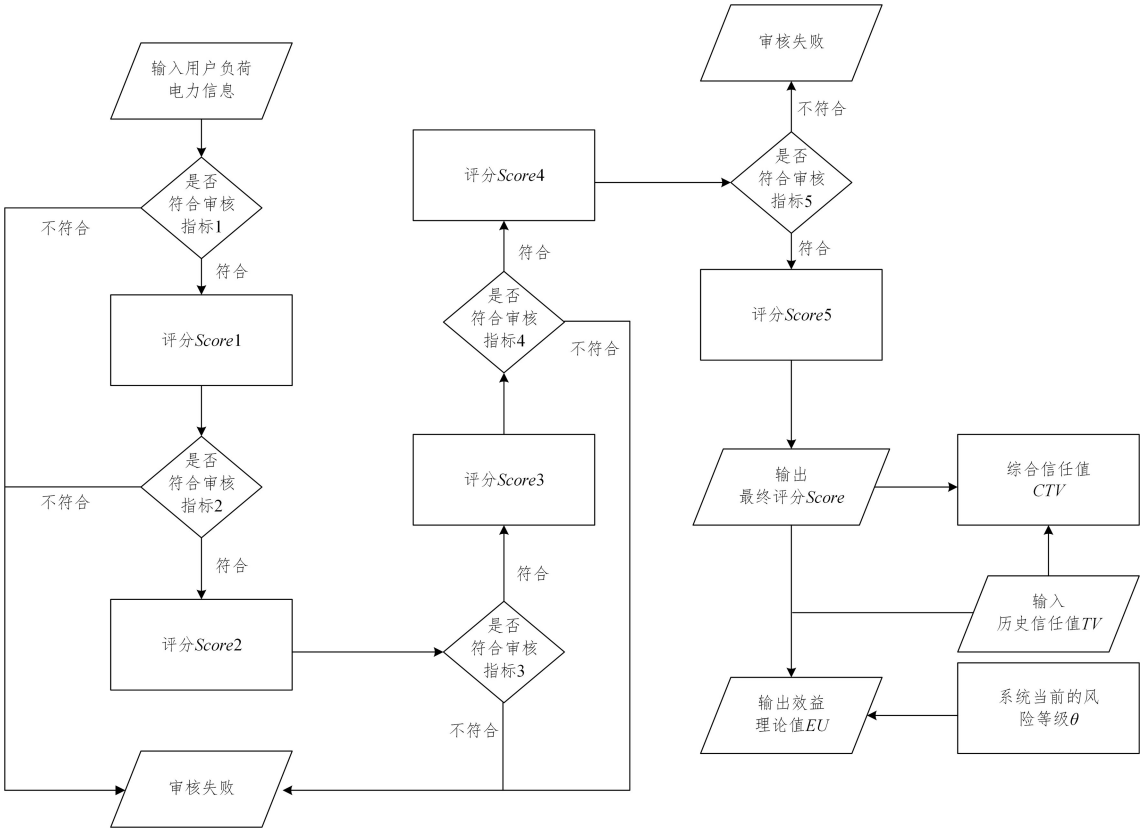

图 3 效益值计算流程

Fig. 3 Utility value calculation process

4.2 实验结果分析

通过实验仿真，数据可靠性评估合约能够对资源调度用户的上链行为进行分析。图 4 中展示了调度用户的需求电量、供给电量、及评分值三者之间的关系。

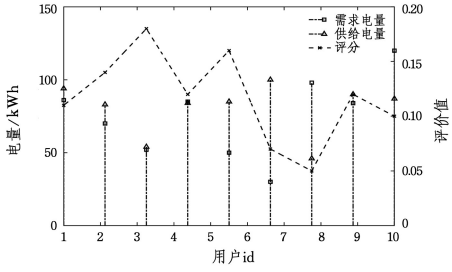

图 4 调度用户需求电量、供给电量及评分关系图

Fig. 4 Relationship diagram of scheduling user demand for electricity, supply quantity and score

实验测试 9 组调度用户数据，从图中容易看出，第 6，7 组数据的供给电量与需求电量的差值较大，超出评分幅度范围，对应的评分值在这两个数据点位大幅下降，审核结果为 false，阻止上链。第 9 组用户数据超出上限 100 kWh，审核结果为 false，阻止上链，但评分依然存在，该评分隐含了超出上限的幅度。详细的数据可靠性评估结果如表 1 所列。

表 1 用户电力信息评分结果

Table 1 User electricity information scoring results

用户 id	需求电量	供给电量	审核结果	评分
1	86	94	true	0.11
2	70	83	true	0.14
3	52	54	true	0.18
4	85	84	true	0.12
5	50	85	true	0.16
6	30	100	false	0.07
7	98	46	false	0.05
8	84	90	true	0.12
9	120	87	false	0.10

由此可见，数据可靠性评估能够识别出存在异常数据的调度用户，并采取阻止信息上链的决策，将风险规避在了链下。

对于成功上链的用户数据，调度系统才能进行调度决策。

调度决策的选择依据调度系统对各用户进行效益理论的计算结果。

为测试实际调度场景的有效性，实验选取 19 条公司户数据和 10 条个体户数据。其中，公司户数据分布如图 5 所示。通过风险等级计算，系统总需求电量小于公司户电量，表现为供不应求的情况，此时系统的风险状态表现为风险追求。

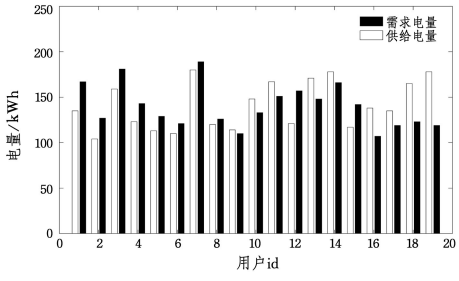

图 5 公司户电力数据

Fig. 5 Company power data

在风险追求状态下，此时系统采用让安全级别低的个体户参与调度的策略。实验选取的个体用户调度数据如表 2 所列，从表中可以看出，1 号和 2 号用户的数据可靠性审核结果为 false，数据不予上链，不参与本次调度，效益值为 0。为满足本次电力调度的缺额 18 kWh，如图 6 所列，实验最终抉择调度 id 为 6，7，8，10 的用户，淘汰掉 id 为 1，2，9 的用户，因 9 号用户没有足够多余的电量参与电力调度。

表 2 个体户电力调度数据信息

Table 2 Self-employed power dispatching data

用户 id	需求电量、供给电量	审核结果	效益值
1	39，43	false	0
2	94，100	false	0
3	79，80	true	0.15
4	27，29	true	0.21
5	25，49	true	0.27
6	88，92	true	0.31
7	65，72	true	0.34
8	54，60	true	0.69
9	90，90	true	1.90
10	71，73	true	2.05

5 号用户虽然能够满足调度缺额，但并未被调度，原因是系统经过风险评估，优先选择效益值高、风险低的用户进行调度。实验仿真结果验证了调度方案的有效性。

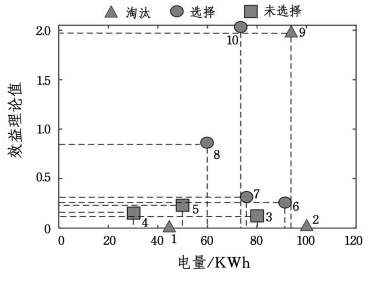

图 6 调度选择结果

Fig. 6 Scheduling selection results

表 3 列出了个体户在风险追求状态下的效益值。容易看出，当前调度用户的信任值越大，被调度选择的可能性就越大，当用户信任值相同的时候，供给电量越多被调度的可能性越大，原因是此时选择高供给电量的用户可以减少系统总调度次数，降低系统的调度成本。

表 3 个体户在风险追求状态下的效益值

Table 3 Benefit value of self-employed in risk-seeking state

用户 id	信任值	供给电量	效益值
1	27	20	0.02
2	34	13	0.08
3	30	67	0.22
4	40	31	0.38
5	33	72	0.40
6	32	94	0.45
7	41	35	0.47
8	45	32	0.59
9	38	74	0.75
10	42	65	0.95

调度周期结束之后，用户调度结果可分为 3 种：1）调度成功；2）调度失败；3）未被调度。如图 7 所示，当调度失败的时候，信任值会相应下降，信任值越高的用户下降越明显，目的是鼓励信任值低的用户。当调度成功的时候，信任值会有所提高，且提高的幅度与历史信任值的高低无关，即无论历史信任处于什么水平，良好的调度行为都能带来良好的信任更新。对于未被调度的用户，信任值也会随着数据可靠性评估的良好评分有所提高。

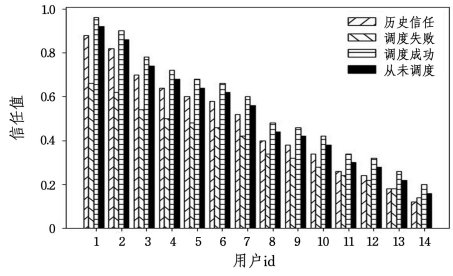

图 7 不同调度结果对用户信任值更新的影响

Fig. 7 Impact of different scheduling results on user trust value update

对用户调度 100 次，用户在调度中不同的行为会有不同的调度结果，也会改变用户的信任值。收集用户 100 次调度的信任值变化，如图 8 所示。容易看出，在调度过程中表现良好的用户，随着调度次数的增加，以 20 次调度为一组统计信任值平均值为 0.44，0.68，0.89，1，1，其信任值呈现上升趋势，并且增长过程平稳。相反，表现出恶意行为的用户在调度过程中会遭受信任值的下降。

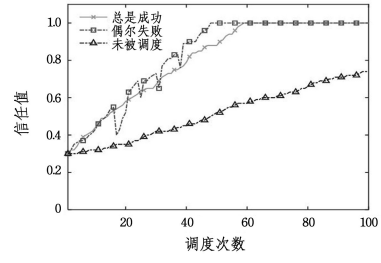

图 8 用户累次信任值变化轨迹对比

Fig. 8 Comparison of the change trajectory of user trust value

从图中可以看出，用户在第 20，30，38，43 次调度过程中出现了恶意行为，用户的信任值出现了波动，分组平均信任值为 0.39，0.61，0.87，1，1，相较表现良好的用户信任值的平均值较低。前 50 次调度下表现良好的用户的信任值的 SD 值为 0.025，有恶意行为用户的 SD 值为 0.031，这是由于恶意行为导致评分的不稳定波动，但随着用户的后续表现良好，信任

值又会稳步增长，恢复到良好水平，总体趋势呈现一个波动式上涨。未被调度的用户的信任值增长最慢，且在整个评价过程中信任值逐渐增加，但没有达到稳态，等待被系统调度。

图 9 对比了本文所提可靠电力数据调度方案和消息认证方案随着恶意节点数量的增加，系统中恶意节点参与度的变化情况。随着系统中恶意节点的逐渐增多，成功参与调度的恶意节点数量也会逐渐增加。在恶意节点数量低于 50%时，两种方案下恶意节点的参与度维持在较低水平，二者相差不大。当恶意节点数量高于 50%后，二者的结果均出现较大的波动，但本方案始终低于消息认证方案，可见本文所提出的将信任值引入调度中并根据用户行为动态调整的可靠电力数据调度方案，相较于消息认证方案，能够降低恶意节点的参与度。信任值更新除了与调度结果有关，针对数据可靠性评估的结果也会对信任值产生一定的影响。图 10 测试了 3 种不同的调度结果下，信任值变化与当前行为的相关关系。从图中可以看出，当调度执行失败的时候，会显著降低信任值，为鼓励用户后续行为良好，若后续行为评分较高，会设置更高的增长幅度，信任值会快速增长。当调度执行成功的时候，可以明显看到综合信任较历史信任增长许多，且随当前行为评分的升高，综合信任值较历史信任增加的幅度也升高。但信任有上限，当信任达到上限 1 之后，便保持不变。当用户未被选择调度的时候，用户的信任值会随当前数据可靠性评估值的增加而增加，但变化幅度更小，表明良好的调度结果对用户起到正向激励作用。

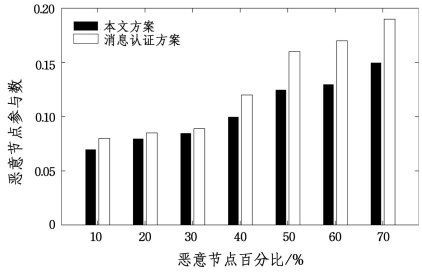

图 9　不同方案恶意节点参与率对比

Fig. 9　Comparison of the participation rate of malicious nodes in different schemes

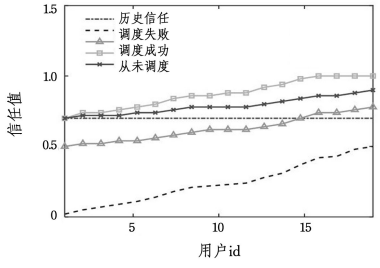

图 10　数据可靠性评分对用户信任值更新的影响

Fig. 10　Influence of data reliability score on user trust value update

图 11 对比了采用本文所提可靠电力数据调度方案和无视风险的调度方案。从图中可以看出，随着恶意行为次数(不诚信调度行为)的增多，两种方法下的调度成功率都是会呈现下降趋势，说明随着恶意行为的增多，系统的整体不稳定性在增高。可以明显地看出，采用本文所提可靠电力数据调度方案下降更平稳，能够将调度成功率维持在一个较高的水平，证明了本文所设计可靠电力数据调度方案的有效性。图 12 对比了本文所提可靠电力数据调度方案和原始调度方案随着恶意行为的增加，系统总收益的变化。恶意行为百分比小于 40%时，系统内的风险较小，此时单考虑信任方案的收益始终高于单考虑风险；随着恶意行为的增多，系统内的不稳定因素增加，风险升高，这时单考虑恶意节点的方案的收益高于单考虑信任方案。而本方案兼顾信任与风险方案，在不同的恶意行为情况下的收益均高于二者，本章所提可靠电力数据调度方案要优于无视风险的调度方案，能够在恶意行为用户增多的时候保持一个更为稳定的收益。

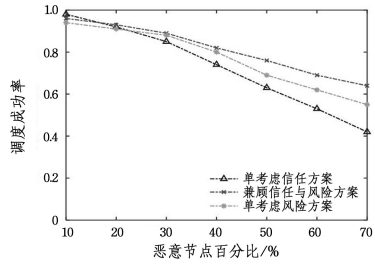

图 11　不同方案交易成功率对比

Fig. 11　Comparison of transaction success rates of different schemes

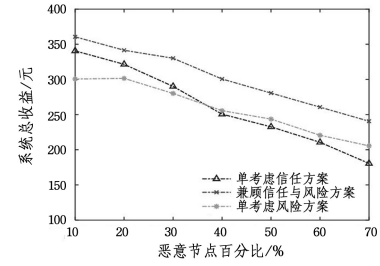

图 12　不同方案系统总收益对比

Fig. 12　Comparison of total system revenue of different schemes

综上所述，实验通过测试针对电力调度数据设计的数据可靠性评估方法的有效性，证明其能够配合区块链系统将调度风险规避在链下。测试了在实际电力调度场景下，基于效益理论的多策略调度模型的有效性，系统会自动根据当前供需确定风险状态，根据不同的状态信息进行调度决策的调整，通过不同数量的恶意节点和恶意行为设置不同对比实验。测试了设计适用于电力调度场景下的基于动静评价结合的信任值更新方法的有效性，通过信任值的跟踪记录有效地约束了参与调度的用户的行为。另外，基于系统调度成功率及总收益指标，测试证明了随着测试规模的不断增加，本方案能够兼顾效益和可靠性。

结束语　本文针对电力数据调度场景存在的信息共享难、安全性低、难以兼顾安全和效益的问题，提出了基于区块链、信任评估、效益理论等技术的可靠电力数据调度方案，通过设计基于 RSA 与 PKI 技术的准入机制、基于数据可靠性评估的数据发布方法、基于效益理论的多策略调度模型与基于动静态评价相结合的信任更新计算方法，解决了电力数据调度场景下可靠性及效益难兼容的问题，并通过仿真验证了方案的有效性，为电力数据调度提供了有效保障。但仍然存在一些能够进一步改进的方面：从安全角度出发，没有考虑网络攻击对系统的影响，潜在的网络攻击可能会引起数据可靠性方面的问题，这会严重影响到系统的调度；从系统角度出发，没有考虑在大电网环境下的系统故障问题，包括软件和硬件问题，这也会降低电网运行的稳定性和可靠性；从效益角度出发，影响调度效益的因素有很多，比如考虑电力市场政策和

法规，优化电网结构可以降低传输损耗，提高能源传输效率，从而增强电网的经济效益。下一步的研究是如何综合考虑其他相关因素进一步提高电网运行的安全性、高效性和经济性。

参 考 文 献

[1] ZHANG Y, WANG A H, ZHANG H. Overview of smart grid development in China[J]. Power System Protection and Control, 2021, 49(5): 180-187.

[2] CHEN J, LI X D, LU B. Point To Point Power Market Mode and Behavior Evolution from the Perspective of Cooperative Alliance[J]. Power System Technology, 2023, 47(8): 3227-3238.

[3] ZHANG Y, WANG L Z, WU J, et al. Blockchain and Integrated Energy System: Appl- ication and Prospect[J]. Fundamental Research Science Foundation in China, 2020, 34(1): 31-37.

[4] WANG H R, FU J, LIU J R. Encryption and sharing of power grid comprehensive operation and maintenance information under multi-level access security[J], Information Technology, 2023(8): 88-93.

[5] LIANG Y L, LING J. Encrypted Data Sharing Scheme in Cloud Storage Based on Blockchain[J]. Computer Engineering and Applications, 2020, 56(17): 41-47.

[6] GAO Z X, FAN Z Y. The application research of electrical engineering technology in the construction of smart grids[J]. China Plant Engineering, 2023(18): 26-28.

[7] ZHAOW, QI Q, ZHOU J, et al. Blockchain-Based Applications for Smart Grids: An Umbrella Review [J]. Energies, 2023, 16(17).

[8] YU X B, ZHENG D D. Application and exploration of blockchain technology in energy and electricity[J]. Huadian Technology, 2020, 42(8): 17-23.

[9] WEN Y D. Analysis on Distributed Energy Trading Mechanism in West Inner MongoliaPower Market Under Background of New Power System[J]. Inner Mongolia Electric Power, 2023, 41(3): 78-85.

[10] LIU C, WANG S J, ZHAO Y L, et al. Review of the Application of Blockchain Technology in Virtual Power Plant Transactions [J]. Electric Power Construction, 2023, 44(4): 130-144.

[11] ZHANGG Y, SUN R H, MA C G, et al. Survey of Sensor Networks Management and Authentication[J]. Computer Science, 2010, 37(2): 1-6, 11.

[12] LUO X, XUE K, XU J, et al. Blockchain Based Secure Data Aggregation and Distributed Power Dispatching for Microgrids[J]. IEEE Transactions on Smart Grid, 2021, PP(99): 1-1.

[13] XU Y, LIU Z, ZHANG C, et al. Blockchain-based trustworthy energy dispatching approach for high renewable energy penetrated power systems[J]. IEEE Internet of Things Journal, 2022, 9(12): 10036-10047.

[14] LI X, WU F, KUMARI S, et al. A Provably Secure and Anonymous Message Authentication Scheme for Smart Grids[J]. Journal of Parallel and Distributed Computing, 2019, 132(OCT.): 242-249.

[15] LI X. A Provably Secure and Anonymous Message Authentication Scheme for Smart Grids[J]. Journal of Parallel and Distributed Computing, 2019, 132(OCT.): 242-249.

[16] FIRDAUS A, AB RAZAK M F, FEIZOLLAH A, et al. The rise of "blockchain": bibliometric analysis of blockchain study[J]. Scientometrics, 2019, 120(3): 1289-1331.

[17] LIU C, WANG S J, ZHAO Y L, et al. Review of the Application of Blockchain Technology in Virtual Power Plant Transactions [J]. Electric Power Construction, 2023, 44(4): 130-144.

[18] ZHAO T J, KAN T, HE B, et al. Smart Grid Security Analysis under Blockchain[J]. Electronic Components and Information Technology, 2023, 7(2): 6-9.

[19] SHUAI W, YONG Y, WANG X, et al. An Overview of Smart Contract: Architecture, Applications, and Future Trends[C]// 2018 IEEE Intelligent Vehicles Symposium(IV). IEEE, 2018.

[20] ZHOU J, YE L P, NI Y Y, et al. Review of Intelligent Contract [J]. China New Telecommunications, 2021, 23(3): 37-39.

[21] NEUMANN J V. Theory of games and economic behavior[M]. Princeton University Press, 1944.

[22] JIANG M J, WANG W T. Risk quantification and security benefit assessment of clean energygrid connected to power system considering energy storage power stations [J]. Power Demand Side Management, 2021, 23(2): 52-57.

[23] WU X. Trust management technology in cloud computing environments[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2015: 202.

[24] GARBIS J, CHAPMAN J W. Zero Trust Security: An Enterprise Guide [M]. Berkeley, USA: Apress, 2021.

[25] DU Z H. Research and Application of a Borderless Zero Trust Network under the "Internet Plus" Background[J]. Modern Information Technology, 2021, 5(6): 153-157.

[26] KOU W Z, HE S Y. PKI technology-based network security platform design [J]. Information Recording Materials, 2022, 23(9): 102-105.

[27] HAMMI B, MONTEUUIS J, PETIT J. PKIs in C-ITS: Security functions, architectures and projects: A survey [J]. Vehicular Communications, 2022, 38.

[28] WEN X B, ZHENG Y. Algorithm Simulation Applied to Cloud SecurityCredibility Detection of Internet of Things[J]. Computer Simulation, 2022, 39(5): 225-228.

[29] VERGNAUD D. Comment on efficient and secure outsourcing scheme for RSA decryption in internet of things[J]. IEEE Internet of Things Journal, 2020, 7(11): 11327-11329.

[30] DESAIS S, NENE M J. Multihop trust evaluation using memory integrity in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4092-4100

[31] DESAIS S, NENE M J. Node-level trust evaluation in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(8): 2139-2152.

MA Junwei, born in 1982, Ph.D, senior engineer. His main research interests include power system digitalization and blockchain.