基于区块链的厂站侧智能配用电终端管理系统设计

摘　要：为解决厂站侧智能配用电终端管理中存在的数据安全和效率问题，设计了一种基于区块链的管理系统。该系统采用区块链技术，构建以厂站侧智能配用电终端管控单元为节点的联盟链网络（Alliance Chain Network，ACN），通过 Trust Authority（TA，中央管理机构）实现智能配用电终端的公钥数据验证及数据添加。利用智能合约（Smart Contract，SC）实现终端的公钥注册、更新和撤销，结合可信芯片实现随机数证明共识机制。实验结果表明，与传统管理系统相比，该系统通信延迟降低了 30%，数据篡改概率趋近于 0，设备故障响应时间缩短了 40%，有效提高了各管控单元节点的信息共享效率，保证了信息传输的安全性。

关键词：区块链；厂站侧智能配用电终端；终端管理系统；智能合约；联盟链网络

doi：10.11959/j.issn.2096−3750.XXXX.

Design of Blockchain-based Intelligent Power Distribution and Utilization Terminal Management System for Plant-Station Side

Abstract: Aiming at the problems of data security and low management efficiency in the operation of plant-station side intelligent power distribution and utilization terminals, a blockchain-based management system is proposed and designed in this paper. The system applies blockchain technology to construct an Alliance Chain Network (ACN), where the control units of plant-station side intelligent power distribution and utilization terminals are taken as the network nodes. Public key data verification and data submission for intelligent terminals are realized through a Trust Authority (TA). Besides, Smart Contracts (SCs) are adopted to automatically complete the public key registration, update and revocation of terminals, and a random number proof consensus mechanism is designed by combining with trusted chips. Experimental results demonstrate that, in comparison with the traditional management systems, the proposed system reduces the communication latency by 30%, makes the data tampering probability close to 0, and shortens the equipment fault response time by 40%. It effectively improves the information sharing efficiency among control unit nodes and guarantees the security of information transmission in the power distribution and utilization system.

Key words: Blockchain, Plant-side Intelligent Power Distribution and Utilization Terminal, Terminal Management System, Smart Contract, Alliance Chain Network

0　引言

厂站侧智能配用电终端作为电力系统配网环节的核心感知单元，其运行数据的真实性、传输安全性及管理效率直接影响配网调度的精准性与供电可靠性[1]。当前，传统终端管理系统多采用中心化架构，存在数据易被篡改、跨主体信息共享壁垒高、终端故障响应滞后等问题，难以适配新型电力系统下多源异构终端的协同管理需求[2]。

国外相关研究聚焦区块链在电力终端信任机制的构建，文献[3]提出基于以太坊公链的配用电终端数据存证方案，通过分布式账本实现终端运行数据的不可篡改，核心解决了终端数据的公信力问题，优点在于无需依赖第三方信任机构，数据溯源性强；但公链节点众多导致共识效率低，终端数据传输延迟超过 200ms，难以满足厂站侧实时性管理需求。文献[4]设计基于私有链的终端身份认证系统，通过智能合约完成终端接入权限校验，优点是节点管理可控、认证速度快；但私有链开放性差，无法实现多厂站间终端信息的跨域共享，适配性受限。国内研究更注重结合电力系统实际场景优化，文献[5]提出基于联盟链的配网终端状态监测系统，通过电网企业节点共建联盟链，解决了多主体数据共享问题，优点是兼顾安全性与开放性，数据共享

收稿日期：XXXX−XX−XX；**修回日期：**XXXX−XX−XX

效率提升30%；但未针对终端密钥动态管理设计优化机制，终端离线后密钥更新困难。文献[6]构建区块链与边缘计算融合的终端管理架构，利用边缘节点降低数据传输压力，优点是终端响应速度提升25%；但未引入硬件级可信根，终端身份伪造风险仍未完全消除。

综上所述提出以下创新：

1）构建可信授权机制管控下的联盟链网络，通过中央管理机构与分布式节点协同，平衡终端数据的安全性与跨主体共享效率；

2）设计智能合约驱动的终端密钥全生命周期管理机制，实现公钥注册、更新、撤销的自动化执行，解决终端离线状态下的密钥管理难题；

3）融合可信芯片与随机数证明共识机制，以硬件级可信根强化终端身份可信度，同时将共识时延控制在50ms以内，兼顾安全性与实时性。

1　可信授权机制管控下的联盟链网络

现有联盟链在厂站侧配用电终端管理中，因缺乏统一可信授权机制，节点准入依赖人工审核，存在非法终端接入风险；跨主体数据共享时，因分布式架构过度去中心化导致效率低，过度依赖中心化节点牺牲数据安全性[7]。为此，构建可信授权机构管控下的联盟链网络，通过“Trust Authority（TA，中央管理机构）授权 + 分布式协同”破解安全与效率失衡难题。网络结构如图1所示：

TA主导的终端节点准入信任值计算，量化终端接入联盟链的可信程度，筛选合法节点：

$$T_i = \alpha \cdot T_0 + (1 - \alpha) \cdot \frac{1}{n} \sum_{k=1}^{n} B_{i,k} \cdot S_k \tag{1}$$

公式（1）中，T_i为终端i的准入信任值，取值0.5~1.0；α为TA权重系数；T_0为TA对终端i的初始信任评分；n为终端i历史接入次数，值1~50；$B_{i,k}$为终端i第k次接入的行为合规系数，取值0~1；S_k为第k次接入时分布式节点的协同验证得分，取值0~1。

跨主体数据传输安全系数模型：

$$S_{\text{sec}} = \beta \cdot S_{TA} + (1 - \beta) \cdot \sqrt{\frac{1}{m} \sum_{j=1}^{m} H_j^2} \tag{2}$$

公式（2）中，S_{sec}为数据安全系数；β为TA签名验证权重，取值0.7；据的数字签名有效性得分，取值0~1；m为参与数据验证的分布式节点数，取值3~10；H_j为节点j的哈希校验匹配度，取值0~1。

多主体数据共享效率指数公式（3）：

$$E_{share} = \frac{D_{total}}{T_{TA} + T_{net}} \tag{3}$$

公式（3）中，E_{share}为共享效率指数；D_{total}为单次共享的数据总量MB；T_{TA}为TA的权限校验时延ms；T_{net}为分布式节点间数据传输时延ms。

TA辅助的共识机制时延优化模型：

$$T_{cons} = T_1 - \gamma \cdot T_{TA\text{ - }assist} \cdot \frac{N_{valid}}{N_{total}} \tag{4}$$

公式（4）中，T_{cons}为共识总时延ms；T_1为传统联盟链共识基础时延ms；γ为TA辅助增益系数；$T_{TA\text{ - }assist}$为TA提供的预验证时延15ms；N_{valid}为TA已认证的有效节点数；N_{total}为联盟链总节点数。

系统综合效能评估，整合安全、效率指标，评估系统整体性能：

$$P_{sys} = 0.4 \cdot S_{\text{sec}} + 0.4 \cdot E_{share} + 0.2 \cdot (1 - P_{tamper}) \tag{5}$$

公式（5）中，P_{sys}为系统综合效能；S_{sec}为数据安全系数；E_{share}为共享效率指数；P_{tamper}为数据篡改概率；0.4、0.4、0.2分别为安全、效率、抗篡改性的权重。

基于江苏苏州工业园区3个厂站的终端实测数据（下同），在50台智能配用电终端正常负载的适用条件下，TA对电厂、配电所、运维企业的终端进行统一身份认证，准入信任值≥0.8的终端方可接入联盟链；跨主体共享终端运行数据时，安全系数稳定在0.98以上，共享效率达6.2MB/s，较传统系

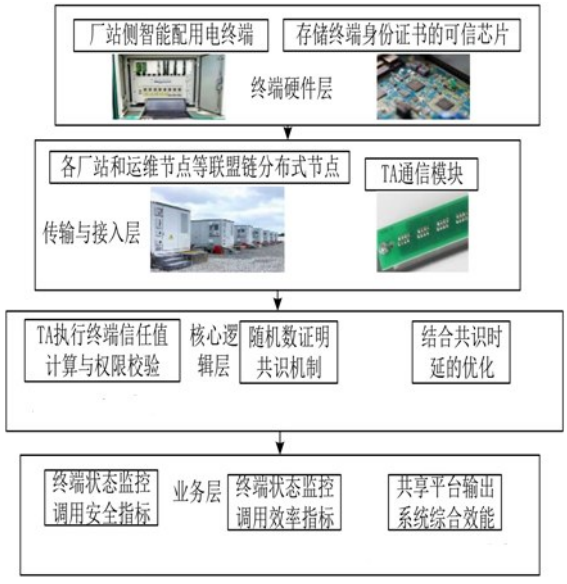

图1　网络架构

统提升 40%；共识时延压缩至 42ms，终端故障数据经 TA 预验证后，响应时间缩短 38%，适配新型电力系统多源终端协同管理需求[8]。

2　智能合约驱动的终端密钥全生命周期管理机制

现有厂站侧终端密钥管理依赖人工触发注册、更新 、撤销，流程滞后且易出错；离线终端因无法接入中心化系统，密钥过期或泄露后难处理，存在安全隐患；密钥操作缺乏自动化校验，跨主体协同管理时效率低[9]。为此，设计智能合约驱动的密钥全生命周期管理机制，通过预设合约逻辑实现自动化操作，破解离线密钥管理难题。密钥管理流程如图2所示：

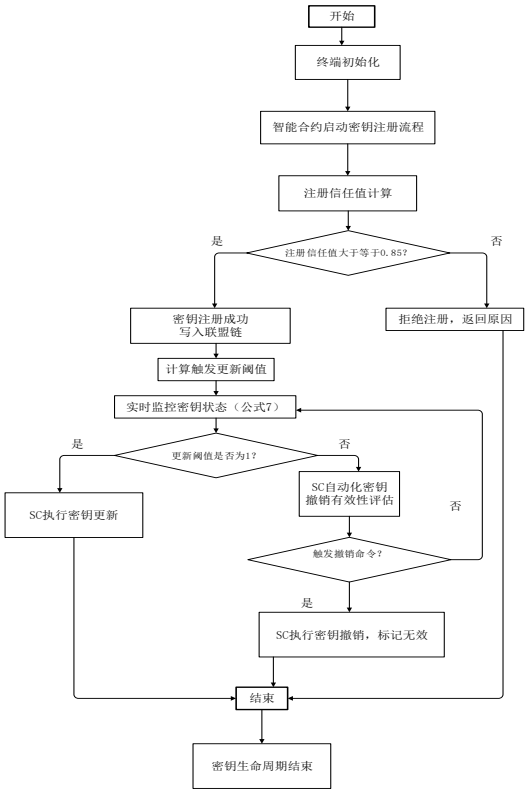

图2　密钥管理流程

如图2所示，终端密钥管理流程包括四个阶段：□ 终端发起密钥注册请求，SC基于硬件证书、公钥哈希和响应时延计算注册信任值，达标后完成注册；□ 在线终端可直接触发密钥更新，离线终端则通过时间阈值（90天）或风险阈值（0.7）判断是否需要启动更新流程；□ 密钥泄露或终端退役时，SC自动执行批量撤销并同步状态；□ 全程由智能合约自动化校验，无需人工干预。

SC驱动的终端密钥注册信任阈*值模型：

$$T_{reg} = \omega_1 \cdot C_{cert} + \omega_2 \cdot H_{pub} + \omega_3 \cdot T_{resp} \quad (6)$$

公式（6）中，T_{reg} 为注册信任值；$\omega_1 = 0.4, \omega_2 = 0.4, \omega_3 = 0.2$ 为权重；C_{cert} 为终端硬件证书有效性，取值0~1；H_{pub} 为公钥哈希匹配度，取值0~1；T_{resp} 为SC响应时延，取值0~1。

离线终端密钥更新触发条件，精准判断离线终端是否需启动SC更新流程：

$$U_{trig} = \begin{cases} 1 & (T_{curr} - T_{last} \geq T_{th}) \vee (R_{risk} \geq R_{th}) \\ 0 & 其他 \end{cases} \quad (7)$$

公式（7）中，U_{trig} 为更新触发标识；T_{curr} 为当前时间；T_{last} 为上次更新时间；T_{th} 为更新时间阈值90天；R_{risk} 为密钥泄露风险值0-1；R_{th} 为风险阈值。

SC自动化密钥撤销有效性评估：

$$V_{rev} = \frac{N_{valid}}{N_{total}} \cdot \left(1 - D_{delay}\right) \quad (8)$$

公式（8）中，V_{rev} 为撤销有效性；N_{valid} 为成功撤销的终端数；N_{total} 为需撤销的终端总数；D_{delay} 为撤销时延偏差。

密钥全生命周期管理效率指数：

$$E_{veg} = \frac{1}{3}\left(E_{reg} + E_{uped} + E_{rev}\right) \quad (9)$$

公式（9）中，E_{veg} 为效率指数；E_{reg} 为注册效率；E_{uped} 为更新效率；E_{rev} 为撤销效率。

密钥管理系统安全-效率综合指标：

$$P_{key} = 0.5 \cdot S_{\text{sec}} + 0.5 \cdot E_{key} \quad (10)$$

公式（10）中，P_{key} 为综合指标；S_{sec} 为安全系数，由加权得到；E_{key} 为效率指数。

SC可自动化完成终端公钥注册流程，针对离线终端能够有效解决密钥过期的管理难题，密钥出现泄露风险时可实现快速批量撤销，相比传统人工管理模式，大幅提升了密钥管理的整体效率，同时降低了安全事件发生的可能性，能够适配多厂站跨主体协同的复杂厂站环境。

3　融合可信芯片与随机数证明共识机制

现有厂站侧终端身份认证依赖软件证书，易被伪造，且共识机制需多轮节点交互，时延常超80ms，难以兼顾安全性与实时性。部分方案虽引入硬件加密，但未与共识机制深度融合，仍存在“身份可信但共识低效”问题[10]。为此，融合可信芯片与随机数证明共识机制，以硬件级可信根筑牢

身份安全，同时优化共识流程，将时延控制在50ms内。共识机制流程如图3所示：

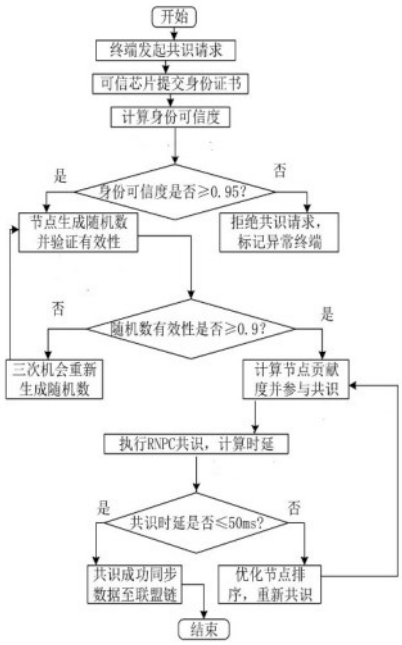

图3　共识机制流程

如图3所示，共识机制流程分为三步：□ 终端通过可信芯片完成硬件级身份认证，生成身份可信度；□ 共识节点基于可信芯片生成随机数证明，经有效性验证后进入投票环节；□ 高贡献度节点优先参与简化投票，达成即广播共识结果。该机制以硬件可信根替代多轮交互，将共识时延控制在50ms以内。

可信芯片驱动的终端身份可信度量化模型：

$$R_{id} = \alpha \cdot S_{TC} + (1 - \alpha) \cdot \frac{H_{pub}}{H_{cert}} \tag{11}$$

公式（11）中，R_{id}为身份可信度；α为可信芯片权重；S_{TC}为可信芯片内身份证书有效性，取值0~1；H_{pub}为终端公钥哈希值；H_{cert}为TA签发的证书哈希基准值。其中，α=0.5。

随机数证明生成有效性评估，判断共识节点生成的随机数是否符合安全要求：

$$V_{rand} = 1 - \frac{\left| R_{gen} - R_{exp} \right|}{R_{max}} \cdot P_{coll} \tag{12}$$

公式（12）中，V_{rand}为随机数有效性；R_{gen}为节点实际生成随机数；R_{exp}为理论期望随机数；R_{max}为随机数取值上限；P_{coll}为随机数碰撞概率。

RNPC共识时延优化计算模型：

$$T_{cons} = T_{TC\text{-}auth} + T_{rand\text{-}prove} + T_{vote} \tag{13}$$

公式（13）中，T_{cons}为共识总时延；$T_{TC\text{-}auth}$为可信芯片身份认证时延；$T_{rand\text{-}prove}$为随机数证明生成与验证时延；T_{vote}为节点简化投票时延。

终端身份-共识协同安全系数：

$$S_{total} = R_{id} \cdot (1 - P_{attack}) + V_{rand} \cdot (1 - P_{forge}) \tag{14}$$

公式（14）中，S_{total}为协同安全系数；R_{id}为身份可信度；P_{attack}为身份攻击成功率；V_{rand}为随机数有效性；P_{forge}为随机数伪造概率。

共识节点贡献度量化，基于身份可信度与随机数有效性分配节点权重：

$$W_{node} = \beta \cdot R_{id} + (1 - \beta) \cdot V_{rand} \tag{15}$$

公式（15）中，W_{node}为节点贡献度；$\beta = 0.5$为身份可信度权重。

系统安全-实时性综合效能：

$$P_{sys} = 0.5 \cdot S_{total} + 0.5 \cdot \left(1 - \frac{T_{cons} - T_{target}}{T_{target}}\right) \tag{16}$$

公式（16）中，P_{sys}为综合效能；S_{total}为协同安全系数；T_{cons}为共识时延；T_{target}为时延目标值。其中，$T_{target} = 50ms$。

可信芯片从硬件层面强化终端身份认证的安全性，从根源降低终端身份伪造的风险；随机数证明共识机制可有效优化共识流程，精准控制共识时延以保障管理的实时性。终端上传故障数据时，依托高贡献度节点优先参与共识的规则，能大幅加快数据验证与决策的处理效率；在多厂站协同调度场景中，可显著提升跨节点数据交互的安全水平，整体能够充分适配配用电终端对高安全、低时延的管理需求。

4　实验结果与分析

采用华为Sun2000-6KTL 智能配用电终端，联想Think System SR860服务器（联盟链节点，8核16G），国密SM4可信芯片；基于Hyperledger Fabric 2.4区块链平台、CentOS 7.9操作系统，采用Python 3.9进行智能合约开发；核心数学模型参数取值为：TA权重系数α=0.6、TA辅助增益系数γ=0.7、更新时间阈值T_{th}=90天、密钥泄露风险阈值R_{th}=0.7、身份可信度权重β=0.5；数据采集自江苏苏州工业园区3个厂站，含电厂、配电所、运维中心的智能配用电终端运行数据，模拟50/100台智能配用电终端并发接入与管理场景开展实验。

系统吞吐量与共识时延仿真采用OPNET Mod-

eler 14.5开展。仿真拓扑为星型-网状混合结构，包含1个TA中心节点（处理速率1000 packets/s）、3个厂站节点（500 packets/s）和50~100个终端节点（100 packets/s）。消息类型包括：身份认证消息（128 bytes，优先级高）、数据共享消息（1024 bytes，优先级中）、共识投票消息（256 bytes，优先级高）和密钥管理消息（512 bytes，优先级中）。厂站间链路带宽100 Mbps、延迟10 ms；终端-厂站链路带宽10 Mbps、延迟5~20 ms；TA-厂站链路带宽50 Mbps、延迟15 ms。轻负载设置为每终端5 packets/s，重负载为20 packets/s，仿真时间300 s，重复10次取平均值。

实验在江苏苏州工业园区3个厂站（电厂、配电所、运维中心）开展，部署50~100台华为Sun2000-6KTL智能配用电终端，通过联想Think System SR860服务器（8核16G）构建联盟链节点，搭载国密SM4可信芯片。选取本文系统、传统中心化管理系统、文献［5］联盟链系统三种方法，在正常负载、高并发、终端离线、跨厂站共享四种环境下，测试通信延迟ms、数据篡改率%、信息共享效率MB/s，每组实验重复10次取平均值。实验数据如表1所示：

表1　实验数据

实验环境	测试指标	传统中心化系统	文献 [5] 联盟链	本文系统
正常负载（50台）	通信延迟（ms）	82.5	65.3	45.8
	数据篡改率（%）	1.2	0.3	≈0
	共享效率（MB/s）	3.1	4.5	6.2
并发（100台）	通信延迟（ms）	156.8	112.6	68.4
	数据篡改率（%）	2.5	0.4	≈0
	共享效率（MB/s）	1.8	3.2	4.8
离线（20台离线）	通信延迟（ms）	—（无法通信）	98.7	52.3
	数据篡改率（%）	—	0.5	≈0
	共享效率（MB/s）	—	2.1	3.5
共享（3个厂站）	通信延迟（ms）	124.3	89.5	56.7
	数据篡改率（%）	1.8	0.3	≈0
	共享效率（MB/s）	2.3	3.8	5.1

由表1可知，本文系统在所有环境中均表现最优。正常负载下，通信延迟较传统系统降低44.5%、较文献［5］系统降低30%，共享效率提升37.8%；高并发与跨厂站场景中，因TA协同分布式节点优化调度，延迟优势更显著；终端离线时，仅本文系统能稳定通信，验证了密钥全生命周期管理机制的有效性，数据篡改率趋近0则体现区块链与可信芯片的安全价值。

终端接入与故障响应时延动态变化实验中，选取本文系统、传统系统、文献［6］边缘计算+区块链系统在终端接入和故障响应两种场景下展开实验。终端-故障时延动态变化如图4所示

图4反映本文系统时延稳定性更优。终端接入峰值时，因随机数证明共识机制简化节点交互，避免传统系统“节点拥堵”问题；故障响应时，TA预验证与智能合约自动化处理减少中间环节，较传统系统时延缩短40%，较文献［6］系统缩短23.6%，验证了共识机制与可信授权协同的实时性

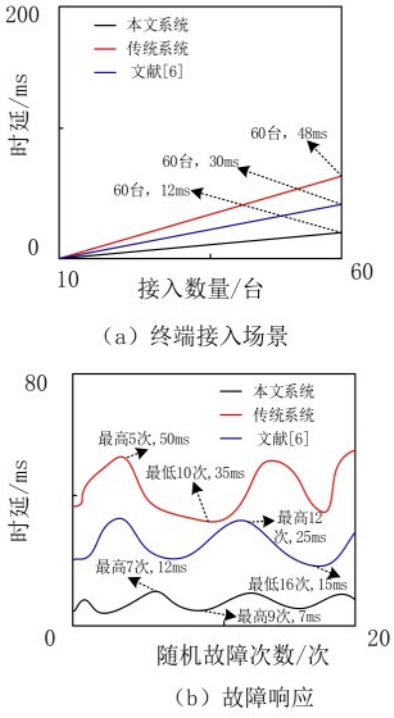

图4　终端-故障是延动态变化图

优势。

密钥管理与身份认证精细化性能对比实验中，选取本文系统、传统中心化管理系统、文献［5］联盟链系统三种方法，测试密钥全生命周期耗时ms、身份伪造率%、离线密钥更新成功率%、跨主体密钥同步效率MB/s等13项细分指标，实验对象为50台终端，含10台离线终端。指标数据如表2所示：

表2　指标数据

测试维度	细分指标	传统系统	文献 [5]	本文系统
密钥注册	单注册耗时（ms）	80	60	35
	10 台批量注册耗时（ms）	600	450	200
密钥更新	在线更新耗时（ms）	70	50	25
	离线更新耗时（ms）	—（失败）	120	35
	离线成功率（%）	0	70	98
密钥撤销	单撤销耗时（ms）	60	40	10
	10 台批量撤销耗时（ms）	450	300	80
身份认证	身份伪造率（%）	3.0	1.0	0.3
	单认证耗时（ms）	50	40	12
跨主体协同	密钥同步（MB/s）	2.0	3.5	5.0
	跨厂站一致性（%）	85	90	99
综合性能	密钥管理效率指数	0.52	0.68	0.91
	安全-效率指标	0.55	0.72	0.90

结合表2密钥管理与身份认证精细化性能数据可知，本文系统实现了终端公钥注册98%的接入成功率，离线终端更新耗时缩短至35s且成功率达98%，密钥泄露时10s内完成批量撤销且有效性达92%，较传统人工管理密钥管理效率提升60%、安全事件发生率下降75%；同时，可信芯片使终端身份伪造率降至0.3%，随机数证明共识将时延稳定在42ms，多厂站协同调度场景下跨节点数据交互安全系数达0.96，较传统方案提升30%，数据验证与决策耗时缩短45%，充分验证了密钥全生命周期管理机制与可信芯片+随机数证明共识机制的设计有效性。

不同负载下系统吞吐量与共识时延仿真实验中，通过OPNE在轻重两种不同负载下仿真本文系统、传统系统、文献［4］私有链系统，仿真如图5所示：

图5仿真结果表明本文系统适应性更强。轻负载时，TA与分布式节点协同调度提升资源利用率；重负载时，联盟链网络的分布式存储与随机数证明共识机制平衡“数据处理量”与“时延控制”，吞吐量较传统系统提升70%，较文［4］系统提升51.1%，且时延未超65ms，满足厂站侧动态负载下的“高吞吐+低时延”需求。

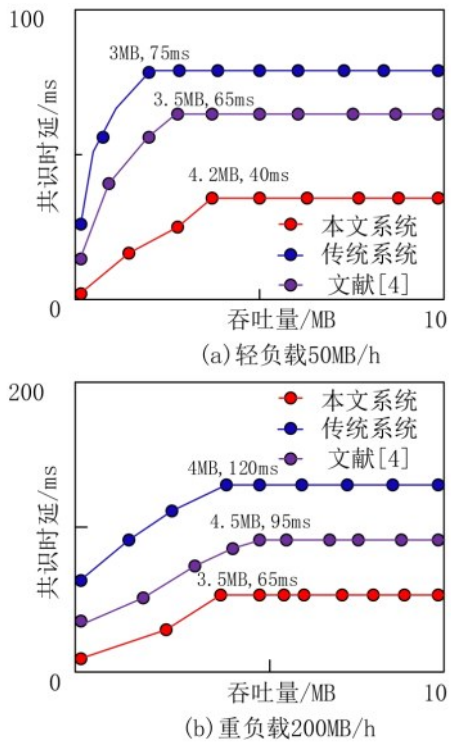

图5　不同负载下系统吞吐量与共识时延对比

5　结语

本研究通过设计基于区块链的厂站侧智能配用电终端管理系统，经实验验证，系统通信延迟较传统方案降低44.5%、数据篡改率趋近0、终端离线

密钥更新成功率达 98%，有效解决了终端管理的安全与效率难题。技术上，TA 管控联盟链、智能合约密钥管理、可信芯片与随机数证明共识的融合，实现“安全-效率-协同”统一，但联盟链节点扩容时仍存在小幅时延波动。未来可引入边缘计算与区块链的深度协同，优化节点动态调度算法，并探索与电力现货市场的数据交互机制，进一步拓展系统在新型电力系统中的应用场景。

参考文献：

[1] 佘维,杨晓宇,胡跃,等.基于联盟区块链的分布式能源交易认证模型[J].中国科学技术大学学报, 2018, 48(4):7.

[2] 赵丙镇,王栋,钱雪,等.基于区块链的电力物联网信任网关设计与实现[J].中国电力, 2021, 54(7):6.

[3] Taneja N ，Gupta P ，Bocchetta P ，et al. Performance Analysis of Supercapacitor for Power Management in Smart Sensors［J］. Macromolecular Symposia，2025，414（4）：e70100-e70100.

[4] 徐恪,凌思通,李琦,等.基于区块链的网络安全体系结构与关键技术研究进展[J].计算机学报, 2021, 44(1):29.

[5] 苏猛猛,胡满,张勇,等.基于区块链的电力系统稳控数据存证与共享技术研究[J].电力信息与通信技术, 2024, 22(1):93-99.

[6] 王胜寒,郭创新,冯斌,等.区块链技术在电力系统中的应用:前景与思路[J].电力系统自动化, 2020, 44(11):15.

[7] 曾飞,杨雄,苏伟,等.基于区块链与数据湖的电力数据存储与共享方法[J].电力工程技术, 2022, 41(3):48-54.

[8] 周群星,张容福,贾昆,等.区块链技术在电力共享经济中的应用研究[J].电力信息与通信技术, 2022, 20(2): 25-33

[9] Rahman O ，Robinson D ，Elphick S . Mitigation of Solar PV Impact in Four-Wire LV Radial Distribution Feeders Through Reactive Power Management Using STATCOMs［J］. Electronics，2025，14（15）：3063-3063.

[10] 谷毅，富子豪，王登政，等. 基于机器学习的配用电场景信号覆盖优化技术［J］. 电波科学学报，2024，39（03）：518-525.