基于区块链预言机的安全高效电力数据共享平台构建方法

鲁宁[1,2]，陈芳玉[1,3]，刘增辉[1]，王庆豪[1]，史闻博[1,2]，马建峰[4]
（1.东北大学计算机科学与工程学院，辽宁 沈阳 110819；2.河北省海洋感知网络与数据处理重点实验室，河北 秦皇岛 066004；
3.国网辽宁省电力有限公司沈阳供电公司，辽宁 沈阳 110811；4.西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘　要：针对已有基于区块链预言机的数据共享平台在面对电力数据规模庞大、共享请求多样和数据隐私性强等特点时存在的可扩展性和安全性不足等问题，提出一种安全高效的电力数据共享平台构建方法，简称Powsharing。首先，遵循高内聚、低耦合的功能划分原则，设计一种基于多预言机协作的数据共享模型，通过可垂直切分的分布式预言机结构，实现功能与性能同步扩展；然后，针对潜在的安全风险（如隐私泄露、降质攻击和假冒攻击等），设计一种安全的电力数据共享协议，利用CKKS同态加密、ECDSA签名、实体信任度评估等技术，有效保障系统的安全性。通过理论分析和实验验证，所提方案相比其他类似方案具有显著优势，在保护数据隐私的同时能够将共享效率至少提升了15%。

关键词：智能电网；电力数据共享；区块链预言机；安全；高效
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025101

Secure and efficient power data sharing platform construction approach based on blockchain oracle

LU Ning[1,2], CHEN Fangyu[1,3], LIU Zenghui[1], WANG Qinghao[1], SHI Wenbo[1,2], MA Jianfeng[4]
1. School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
2. Hebei Key Laboratory of Marine Perception Network and Data Processing, Qinhuangdao 066004, China
3. Shenyang Power Supply Company of State Grid Liaoning Province Electric Power Co., Ltd., Shenyang 110811, China
4. School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: When taking the diversity of power data sharing, the privacy of power data and the large scale of power data into consideration, the existing data sharing platforms would suffer the following disadvantages: the low scalability and the poor security. For this reason, a secure and efficient power data sharing platform construction approach termed Powsharing was proposed. Firstly, a data sharing model based on collaborative multi-blockchain oracles was designed. To support both functional and performance scalability, a vertical division-based distributed oracle architecture was adopted, which followed the principle of high cohesion and low coupling. Next, to mitigate potential security threats in Powsharing (e.g., privacy leakage, degradation attack and spoofing attack), a secure data sharing protocol was developed, incorporating CKKS homomorphic encryption, ECDSA, and trust evaluation mechanisms. The rigorous theoretical analysis and extensive experimental verifications demonstrate that Powsharing significantly outperforms the prior works in terms of the efficiency and security. Specifically, Powsharing can achieve increased sharing efficiency (by about 15%) in comparison to prior work, without leaking the data privacy.

Keywords: smart grid, power data sharing, blockchain oracle, security, efficient

收稿日期：2025-02-08；**修回日期：**2025-06-03
通信作者：刘增辉，liuzenghui1227@163.com
基金项目：国家自然科学基金资助项目（No.62072092, No.62072093）；中央高校基本科研业务专项资金资助项目（No.2023FGYD001, No.2024GFZD003）
Foundation Items: The National Natural Science Foundation of China (No.62072092, No.62072093), The Fundamental Research Funds for the Central Universities (No.2023FGYD001, No.2024GFZD003)

0　引言

随着电力物联网的快速发展，智能电表安装数量逐年增加，其产生的用电数据也与日俱增。截至2022年12月，我国智能电表保有量已超过6.5亿，按每15 min上传32 B进行统计，单位周期电力数据传送量可达19.37 GB[1]。除了能源供应商，政府和市场参与者也需要掌握不同地区、不同用户群体的用电习惯和需求，以便制定更有效的市场策略[2]。因此，构建面向大规模智能电表的数据共享平台具有重要意义。

电力数据共享平台作为数据请求方（如能源供应商、政府等）和数据提供方（如不同地区电力公司）之间的沟通桥梁，其作用是帮助双方高效、可靠地分享电力数据，以便实现电力价格实时调整和源网荷储协同保供。相比于传统基于云服务的中心化数据共享平台[3-9]，考虑到区块链去中心化、可公开审计、防篡改等特性，利用它来直接构建共享平台既能保证系统可靠性，又能实现分享过程公开可验证，该方法一经提出就受到研究者广泛关注[10-15]。当进一步考虑到区块链的封闭性使智能合约无法与现实世界直接交互及其强一致性使智能合约通常只能串行执行[16]，引入预言机来构建区块链共享平台就成为必然选择——既能帮助区块链主动收集链下电力数据，实现数据提供方与共享平台的实时交互，又能辅助智能合约完成数据聚合操作，通过计算卸载加快智能合约执行效率。

鉴于数据提供方的多样性和动态出入等特点，为了在降低模块间耦合度的同时控制系统复杂度，区块链通常引入预言机服务提供商（如Provable Oracle[17]）来构建数据共享平台。基于区块链预言机的电力数据共享过程如图1所示。假设某能源供应商D希望统计某时段内秦皇岛电力公司A和唐山电力公司B的整体平均用电量数据，D首先调用数据共享请求合约来发起共享任务。监听到任务后，预言机服务提供商在链下向A和B分别发送电力数据请求消息。收到A、B回复的消息数据后，预言机服务提供商在链下进行聚合计算操作，并调用聚合结果上链合约将聚合结果上链。D通过监听链上合约来获取结果。

基于区块链预言机的电力数据共享平台需实现2个功能：链下数据获取和聚合结果分享。然而，考虑到电力数据规模庞大、共享请求多样、数据隐私性强等特点，电力数据共享平台构建可能面临如下2个挑战。

1)可扩展性不足。鉴于共享请求的多样性以及智能电表安装规模的不断增加，这就要求电力数据共享平台应具备强扩展性，保证系统性能不会因请求类型增多或数据规模增大而下降。然而，当前区块链共享平台通常采用基于集中式预言机的系统架构[18]，而有限的预言机容量使系统的性能扩展力大都较弱。为此，部分学者提出了基于分布式预言机的数据共享系统架构[19-23]。不过，这些架构往往采用基于拷贝的水平扩展模式，无法应对逐渐增加的共享请求类型，导致功能扩展力低，进而增加部署和维护成本。因此，如何保证共享平台的高可扩展性就成为本文第一个挑战。

2)安全防护能力弱。引入以营利为目的的预言机服务提供商使共享平台存在以下风险：泄露那些潜藏着公司运营和住户用电行为等隐私信息的电力

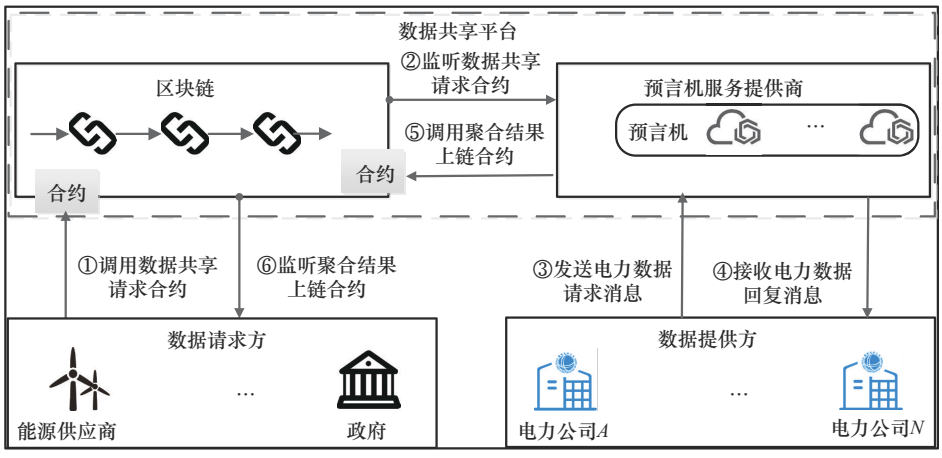

图1　基于区块链预言机的电力数据共享过程

数据；发起降质攻击，通过降低聚合精度来误导请求方，使其做出错误决策。基于此，那些允许数据直接获取和公开计算的基于区块链预言机的数据共享平台不再适用于本文场景[18,20-21]。虽然基于可信硬件的数据共享平台构建方案能够在不泄密和保质的前提下完成数据聚合[19]，但是它们也会带来昂贵的部署和维护成本。此外，少数方案允许预言机通过采用盲化或简单加密技术来隐藏数据，试图在不泄露隐私信息的前提下完成数据提取任务[22-23]。然而，它们通常不支持电力数据聚合操作，若直接使用，则会影响聚合精度。同时，它们也无法抵御降质攻击。因此，如何实现安全的数据共享则成为本文第二个挑战。

针对上述问题，本文提出一种安全高效的电力数据共享平台构建方法——Powsharing。首先，引入可垂直切分的分布式结构，遵循高内聚、低耦合的区块链预言机功能划分原则，设计基于多预言机协作的共享平台系统模型，既能支持因电力数据增加所需要的系统性能扩展，又能支持因共享请求类型增多所需要的系统功能扩展。然后，综合分析聚合运算特点以及预言机服务提供商的信任行为特征，利用 CKKS（Cheon-Kim-Kim-Song）同态加密、椭圆曲线数字签名算法（ECDSA）、实体信任度评估等技术，设计安全的电力数据共享协议，既能实现隐私数据聚合，又能保证结果的可信性。

为了验证本文提出的方法，首先对安全性进行了理论证明；然后利用 FISCO BCOS 区块链、Kafka 消息队列和 MapReduce 等技术搭建了一个电力数据共享原型系统；最后测试不同参数配置下系统性能变化情况，并与其他经典方法进行比较。结果表明，Powsharing 不仅能够有效地保护电表数据隐私，还能很好地提升共享效率；在原型系统中，共享周期约为 0.5 s。

1　研究背景和相关研究

本节给出电力数据共享问题的定义，推断出数据共享平台应满足的性能指标，以此为参照，指出已有方法在应用到电网场景中存在的问题，进而阐明本文研究动机。

1.1　电力数据共享问题定义

定义 1　电力公司数据 $\mathrm{ED}_{w_i}=(\mathrm{SD}^1_{w_i},\cdots,\mathrm{SD}^n_{w_i})$ 表示电力公司 w_i 管辖下的所有智能电表的相关数据，$\mathrm{SD}^k_{w_i}=(a_1,\cdots,a_z)$ 表示 w_i 管辖下智能电表 k 的标识、位置、用电、运行等属性，如电表 ID、地址、用电量、缴费数量、用户数量、电压指数等。

定义 2　电力数据共享请求可被定义为五元组 PDS=(D,W,E,C,O)，具体含义如下。

D 为数据请求方，如能源供应商、政府等。

$W=\{w_1,\cdots,w_k\}$ 为涉及的所有数据提供方。

$E=\{f(\mathrm{ED}_{w_1}),\cdots,f(\mathrm{ED}_{w_k})\}$ 为涉及的所有数据，其中，$f(\cdot)$ 表示属性数据抽取函数，负责从数据 ED_{w_i} 中提取与共享请求相关的电表属性。

$C\in\{c_1,\cdots,c_m\}$ 为涉及的共享请求类型，如指定时段内某地区的用户总数、缴费总量（或用户平均缴费量）、用电总量（或用电平均量）以及电压指数或温度异常的电表数量等。

$O\in\{o_1,\cdots,o_m\}$ 为与共享请求 C 对应的聚合操作函数，如累加、均值、方差、去除均方差大于指定倍数的异常值等。

给定电力数据共享请求 PDS=(D,W,E,C,O)，整个回复过程包括 2 个独立阶段：电力数据获取和结果数据上传。前者负责从所有数据提供方 W 中提取相关电力数据 E；后者对 E 执行聚合操作 O，并将结果 $O(E)$ 返回给数据请求方 D。也就是说，电力数据共享 F_{PSD} 依赖于 2 个独立事件：获取事件 f^E_{PSD} 和上传事件 f^O_{PSD}。根据概率乘法定理，F_{PSD} 可形式化为

$$F_{\mathrm{PSD}}=f^E_{\mathrm{PSD}}f^O_{\mathrm{PSD}} \tag{1}$$

为了适应不断增加的共享请求类型以及随时加入或退出的数据提供方，引入数据共享平台来充当数据请求方与提供方的沟通桥梁就成为一种必然选择。与基于双方直接交互的系统架构相比，这种基于中间件的架构不仅能适应共享请求多变性，还能满足数据提供方的自主性。在此基础上，根据式(1)，为了保证 F_{PSD} 成功率，数据共享平台应同时保证 f^E_{PSD} 和 f^O_{PSD} 高效地执行。然而，考虑到共享请求的庞大规模以及电力数据的隐私性，构建电力数据共享平台需满足以下要求[24-25]。

1)高可靠性。共享平台作为整个系统的核心，除了防止出现单点失效问题，还应保证身份与数据的可靠性。为了应对非法访问，平台应该提供

针对数据请求方行为的公开审计功能，进而完成对未授权请求方的身份追溯；为了保证共享数据的真实性，平台应实现对提供方的数据进行公开验证。

2)高可扩展性。针对共享请求的高并发性，平台应具备资源可扩展，避免请求失败；面对不断新增的共享请求类型，平台应实现功能可扩展，使用户能以较低的部署与维护成本完成共享；考虑到规模庞大的电力公司数据，平台应具备性能可扩展，按电表数据量来调整聚合操作所需的计算能力。

3)强安全性。除了反映地区经济和产业分布，电力数据还体现居民收入、家庭用电设备等情况，一旦泄露必然会给社会和个人带来较大风险。此外，平台一定要保证回复给请求方的数据质量，否则会误导它做出错误的经济决策。

1.2 相关工作

为加快数据要素的流通和激活数据的潜能，数据共享技术一经提出就受到了广泛关注。按照系统架构不同，已有方法可划分为如下3种：基于云服务的中心化数据共享、基于区块链的去中心化数据共享、基于区块链预言机的去中心化数据共享。表1给出了本文方案与现有方案的功能对比。

1.2.1 基于云服务的中心化数据共享

在中心化数据共享中，凭借云服务所拥有的强大存储和计算能力，提供方会将数据托管到第三方公司——云服务提供商（CSP, cloud service provider）和基于云服务的共享平台（如阿里巴巴的淘数据、华为数据集服务等）中，而请求方可以直接向该平台发起数据访问。考虑到CSP并非诚实可信，该方法可能存在数据隐私泄露或恶意篡改等问题。为此，学者们提出一系列可保护数据隐私和安全的共享方案。例如，Sun等[3]提出了一种面向自动驾驶车队的跨域数据共享机制，通过密文转换技术来实现车辆在不同车队之间灵活跨域授权，进而完成安全跨域共享；Deng等[4]设计了一种面向层级用户的数据共享机制，通过可穿刺加密和分层身份加密等技术来达到细粒度数据的分层共享；Sun等[5]提出一种面向多用户的数据共享框架，通过基于广播的可搜索加密技术，允许将目标数据分享给多个数据请求方法；Fugkeaw[6]设计了一种面向工业互联网的数据共享方案，通过融合基于密文策略的属性加密和属性证书技术，能够实现工业数据的细粒度安全共享；Ge等[7]提出了一种可抵御托管数据被恶意篡改的数据共享方法，通过可验证且公平的属性基代理重加密技术，能够准确检测云共享平台可能的恶意行为；Xu等[8]提出了面向群组数据共享的协作式可搜索加密机制，通过引入关键字服务器来抵御关键字猜测攻击和部署加密反向防火墙来对抗版本攻击，从而有效保护用户隐私；Wang等[9]提出面向移动终端的应用级数据共享服务框架，通过在移动级可信执行环境（TEE, trusted execution environment）中编写数据使用逻辑，从而保证它们的安全性。

表1 本文方案与现有方案的功能对比

架构	方案	效率	可扩展性	无单点故障	安全性			聚合功能	无须硬件支持
					非数据托管	共享流程透明	隐私保护		
云服务*	文献[3-9]	高	高	×	×	×	√	×	√
区块链*	文献[10-15]	低	低	√	√	√	√	×	√
区块链预言机	文献[18]	低	低	×	√	√	√	×	√
	文献[19]	高	低	×	√	√	√	×	√
	文献[20]	高	低	√	√	√	√	×	×
	文献[11]	低	低	√	√	√	×	√	√
	文献[22]	低	低	√	√	√	√	×	√
	本文方案	高	高	√	√	√	√	√	√

注：*表示取性能最优的方案。

虽然中心化数据共享具备易于实现、运行效率高、方便扩展等特点，但是存在以下 2 个难以避免的缺陷：单点故障，一旦云共享平台发生故障或遭到攻击，整个系统将面临瘫痪的风险；数据泄露和篡改问题，提供方一旦将数据管控权托付给 CSP，无论采用何种密码保护技术，都难以彻底根除 CSP 对数据造成的潜在风险。

1.2.2　基于区块链的去中心化数据共享

借助区块链的去中心化、防篡改、可追溯等优势，所有共享参与方作为链成员共同组建一个基于区块链的数据共享平台。之后，提供方通过智能合约将数据上传到链上，而请求方在共识结束后则直接从本地获取所需数据。然而，鉴于区块链的吞吐量较低且链上数据公开透明，该方法必然存在效率和隐私泄露问题。为此，学者们提出一系列可保护隐私的高效数据共享方案。例如，Hu 等[10]最早设计一种基于区块链的电子病历共享方案，其中数据提供方将病历的元数据上传到区块链，而数据请求方以矿工身份参与共识，采矿的奖励为访问数据的权利；Huang 等[11]提出了面向车联网的安全数据共享方案，通过零知识证明和区块链分片等技术，在提升共享效率的同时保护了分享车辆的身份隐私；Hassija 等[12]提出了面向车辆到电网（V2G, vehicle-to-grid）的数据共享方案，将基于区块链的 V2G 网络改造为有向无环图，提升微事务的吞吐量；Garcia 等[13]提出了一种面向健康生态的数据共享方案，通过设计新型的共识协议和交易结构，使区块链适应健康数据高效共享的需求；Tan 等[14]提出一种针对传染性病人的医疗数据共享方案，利用区块链进行统一身份认证，并将公钥、撤销身份列表等信息共享到区块链上，实现病历随时可追踪、可撤销；Zhang 等[15]提出一种面向元宇宙的数据共享方案，该方案将非交互式零知识证明集成到基于密文策略的属性加密（CP-ABE）的密钥并用智能合约来完成访问控制。

虽然基于区块链的数据共享能够避免中心化数据共享所引发的单点故障和数据篡改问题，但是它存在严重的效率问题，具体原因如下。首先，区块链的封闭性要求每个数据提供方只有在全部数据都上链后（而不是按需上链），才允许数据请求方对它们进行提取。考虑到提供方的数据规模庞大且不断增加，其数据的上链共识时间必然很长，从而延长数据共享时间。然后，由于部分请求方通常不需要电表数据本身，而是它们聚合后的数据，因此共享平台必须使用智能合约对电表数据进行聚合。考虑到共享请求的高并发性和智能合约的串行化执行，这会影响共享请求处理时间。

1.2.3　基于区块链预言机的去中心化数据共享

为了减少上链数据和降低区块链计算负载，通过引入预言机来打破区块链封闭性、卸载链上聚合操作，成为实现聚合数据按需共享的必然途径。然而，预言机作为链上与链下的桥梁，其计算力、隐私性和安全性必然会影响系统整体性能。为此，研究者们提出一些解决方案。比较经典的方案包括：Shi 等[18]提出一种面向大规模物联网设备、可达三重信任的数据共享方法，分别设计基于预言机的数据收集机制来保证数据真实、基于区块链的分布式身份管理机制来保证设备身份安全可信、轻量拜占庭容错算法来提升物联网场景下区块链协作可靠性及性能；Woo 等[19]提出一种面向供应链的时变数据共享方案，通过使用 Intel 软件防护扩展（SGX, software guard extension）和安全传输层协议（TLS, transport layer security）来保证数据完整性，同时设计面向分布式预言机的信任评估策略来最小化预言机响应时间，提升共享效率；Lin 等[20]提出一种面向工业物联网的数据交换方案，借助基于水平扩展的分布式预言机来获取外部实时数据和孤立数据，通过协作计算机制来扩展工业生态的学习能力；Pasdar 等[21]提出了一种面向畜牧供应链的数据共享方案，通过将私有链与预言机相结合，在保护 DNA 指纹数据隐私的同时实现链下数据自动化访问；Manoj 等[22]提出面向农业物联网的数据共享方案，分别通过分布式数字身份技术来实现隐私保护下的农业设备认证，以及分布式预言机与多方安全计算技术来实现安全地链下数据获取；Zhang 等[23]提出了车联网群智感知下基于区块链预言机的数据共享方案，通过设计基于修剪前缀二叉树的车辆数据聚合和隐私保护、公平的链上数据聚合，既能保证感知数据在发布到区块链之前的可靠性，又能保证链上数据的隐私性。

基于区块链预言机的去中心化数据共享确实能够提升分享效率，但是已有相关研究在应用到电网场景中存在以下不适：规模庞大的电表数据要求预言机采用分布式结构模型（即多个预言机协同服

务），然而传统基于水平扩展的分布式预言机无法应对不断变化的共享请求；电表数据的隐私性要求预言机在不泄密的前提下完成针对数值数据、运算较复杂的聚合操作，然而简单的混淆或加密技术无法实现此类功能。

2　扩展性增强的电力数据共享平台构建方法

为了高效地实现电力数据分享，本文设计一种可扩展性增强的数据共享平台构建方法Powsharing。在智能电网场景下，数据请求方不需要电表源数据，而是它们聚合后的结果。再结合数据自身的特点，本文方法采用与传统共享平台不同的系统模型。

2.1　系统模型

当接收到数据共享请求PDS=(D,W,E,C,O)时，数据共享平台需要先从所有数据提供方W中提取相关电力数据E，然后对E执行聚合操作O，将结果$O(E)$返回给数据请求方D。基于此，为了保证系统可靠性和运行效率，本文同时引入区块链与预言机来共同构建数据共享平台，其中前者负责发布共享任务和聚合结果，后者负责收集数据和聚合操作。相比于公有链，联盟链（如HyperLedger Fabric）更适合搭建共享平台，原因如下：增加访问控制功能——只有被提供方允许的请求方才能加入共享平台，进而发起共享请求任务；高吞吐量——即使面对因请求规模增大而不断增加的海量区块，其高效的共识机制也能保证相关存储任务迅速完成；扩展功能——除了数字交易，它更容易实现本文所需的信息交互功能。因为，本文使用联盟链来作为共享平台的基础，从而保障共享用户身份的可控性和对大规模共享请求的支持。此外，鉴于电力数据规模和共享请求类型的不断增加，基于垂直切分的多预言机分布式协同结构明显更适合电网场景。为了方便扩展共享请求类型，遵循功能高内聚、低耦合的原则，本文又将预言机细分为4类：监听预言机（MO, monitoring oracle）、提取预言机（EO, extracting oracle）、聚合预言机（AO, aggregating oracle）和上链预言机（UO, uploading oracle）。此外，为了降低系统复杂度和控制运营成本，它们可租用预言机服务提供商（OSP, oracle service provider）的设备。为了避免单点故障，每个OSP应根据预言机负载情况灵活调整其数量；为了实现去中心化，保证系统高可信，请求方可以选择多个独立的OSP来并行执行共享任务。

基于上述分析，本文提出了一种基于多区块链预言机协作的电力数据共享平台系统模型，如图2所示。一方面，为了增强结果可靠性和提升系统可用性，本文允许数据请求方同时租用多个OSP为其并行重复地执行监听、提取和聚合任务（即使其中一个发生故障，也不会中断服务）；另一方面，为了适应不同请求方的格式需求和方便聚合结果的整合，上链预言机应由政府部门来统一提供。此外，所有在区块链上实现的功能需用智能合约来编写并将它们成功部署。之后，相关用户就可调用合约，而每个链上节点都可监听、查看合约运行后的日志。基于此，实体之间的通信方式总共包括3种：主动调用链上智能合约、被动监听链上合约运行日志和直接消息传递。

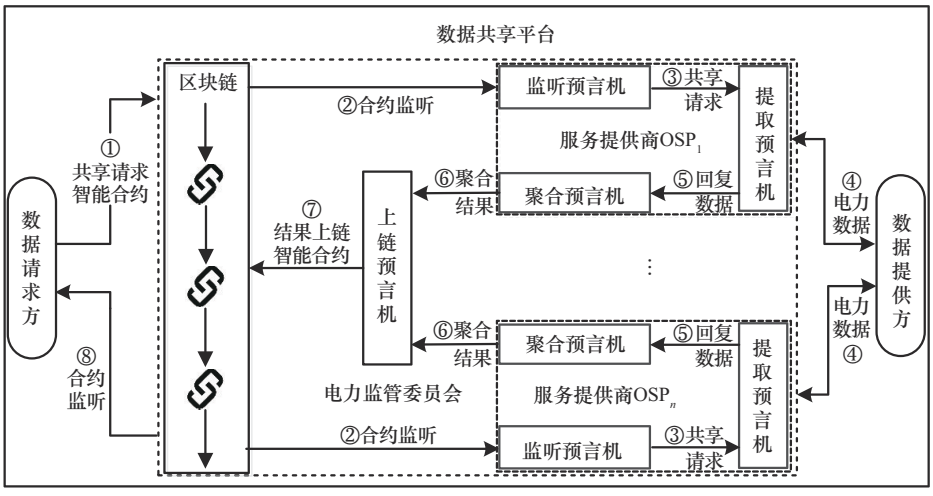

图2　基于多区块链预言机协作的电力数据共享平台系统模型

本文假设数据请求方和提供方均为可信方。除此之外，电力数据共享平台系统模型还包含 5 类实体，其功能描述如下。

区块链由所有数据请求方、数据提供方、预言机服务提供商以及国家电力监管委员共同组建而成，主要用于发布共享任务与聚合结果。其上部署 3 类智能合约：数据共享请求、监听预言机和上链预言机合约。为了在高并发环境下提升合约运行速度，每种类型的数据共享请求对应一个数据共享请求合约和上链预言机合约。

监听预言机由预言机服务提供商来维护，主要负责实时检查区块链上被数据共享合约调用的监听预言机合约状态。如果该数据共享合约与自身提供商相关，那么就生成与之对应的共享任务，并将该任务发送给提取预言机。

提取预言机由预言机服务提供商来维护，主要负责源电力数据的获取。根据共享任务，它向所有相关数据提供方发送源数据请求消息，并在接收到数据后直接将其转发给聚合预言机。

聚合预言机由预言机服务提供商来维护，主要负责面向源电力数据的聚合计算，并将计算结果转发给上链预言机。计算类型由共享请求类型来决定，包括累加、均值、方差和去除均方差大于指定倍数的异常值等。

上链预言机由国家电力监管委员会来搭建和维护，通过调用上链预言机合约，将聚合结果发布到区块链。本文假设上链预言机是诚实且好奇的。

在系统初始化阶段，每个数据请求方根据自身需求来编写和部署数据共享请求合约和上链预言机合约。除了数据共享请求 PDS 的参数，该合约还需指明由哪些 OSP 来负责。假设某请求方 D_i 希望发起数据共享请求 PDS_j，与其对应的数据共享请求合约和上链预言机合约分别为 SSC_j 和 USC_j。根据式(1)，整个共享流程应分为以下 2 个阶段。

阶段 1：电力数据获取（包含步骤①~步骤④）。请求方 D_i 作为区块链节点，通过调用合约 SSC_j 在链上生成任务日志；一旦某 OSP 的 MO 发现该任务日志与自己相关，立即将链上日志转换为可执行任务并放入任务列表中，同时将其推送到 EO；根据任务信息，EO 向所有提供方 $W=\{w_1,\cdots,w_k\}$ 发起数据提取消息，同时任何 w_i 都有义务向 D_i 回复数据。

阶段 2：结果数据上传（包含步骤⑤~步骤⑧）。当收齐所有电力数据 $E=\{f(\mathrm{ED}_{w_1}),\cdots,f(\mathrm{ED}_{w_k})\}$ 后，EO 立即把它们推送给 AO；AO 执行聚合操作 O，并将结果 $O(E)$ 发送给 UO；UO 调用合约 USC_j，在链上生成结果日志；当 D_i 从结果日志中提取出所需数据时，整个共享任务结束。

2.2　基于垂直切分的分布式预言机设计

当面对大规模数据共享请求时，平台能否快速响应是评价其高效性的重要指标。基于此，本文重点设计基于垂直切分的分布式预言机。

2.2.1　具体实现

MO、EO 和 UO 是影响平台性能主要实体，其设计思路如下。

1)考虑到共享任务数量的动态变化，为了灵活调整系统运行成本，本文引入分布式消息队列技术（如 Kafka）来实现 MO，即在 MO 与 EO 之间构建消息队列，解耦消息传递流程，如图 3 所示。通过降低 MO 与 EO 的耦合性来使后者的投入数量能够随着消息队列长度动态伸缩，这既能控制投入成本，又能避免因资源短缺而造成的任务失败。

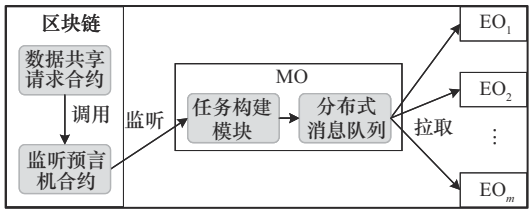

图 3　基于分布式消息队列的监听预言机

为了降低请求方与 OSP 耦合性，方便共享请求类型扩展，本文引入监听预言机合约 LSC，允许监听预言机在不做任何改动的条件下监听新增的共享请求类型，如合约 1 所示。此外，本文设计了数据共享请求合约 SSC，用于数据请求方生成任务日志并调用 LSC，如合约 2 所示。

合约 1　监听预言机合约 LSC

① 合约 LSC {

② 事件 LReq(string *D*, string *W*, string OSP, string *E*, string *C*, string *O*);

③ 函数 dataRequest(string *D*, string *W*, string OSP, string *E*, string *C*, string *O*) external {

④ 触发 LReq (*D*, *W*, OSP, *E*, *C*, *O*); //监听请求任务

⑤ }}

合约 2 数据共享请求合约 SSC

① 合约 SSC {

② address public ALSC;//监听预言机合约地址

③ address public AUSC;//上链预言机合约地址

④ 函数 setLSCaddress(address _LSCaddr) external{A_{LSC} = _LSCaddr;} //设置 LSC 地址

⑤ 函数 PDS(string *D*, string *W*, string OSP, string *E*, string *C*, string O) external {

⑥ 要求(A_{LSC}!=address(0),"LSCaddr not set");

⑦ LSC(A_{LSC}).dataRequest(*D*, *W*, OSP, *E*, *C*, *O*); //发布请求

⑧ }}

⑨ 接口 LSC{

⑩ 函数 dataRequest(string *D*, string *W*, string OSP, string *E*, string *C*, string *O*) external; //LSC 接口定义

⑪ }

2)考虑到提供方的数量众多且其数据分布异构化严重，本文引入 MapReduce 编程模式来实现 EO，每个数据提供方可作为一个 Map 节点，负责“映射”任务，而 EO 作为 Reduce 节点，负责“化简”任务，图 4 举例说明了详细过程。

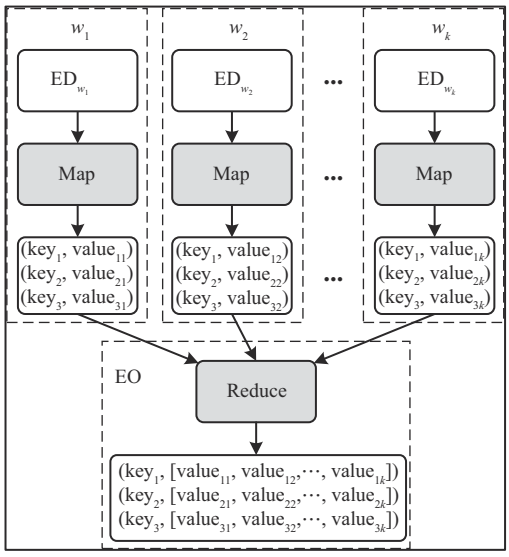

图 4 基于 MapReduce 的提取预言机

设数据提供方集合为$\{w_1,\cdots,w_k\}$，其中每个提供方 w_i 持有本地电力数据 EDw_i。在 Map 阶段，每个提供方 w_i 本地执行如下映射函数

$$\mathrm{Map}_{w_i}:\mathrm{ED}_{w_i}\rightarrow\{(k_j,v_{ij})|j\in[1,m]\} \tag{2}$$

其中，k_j 表示数据的特征键，m 为特征键数量，v_{ij} 为 k_j 对应的值。之后，w_i 将映射后的键值对发送给 EO。在 Reduce 阶段，EO 对收到的键值对数据执行如下化简函数

$$\mathrm{Reduce}:\{(k_j,v_{ij})|i\in[1,k],j\in[1,m]\}\rightarrow\{(k_j,V_j)|j\in[1,m]\} \tag{3}$$

其中，$V_j=\{v_{ij}|i=1\cdots k\}$。这种模式既能减少数据提供方与 EO 之间的数据传输量，节省带宽，又能支持绝大部分聚合运算，不影响共享请求类型的扩展。

3)UO 的功能较为单一，可以直接利用集群技术采用水平扩展方式来实现。这既能加快处理速度，又能避免其出现单点故障。UO 通过调用上链预言机合约 USC 来发布聚合结果，如合约 3 所示。

合约 3 上链预言机合约 USC

① 合约 USC{

② string public aggrData; //上链数据

③ 事件 DataReceived(address from, string data);

④ 函数 uploadDataOnChain(string data) external{

⑤ aggrData = data;

⑥ 触发 DataReceived(msg.sender, data);}//发布结果

⑦ 函数 getData() public view returns (string) {return aggrData;}

⑧ }

2.2.2 案例分析

假设河北省工业和信息化厅欲统计省内钢铁 H_1、机械制造 H_2、车辆制造 H_3、石油化工 H_4 等 m 种不同产业的全年用电总量。它的数据共享请求可定义为 PDS=(D,W,E,C,O)，其中，D=河北省工业和信息化厅，W= {w_1=石家庄供电公司,…,w_k=秦皇岛供电公司}，E={ $f(\mathrm{ED}_{w_1}),\cdots,f(\mathrm{ED}_{w_k})$ }，$f(\cdot)=\{\mathrm{ED}_{w_i}\rightarrow(k_i,c_i)|i=1\cdots m\}$，$C$=$m$ 种用电统计量，$O=\{(k_i,\sum_1^{|w|}c_i)|i=1\cdots m\}$。

在系统初始阶段，国家电力监管委员需要将合约 1 部署到区块链，数据请求方将合约 2 和合约 3 部署到区块链。在电力数据获取阶段，当监听到任务日志，MO 首先检查己方是否包含在 OSP 列表中。若包含，则立即提取任务信息{请求方 D，提供方列表 W，OSP 列表 OSPL，任务类型 C，聚合

操作 O，任务编号 T_{ID}=Hash($D||W||E||C||O$)，USC 地址 A_{USC}}并将它推送到任务消息队列中，然后由空闲 EO 主动从消息队列中拉取新任务。一旦获取任务信息，它以多线程方式分别向{$w_1,\cdots,w_k$}发起数据提取请求{D,w_i,OSP,C,O,T_{ID}}。针对共享请求类型 C，每个 w 会按照事先规定的 Map 函数完成属性数据的映射。在结果数据上传阶段，EO 会把从 w_i 收集到的数据{D,T_{ID},映射数据 mapData$_i$}按照 key 相同重新整合为{D,T_{ID},化简数据 reduceData}，然后 AO 针对每个 key 都执行一次累加聚合操作 O，并将{D, T_{ID}, <key,聚合结果 aggrData>}传给 UO，由 UO 调用合约 3，进而将 aggrData 上链。

3　安全的电力数据共享协议

考虑到当前复杂的网络环境，以营利为目的的第三方——OSP 的引入会使第 2 节设计的电力数据共享平台存在以下安全风险。

隐私泄露：借助预言机处理电力数据的契机，OSP 通过窃听与分析来探测数据中潜藏的公司运营和住户用电行为等隐私信息。

降质攻击：为了误导请求方做出错误决策，OSP 会控制聚合预言机 AO 降低服务质量，从而影响聚合结果精度。

假冒攻击：为了窃取电力数据，OSP 可能伪造请求方的身份，进而指使 EO 向提供方发起数据提取消息。

为了抵御上述攻击，本节提出一种安全的电力数据共享协议，以提高平台的安全性。

3.1　整体思路

防御上述威胁可能存在以下挑战。首先，为了防止 OSP 窥探隐私，最佳手段是在不影响聚合操作的前提下对提供方数据进行加密，这就需要可以支持加法、乘法、均方差的同态加密技术。然而，常见的同态加密技术要么只支持加法或乘法，却不支持均方差，如 Paillier 加密[26]和 ElGamal 加密[27]，要么需要配置可信第三方[28]。这些都不适合电力数据共享场景。然后，针对降质攻击，传统手段是通过可验证计算技术对聚合结果进行审计[29]。然而，可验证计算技术在生成证明时通常计算开销较大，影响共享平台的高效性。另一种可能的手段是要求 OSP 使用 SGX 来确保可信的聚合过程，但是这依赖于额外的硬件支持。最后，为了抵抗假冒攻击，最佳手段就是通过数字签名来保证请求方身份真实可信。不过，常见技术要么因签名长度过长而无法储藏于交易块容量较小的区块链，如 RSA 签名[30]和 Bliss 签名[31]，要么因尚未标准化而造成实现成本高，如 Schnorr 签名[32]。

基于上述分析，本文分别采用 CKKS 同态加密[30]、基于信任度的多方聚合结果融合策略和 ECDSA 签名来应对上述威胁。首先，CKKS 同态加密相比 BGV 方案和 BFV 方案，能够在密文上同时执行浮点数的加法、乘法、均方差等运算，且保持较为高效的计算性能。然后，多方聚合结果融合策略允许多个不相关的 OSP 反复聚合数据，依据信任度将它们的结果进行融合，能够有效缓解恶意 OSP 对最终结果的影响。该策略对聚合效率的影响较小，也不依赖可信硬件。最后，ECDSA 签名的长度较短、验证效率较快且已被广泛标准化，因此兼具安全性、效率和易实现等优势。

图 5 阐述了安全电力数据共享协议的工作流程。除了 PDS=(D,W,E,C,O) 和 OSP 列表 OSPL={OSP$_1$,$\cdots$,OSP$_m$}，数据请求方还使用 ECDSA 生成相关签名并将其写入 USC 中。此外，为了缓解恶意 OSP 对结果的影响，请求方会同时雇用多个 OSP 反复执行共享任务。一旦 MO 监听到任务日志，对应 OSP 就建立带有签名的共享任务。数据提供方通过验证签名就可确认请求方的身份，随后使用 CKKS 对 Map 函数的输出 value 进行加密，并将结果回传给 OSP。对应 EO 和 AO 能够在密文状态下顺利完成 Reduce 函数和聚合操作。之后，OSP 对聚合结果签名，并将结果和签名传给 UO。当 UO 收到所有 OSP 的聚合结果并验证签名后，通过评估每个 OSP 的信任度来计算结果权重，进一步计算所有结果的加权平均值，将其作为最终结果上链。

3.2　具体设计

整个安全电力数据共享协议包含以下 3 个阶段：系统初始化、电力数据获取和结果数据上传。

3.2.1　系统初始化阶段

该阶段主要完成密钥分配和合约部署，前者是通过区块链来传递 CKKS 和 ECDSA 的密钥；后者不仅需要计算 PDS 签名，还需将它写入 USC 中。

步骤 1：密钥分配。就 CKKS 同态加密来说，

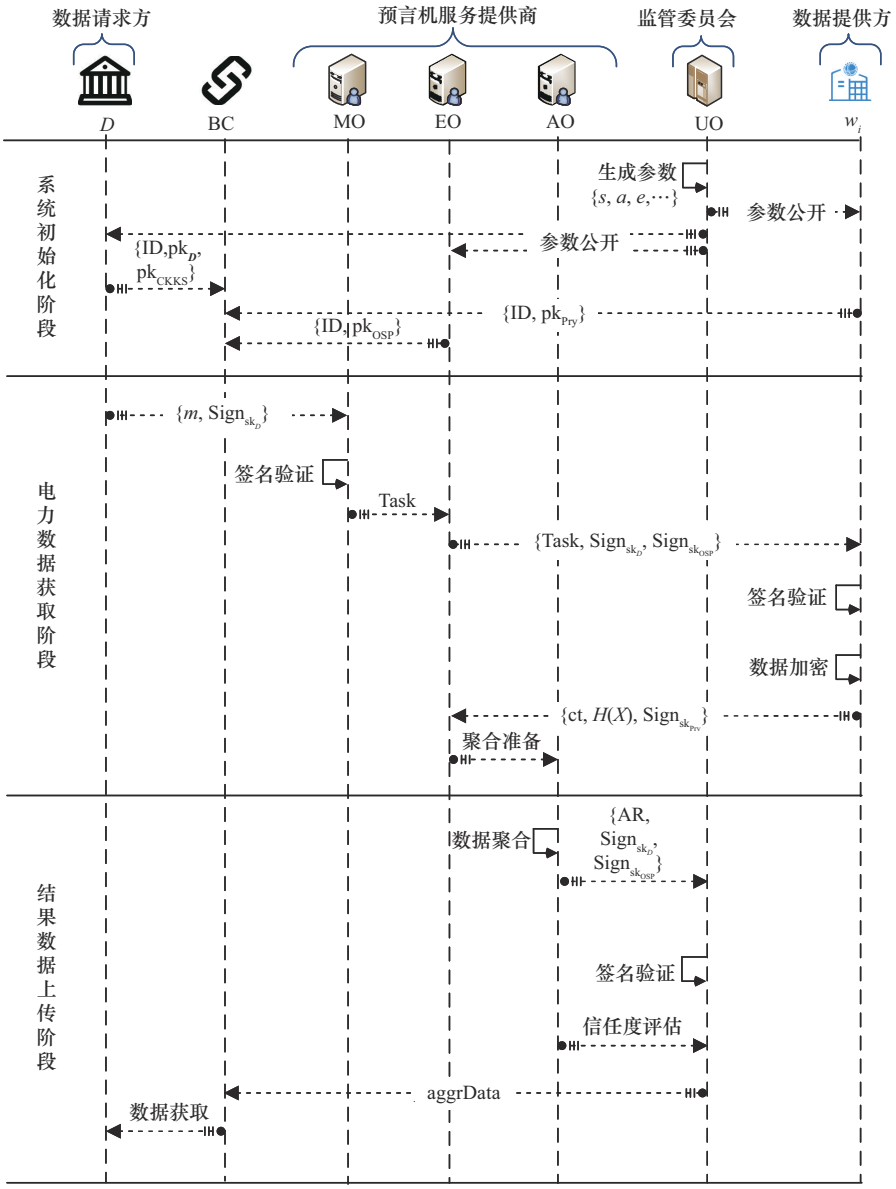

图5　安全电力数据共享协议的工作流程

首先UO定义多项式环$R_q=\mathbb{Z}_q[X]/(X^N+1)$，其中$q$为大素数，$N=2^k$为多项式阶次；选择3个随机多项式$s\in R_q$和$a\in R_q$，生成噪声多项式$e$。然后，数据请求方选择随机多项式$a_2\in R_q$，生成公私钥对$(\mathrm{sk}_{\mathrm{CKKS}}, \mathrm{pk}_{\mathrm{CKKS}})$和重线性化密钥$\mathrm{rlk}=(b_2,a_2)$，其中$\mathrm{sk}_{\mathrm{CKKS}}=(1, s)$，$\mathrm{pk}_{\mathrm{CKKS}}=((-a\cdot s+e) \bmod q, a)$，$b_2=e_2-a_2\cdot s^2$。最后，将$\{R_q, \mathrm{pk}_{\mathrm{CKKS}}, N\}$公布到区块链上。就ECDSA签名来说，首先选择一条椭圆曲线$E_p(a,b)$和基点G；给定私钥$\mathrm{sk}\in\mathbb{Z}_q$，公钥$\mathrm{pk}=\mathrm{sk}\cdot G$。然后，数据请求方、数据提供方和OSP分别生成公私钥对$(\mathrm{sk}_D, \mathrm{pk}_D)$、$(\mathrm{sk}_{\mathrm{Prv}}, \mathrm{pk}_{\mathrm{Prv}})$和$(\mathrm{sk}_{\mathrm{OSP}}, \mathrm{pk}_{\mathrm{OSP}})$。最后，将它们各自身份ID及其公钥发布到区块链上。

步骤2：合约部署。国家电力监委会部署LSC，同时将合约地址及接口公布给各个预言机服务提供商。数据请求方分别将SSC和USC部署到区块链上以便数据请求的发布。

3.2.2　电力数据获取阶段

该阶段主要完成数据获取的过程，与基本过程相比，重点增加了签名验证和同态加密过程。

步骤1：请求发起。数据请求方D首先生成数据请求消息m以及相关ECDSA签名$\mathrm{Sign}_{\mathrm{sk}_D}(m)=\{r, s\}$，其中，$r$为点$k\cdot G$关于$x$轴的值，$s=k^{-1}(H(m)+\mathrm{sk}_D\cdot r) \bmod n$，$k\in\mathbb{Z}_q$为随机数，$H()$表示具备单向性与抗碰撞性的SHA-256哈希函数；然后通过SSC

将包含 m 与 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$的请求发布到链上。

步骤 2：任务构建。当预言机服务提供商 OSP 的 MO 接收到数据请求后，首先利用公钥 pk_D 验证签名 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$，确保请求的合法性。若 $(H(m)\cdot s^{-1}\cdot G+ r\cdot s^{-1}\cdot \mathrm{pk}_D) \bmod n$ 的结果关于 x 轴的值与 r 相等则签名验证成功，否则验证失败。然后，MO 生成任务 task 连带签名 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$一起添加到消息队列中。根据队列长度，OSP 动态调整 EO 的数量，由其执行任务 task。

步骤 3：数据提取。当 EO 从 MO 处收到任务 task 后，首先生成签名 $\mathrm{Sign}_{\mathrm{sk}_{\mathrm{OSP}}}(\mathrm{task})$，其生成过程与 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$类似。然后，EO 向数据提供方 w_i 发送数据提取请求，包括任务 task、签名 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$和 $\mathrm{Sign}_{\mathrm{sk}_{\mathrm{OSP}}}(\mathrm{task})$。收到任务消息后，$w_i$ 首先利用公钥 pk_D 验证签名 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$，避免 OSP 伪造请求，同时利用公钥 $\mathrm{pk}_{\mathrm{OSP}}$ 验证签名 $\mathrm{Sign}_{\mathrm{sk}_{\mathrm{OSP}}}(\mathrm{task})$，确保 OSP 的身份真实性。一旦验证成功，$w_i$ 立即对上传数据 $\{x_0,x_1,\cdots,x_{n-1}\}$进行加密，具体过程如下：1)将数据编码为明文多项式 $m(X)=\Delta\cdot\sum_{i=0}^{n-1}x_iX^i$，其中 $\Delta=2^{\mathrm{scale}}$，scale 表示大整数；2)给定随机多项式 $u\in R_q$ 和噪声多项式 $e_1\in R_q$ 与 $e_2\in R_q$，使用公钥 $\mathrm{pk}_{\mathrm{CKKS}}$ 生成密文 $\mathrm{ct}=(c_0, c_1)$，其中 $c_0=b\cdot u+m(X)+e_1 \bmod q$，$c_1=a\cdot u+e_2 \bmod q$。然后，$w_i$ 将密文 ct 和签名 $\mathrm{Sign}_{\mathrm{sk}_{\mathrm{Prv}}}(\mathrm{ct})$提供给 EO。最后，EO 将提供方上传的数据发送到聚合预言机 AO。

3.2.3　结果数据上传阶段

该阶段主要完成数据聚合和结果上链，前者重点实现密文计算，而后者须融合多方聚合结果。

步骤 1：数据聚合。收到 EO 上传的数据后，AO 根据任务要求执行数据聚合操作。在电力数据共享场景中，常见的聚合操作包括求和 $\mathrm{ct}_{\mathrm{sum}}$、均值 $\mathrm{ct}_{\mathrm{mean}}$和方差 ct_σ。给定密文 $\{\mathrm{ct}_1, \mathrm{ct}_2, \cdots, \mathrm{ct}_n\}$，同态求和公式为

$$\mathrm{ct}_{\mathrm{sum}}=\left(\sum_{i=1}^{n}\mathrm{ct}_i\right) \bmod q=\left(\sum_{i=1}^{n}c_{0,i},\sum_{i=1}^{n}c_{1,i}\right) \bmod q \quad (4)$$

在此基础上，同态均值计算式为

$$\mathrm{ct}_{\mathrm{mean}}=\left(\frac{1}{n}\cdot\mathrm{ct}_{\mathrm{sum}}\right) \bmod q=\left(\frac{1}{n}\cdot\sum_{i=1}^{n}c_{0,i},\frac{1}{n}\cdot\sum_{i=1}^{n}c_{1,i}\right) \bmod q \quad (5)$$

同态方差计算式为

$$\mathrm{ct}_{\sigma^2}=\left[\frac{1}{n}\cdot\sum_{i=1}^{n}\left(\mathrm{ct}_i^2-2\cdot\mathrm{ct}_i\cdot\mathrm{ct}_{\mathrm{mean}}+\mathrm{ct}_{\mathrm{mean}}^2\right)\right] \bmod q \quad (6)$$

其中，ct_i^2、$\mathrm{ct}_i\cdot\mathrm{ct}_{\mathrm{mean}}$和 $\mathrm{ct}_{\mathrm{mean}}^2$ 都涉及同态乘法。给定密文数据为 $\mathrm{ct}_1=(c_{0,1},c_{1,1})$和 $\mathrm{ct}_2=(c_{0,2},c_{1,2})$，同态乘法计算式为

$$\mathrm{ct}_{\mathrm{mul}}=\left(c_{0,\mathrm{mul}},c_{1,\mathrm{mul}},c_{2,\mathrm{mul}}\right) \quad (7)$$

其中，$c_{0,\mathrm{mul}}=(c_{0,1}\cdot c_{0,2}) \bmod q$，$c_{1,\mathrm{mul}}=(c_{0,1}\cdot c_{1,2}+c_{1,1}\cdot c_{0,2}) \bmod q$ 和 $c_{2,\mathrm{mul}}=(c_{1,1}\cdot c_{1,2}) \bmod q$。然后，通过 $\mathrm{rlk}=(b_2, a_2)$将 $\mathrm{ct}_{\mathrm{mul}}$转化为二元组 $\mathrm{ct}_{\mathrm{remul}}=(c_0', c_1')$，其中 $c_0'=(c_{0,\mathrm{mul}}+c_{2,\mathrm{mul}}\cdot b_2) \bmod q$ 和 $c_1'=(c_{1,\mathrm{mul}}+c_{2,\mathrm{mul}}\cdot a_2) \bmod q$。

$\forall \mathrm{OSP}_i\in\mathrm{OSP}$，它的聚合结果为 $\mathrm{AR}^i=\{D, T_{\mathrm{ID}}, <\mathrm{key},\mathrm{aggrData}^i>\}$。一旦完成聚合过程，OSP 将数据请求方的签名 $\mathrm{Sign}_{\mathrm{sk}_D}(m)$、聚合结果 AR 以及聚合结果的签名 $\mathrm{Sign}_{\mathrm{sk}_{\mathrm{OSP}}}(\mathrm{AR})$发送给 UO。

步骤 2：聚合结果融合。当 UO 收到 OSP 的所有结果 $\{\mathrm{AR}^1,\cdots,\mathrm{AR}^{|\mathrm{OSP}|}\}$及相应的签名时，首先验证签名以确认数据请求与 OSP 身份的对应关系，未通过验证的聚合结果将被丢弃。然后，监管委员会须评估在 t_k 时刻每个 OSP_i 聚合结果的信任度 $z(\mathrm{OSP}_i|t_k)$。为了保证信任评估的准确性和客观性，本文除了给出了基于多维证据的交互满意度评估公式，如定义 5 所示，还进一步考虑时间因素对实体信任度的影响，给出基于满意度迭代的信任度评估公式，如定义 6 所示。给定信任度集合 $\mathrm{CS}=\{z(\mathrm{OSP}_1|t_k),\cdots,z(\mathrm{OSP}_{|\mathrm{OSP}|}|t_k)\}$，对其进行归一化处理：$\forall \mathrm{OSP}_i$，信任权重 $w_i=\frac{z(\mathrm{OSP}_1)}{\sum_{\mathrm{CS}}[z(\mathrm{OSP}_j|t_k)]}$。基于此，融合多方聚合结果的 aggrData 为

$$\mathrm{aggrData}=w_1\,\mathrm{aggrData}^1+\cdots+w_{|\mathrm{OSP}|}\,\mathrm{aggrData}^{|\mathrm{OSP}|} \quad (8)$$

需要注意的是，这些数据通常在密文状态下完成同态运算。当所有 OSP 的信任度都较低时，监管委员会应建议数据请求方重新选择一组 OSP。此外，当不同 OSP 的信任度偏差远大于均值时，建议去除影响较大的 OSP。

步骤 3：聚合结果上链。完成多方聚合结果的融合后，UO 将结果 aggrData 发布到链上。数据请求方从链上获取 aggrData 后，使用私钥 $\mathrm{sk}_{\mathrm{CKKS}}$ 解密数据，获得明文结果。

定义3 OSP信任证据被定义为五元组TE=(tr_1, tr_2,tr_3,tr_4,tr_5)，其中，tr_1∈{非常好用tr_1^1,比较好用tr_1^2,基本可用tr_1^3,不确定tr_1^4,不可用tr_1^5}表示OSP的可用性，即共享任务完成度，tr_2∈{非常可靠tr_2^1,比较可靠tr_2^2,基本可靠tr_2^3,不确定tr_2^4,不可靠tr_2^5}表示OSP的可靠性，即执行结果的接受度，tr_3∈{非常安全tr_3^1,遭遇攻击或泄露数据tr_3^2}表示OSP的安全性，即当前OSP是否已被恶意攻击或存在泄露数据的风险，tr_4∈{非常好tr_4^1,比较好tr_4^2,一般tr_4^3,不确定tr_4^4,差tr_4^5}表示OSP的实时性，即共享任务响应时间，tr_5∈{非常一致tr_5^1,比较一致tr_5^2,基本一致tr_5^3,不确定tr_5^4,部分不一致tr_5^5,不一致tr_5^6}表示OSP的执行行为与其承诺的预期行为一致性的符合程度。

定义4 ∀OSP_i∈Ω和tr_j∈TE，假设监管委员会评估OSP_i在tr_j上交互满意程度，则e:tr_j→l为交互满意度等级评估函数，其中l为信任等级评价结果。

定义5 假设$g(OSP_i,t)$表示监管委员会对OSP_i在t时刻的交互满意度，令

$$g\left(\mathrm{OSP}_i,t\right)=\begin{cases}<0, & f\left(\mathrm{tr}_3\right)=\mathrm{tr}_3^2\\ \sum_{j=1}^{|\mathrm{TE}|}\sum d\left(e\left(\mathrm{tr}_j\right)\right)\sigma\left(\mathrm{tr}_j\right), & \text{其他}\end{cases}\tag{9}$$

其中，$d(\cdot)$负责将$e(tr_j)$生成的满意度等级转换为数值，$\sigma(\cdot)$∈(0,1)且$\sum_{j=1}^{|\mathrm{TE}|}\sigma(\mathrm{tr}_j)=1$表示$tr_j$的权重因子，可由监管委员会依据请求方的偏好度动态分配。

定义6 假设$z(OSP_i|t_k)$表示监管委员会对OSP_i在t_k时刻的直接信任度，即对OSP_i历史交互满意度的迭代计算，令

$$z\left(\mathrm{OSP}_i\middle|t_k\right)=\begin{cases}0, & g\left(\mathrm{OSP}_i,t_k\right)<0\\ g\left(\mathrm{OSP}_i,t_k\right), & z\left(\mathrm{OSP}_i\middle|t_{k-1}\right)=\varphi\\ z\left(\mathrm{OSP}_i\middle|t_{k-1}\right)\theta\left(t_{k-1},t_k\right), & t_k-t_{k-1}\geqslant T\cap T_k>0.5\\ \delta z\left(\mathrm{OSP}_i\middle|t_{k-1}\right)+(1-\delta)g\left(\mathrm{OSP}_i,t_k\right), & \text{其他}\end{cases}\tag{10}$$

其中，t_k、t_{k-1}和T分别表示当前交互时刻、上一次信任建立且交互的时刻和信任衰减周期。当$g(OSP_i, t_k)$<0时，说明在t_k时刻OSP_i正在遭到攻击，因此它的信任度为0；当$z(OSP_i|t_{k-1})=\varphi$时，说明OSP_i刚加入共享平台，之前从未有交互记录，因此它的信任度就是当前t_k时刻的交互满意度；当$t_k-t_{k-1}\geqslant T\cap T_k>0.5$时，说明在时间衰减周期$T$内$OSP_i$未被选中过，没有交互记录，因此它的信任度既依赖于以前评估的结果，也取决于信任关系的时效性，即随着时间推移，OSP_i的历史信任度应乘以时间衰减函数$\Theta(t_k, t_{k-1})=2^{-(1-\alpha)(tk-tk-1)}$，其中$\alpha$∈(0,1)表示衰减速度的调节因子，其值越大表示信任值衰减速度越慢，反之亦然；在其他情况下，将t_{k-1}时刻的直接信任度和t_k时刻的交互满意度进行基于权重因子δ的加权求和，δ根据历史交互满意度在迭代过程中所占比重来进行取值。

4 安全性分析

本节从理论上证明Powsharing能够有效地抵抗隐私泄露、降质攻击和假冒攻击。

定理1 Powsharing可抵御OSP的窃听行为，避免隐私信息泄露。

证明 攻击者只有破解了CKKS全同态加密算法才能窃取Powsharing的隐私，因此只需证明CKKS算法无法被破解就可说明Powsharing可抵御隐私窃取攻击。为此，首先引入一些具体的参数和数学定义，然后给出环学习带误差（Ring-LWE）问题的定义，最后描述详细的安全性分析过程。

参数定义：n为多项式环$Z[x]/(x^n+1)$的维度，通常n是2的幂；q为模数，通常是个较大的质数，用于定义多项式系数的模空间；x为误差分布，通常是一个中心在0的离散高斯分布，具有标准差σ。

Ring-LWE问题：给定一个环$Z[x]/(x^n+1)$，选取一个秘密多项式$s(x)$∈$Z_q[x]/(x^n+1)$，并给出多项式$A(x)$和噪声多项式$e(x)$对$(A(x),b(x)=A(x)\cdot s(x)+e(x))$，要求在不知道$s(x)$的情况下，从$(A(x),b(x))$中恢复$s(x)$。该问题在已知$A(x)$和$b(x)$的情况下求解$s(x)$是计算上困难的。

假设存在一个攻击者A，能够在多项式时间内从CKKS密文$c(x)$中恢复出近似的明文$m(x)$。本文构建一个归约算法R，利用这个攻击者来解决Ring-LWE问题。

归约算法R的步骤如下。

1) 输入。算法R接收Ring-LWE实例$(A(x), b(x))$，其中$b(x)=A(x)\cdot s(x)+e(x)$。

2) 构造CKKS密文。设Ring-LWE实例中的$A(x)$为公钥多项式，选择一个随机的明文$m(x)$并生

成相应的密文 $c(x) = (c_0(x),c_1(x))$，其中 $c_0(x) = A(x)\cdot r(x) + m(x) + e_0(x)$，$c_1(x) = b(x)\cdot r(x) + e_1(x)$，$r(x)$、$e_0(x)$、$e_1(x)$是从相应分布中随机选择的多项式。

3)运行攻击者 A。将构造的密文 $c(x)$输入给攻击者 A，如果攻击者能够成功恢复明文 $m'(x)$，则算法 R 可以从密文中消除已知的 $r'(x)$和 $e'(x)$，进而还原 $s(x)$的信息。

4)解 Ring-LWE 问题。通过多次运行攻击者 A，算法 R 可以累积足够的信息，从而解出 Ring-LWE 问题中的秘密向量 $s(x)$。假设攻击者 A 能够以非零概率 ϵ 成功破译 CKKS 密文，即恢复明文 $m(x)$。则归约算法 R 能够通过多次交互在多项式时间内成功解出 Ring-LWE 问题中的秘密向量 $s(x)$。

证毕。

定理 2　Powsharing 在一定程度上能够抵御降质攻击，保证聚合结果的准确性。

证明　从概率论的观点来看多方聚合结果融合，所有可能聚合结果被看作样本空间 S={aggrData^1,⋯,aggrData^n}，∀aggrData^i∈S，其信任权重 w_i 被看作该样本被选中的概率。基于此，假设正确的聚合结果为 A，∀ε≥0，多方聚合结果融合策略的安全目标可形式化为

$$\left|\left(w_1\,\text{aggrData}^1 + \cdots + w_n\,\text{aggrData}^n\right) - A\right| \leqslant \varepsilon \tag{11}$$

其中，未被选中样本的概率为 0。为了提高聚合结果的准确度，若使|aggrData^i−A|越小，w_i 就应该越大；反之亦然。也就是说，可假设二者成反比例关系，即∀w_i，可得

$$w_i = \frac{k}{\left|A - \text{aggrData}^i\right|} \tag{12}$$

其中，k>0。当 aggrData^i−A>0 时，aggrData^i=$\frac{k}{w_i}$+A，将其代入式(12)，可得|m×k|⩽ε，m 表示选中样本数量；当 A−aggrData^i<0 时，aggrData^i=A−$\frac{k}{w_i}$，将其代入式(12)，可得|m×k|⩽ε。这也就意味着，只有当 k⩽$\frac{\varepsilon}{m}$时，才能满足 ε 的需求，进而可得

$$w_i = \frac{\varepsilon}{m \times \left|A - \text{aggrData}^i\right|} \tag{13}$$

当信任权重满足式(12)时，即可满足安全目标。证毕。

定理 3　Powsharing 可抵御假冒攻击，防止电力数据被 OSP 窃取。

证明　攻击者只有破解了 ECDSA 才能篡改身份，因此只需证明 ECDSA 无法被破解就可说明 Powsharing 可抵御身份篡改攻击。首先定义 ECDSA 防篡改安全属性。然后采用反证法：如果攻击者能够伪造有效的 ECDSA 签名，那么就能解决椭圆曲线离散对数问题（ECDLP, elliptic curve discrete logarithm problem），而这在计算上是不可行的。

签名参数设置：$E(F_q)$表示在有限域 F_q 上椭圆曲线 E，其中 q 是一个大素数；G 表示椭圆曲线上一个阶为 n 的基点（生成元）；n 表示基点 G 的阶，通常是大素数。

假设存在一个攻击者 A，能够在多项式时间内成功伪造出有效的 ECDSA 签名对(r,s)。构建一个归约算法 R，利用这个攻击者来解决 ECDLP 问题。

归约算法 R 的步骤如下。

1)输入。算法 R 接收 ECDLP 实例(G,Q=d·G)，其中 d 是未知的私钥，目标是计算 d。

2)伪造签名。算法 R 利用攻击者 A 提供的签名伪造能力，让攻击者对某个消息 m 伪造一个有效签名对(r_1,s_1)；设伪造的签名对为(r_1,s_1)对应消息 m_1，归约算法 R 提供相同的消息 m_1 进行第二次签名伪造，得到另一个签名对(r_2,s_2)。

3) 解离散对数问题。因为 r_1 和 r_2 是由相同 k 值生成的，所以 k 是攻击者在伪造签名过程中使用的随机数，可得

$$s_1 = k^{-1}\left(H\left(m_1\right) + dr_1\right) \bmod n \tag{14}$$

$$s_2 = k^{-1}\left(H\left(m_2\right) + dr_2\right) \bmod n \tag{15}$$

2 个方程联立可得：$k(s_1-s_2) \equiv H(m_1)-H(m_2) + d(r_1-r_2) \bmod n$。由于 $s_1 \neq s_2$，因此可以通过上述方程求解出 k，进而计算出私钥 d。假设攻击者 A 能够以非零概率 ϵ 成功伪造 ECDSA 签名对，则归约算法 R 能够通过多次运行攻击者 A，以多项式时间内非零概率成功解出 ECDLP 中的秘密私钥 d。证毕。

5　性能评估

本节首先对 Powsharing 的性能进行理论评估，然后通过搭建原型系统来证明其有效性，同时对理论分析结果进行补充，最后将其与已有方法对比，证明其先进性。

5.1　理论分析

共享系统的高效性主要体现在以下 2 个指标：

数据共享周期（DSP, data sharing period）和数据共享频率（DSF, data sharing frequency）。数据共享周期是指完成一次数据共享请求的时间间隔。数据共享频率是指单位时间内完成数据共享的最大次数。

5.1.1 *数据共享周期*

整个数据共享过程可分为电力数据获取阶段CS和结果数据上传阶段US。前者包含任务构建c_1和数据提取c_2；后者包含数据聚合u_1和聚合结果上链u_2。c_1的时间开销取决于SSC运行时间T_{SC}和任务签名生成时间$T_{\mathrm{TSIG\text{-}G}}$；$c_2$的时间开销取决于签名验证时间$T_{\mathrm{SIG\text{-}V}}$和数据加密时间$T_{\mathrm{VD\text{-}E}}$；$u_1$的时间开销取决于聚合时间$T_{\mathrm{AGG}}$；$u_2$的时间开销取决于融合时间$T_{\mathrm{MEG}}$和USC运行时间$T_{\mathrm{SC}}$。特别地，ECDSA签名生成和验证开销主要涉及椭圆曲线点乘M_G运算、模逆运算I_G、有限域上的乘法运算M_{Zp}、有限域上的加法运算A_{Zp}、有限域上的哈希运算H_{Zp}；CKKS同态加密、聚合和融合涉及多项式乘法运算M_p和多项式加法运算A_p。基于此，数据共享周期可表示为

$$\mathrm{DSP}=2T_{\mathrm{SC}}+T_{\mathrm{TSIG\text{-}G}}+2T_{\mathrm{SIG\text{-}V}}+T_{\mathrm{VD\text{-}E}}+T_{\mathrm{AGG}}+T_{\mathrm{MEG}} \tag{16}$$

其中，$T_{\mathrm{TSIG\text{-}G}}=H_{Zp}+M_G+I_G+M_{Zp}$，$T_{\mathrm{SIG\text{-}V}}=H_{Zp}+I_G+2M_{Zp}+2M_G$，$T_{\mathrm{VD\text{-}E}}=2M_p+3A_p$，$T_{\mathrm{AGG}}=3A_p+4M_G$。

5.1.2 *数据共享频率*

如上所述，每个数据共享过程可分解为4个子过程：c_1、c_2、u_1和u_2。由于区块链的强一致性只允许智能合约串行执行，因此c_1与u_2无法并行运行，而其他子过程则允许。这也意味着共享系统可以通过流水线技术来完成多个共享请求。基于此，给定n个共享请求，完成时间T_n可表示为

$$\begin{aligned}T_n=\left\lceil\frac{n}{3}\right\rceil\times\Big[&T(c_1)+\max\{T(c_2),T(c_1)\}+\\&\max\{T(u_1),T(u_2),T(c_1)\}+\\&\max\{T(u_1),T(u_2),T(c_2)\}+\\&\max\{T(u_1),T(u_2)\}\Big]\end{aligned} \tag{17}$$

那么数据共享频率为

$$\mathrm{DSF}=\frac{1}{T_n} \tag{18}$$

结合5.1.1节的具体操作开销，可知$c_2>u_1$。基于此，当$T(c_1)>T(c_2)$且$T(u_1)>T(u_2)$，可得

$$\begin{aligned}T_n=&\frac{n}{3}\times\left[3T(c_1)+T(c_2)+T(u_1)\right]=\\&\frac{n}{3}\times\Big[3T(c_1)+3H_{Z_p}+13M_G+3I_G+\\&5M_{Z_p}+2M_p+6A_p+2T_{\mathrm{SC}}\Big]\end{aligned} \tag{19}$$

当$T(c_1)>T(c_2)$且$T(u_1)<T(u_2)$，可得

$$\begin{aligned}T_n=&\frac{n}{3}\times\Big[2T(c_1)+T(c_2)+\\&\max\{T(u_2),T(c_2)\}+T(u_2)\Big]=\\&\frac{n}{3}\times\Big[2T(c_1)+2T_{SC}+3H_{Z_p}+\\&13M_G+3I_G+5M_{Z_p}+2M_p+6A_p+\\&\max\{T(u_2),T(c_2)\}+T(u_2)\Big]\end{aligned} \tag{20}$$

当$T(c_1)<T(c_2)$且$T(u_1)>T(u_2)$，可得

$$\begin{aligned}T_n=&\frac{n}{3}\times\left[2T(c_1)+2T(c_2)+T(u_1)\right]=\\&\frac{n}{3}\times\Big[2T(c_1)+2T_{SC}+6H_{Z_p}+\\&26M_G+6I_G+10M_{Z_p}+9M_p+15A_p\Big]\end{aligned} \tag{21}$$

当$T(c_1)<T(c_2)$且$T(u_1)<T(u_2)$，可得

$$\begin{aligned}T_n=&\frac{n}{3}\times\Big[T(c_1)+T(c_2)+\max\{T(u_2),T(c_2)\}+\\&\max\{T(u_2),T(c_2)\}+T(u_2)\Big]=\\&\frac{n}{3}\times\Big[T(c_1)+3H_{Z_p}+13M_G+3I_G+5M_{Z_p}+2M_p+\\&6A_p+\max\{T(u_2),T(c_2)\}+T(u_2)\Big]\end{aligned} \tag{22}$$

5.2 系统实现

为了证明所提方法的有效性，本文实现了一个Powsharing的原型系统，其开发框架如图6所示。借鉴当前流行的JavaWeb开发框架，该系统由下至上可划分为4层：数据采集层I、存储控制层II、业务处理层III和应用展示层IV。第I层负责智能合约和电力源数据的收集任务，前者采用基于EVM的Solidity语言进行编写，后者使用HTTP接口直接与数据提供方进行通信。除了用户注册信息，第II层还负责存储智能合约和聚合结果等信息，其中用户注册信息存储在MySQL关系数据库中，智能合约和聚合结果等信息存储在FISCO BCOS平台搭建的区块链中。聚合结果由预言机来负责获取、计算并上传到区块链上。具体来说，监听预言机通过FISCO BCOS平台提供的JAVA SDK来实现区块链

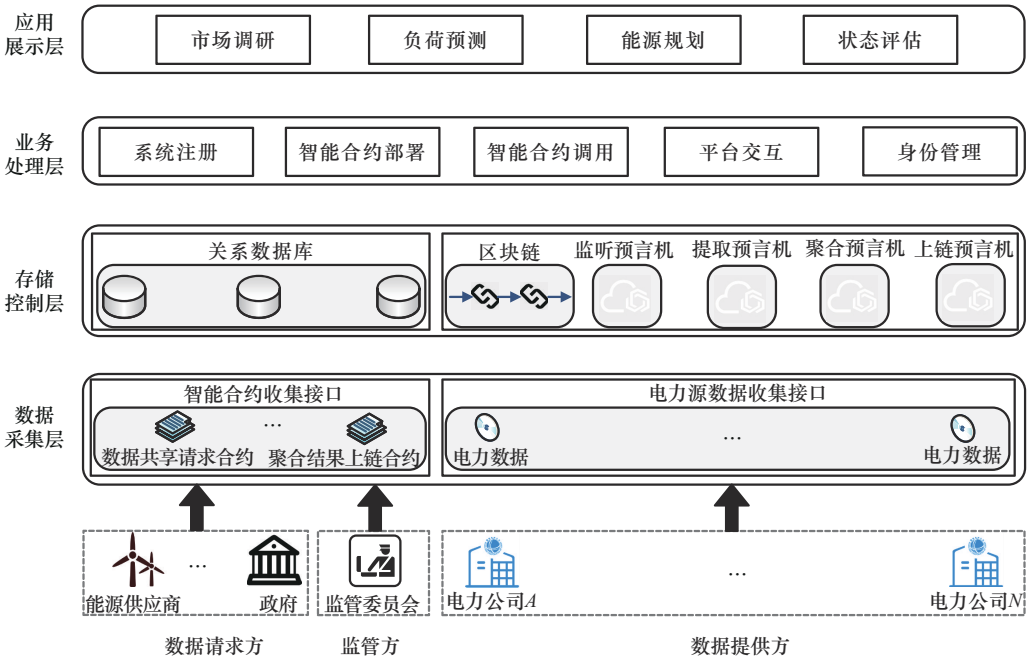

图 6　Powsharing 原型系统的开发框架

Eventlog 的监听功能以及通过 Kafka 消息队列技术来实现任务发布。具体过程如下：注册——配置证书、编译合约 ABI 文件、依次配置与部署 SSC、LSC 和 USC；解析——根据 ABI 文件对订阅的区块链合约生成的 Eventlog 进行解析，生成任务并将其加入任务消息列表。为了接收不同数据提供方异步发送的源数据，提取预言机通过 Redis 来缓存它们，而聚合预言机只有在获得所有源数据后才执行聚合任务。上链预言机调用 oracleCallback 函数，通过 JAVA SDK 外部调用方式将数据发送给链上回调合约。第 III 层是用户与区块链沟通的媒介，主要包括调用智能合约和身份管理等模块，通过 SpringBoot 开发框架和 MyBatis-Plus 持久层框架与存储控制层建立通信来实现。第 IV 层是电力数据共享的最终目的与价值体现——应用，通过 Vue.js 前端框架和 Element UI 组件库来实现，同时采用 Axios 完成前后端通信。

该原型系统可为市场调研、负荷预测、能源规划、状态评估等应用程序提供电力数据获取服务。系统功能分为身份管理模块、数据共享模块以及系统状态模块。身份管理模块包括数据请求方身份管理、监管委员会身份管理、数据提供方身份管理和预言机服务提供商身份管理，其中数据请求方身份管理包括上传和部署 SSC；监管委员会身份管理包括上传和部署 USC；数据提供方身份管理包括设置被允许访问的请求方 ID；预言机服务提供商身份管理包括设置服务费用及描述其服务能力等。数据共享模块负责在共享请求时选定调用的智能合约和展示历史共享请求返回的聚合结果。系统状态模块负责展示当前任务情况等。

5.3　实验分析

第 5.1 节对 Powsharing 方法的性能进行了理论分析，指出了影响性能的主要参数，包括智能合约运行时间 T_{SC}、数据加密时间 $T_{VD\text{-}E}$ 及聚合时间 T_{AGG}，而本节则重点评估它们在原型系统中的真实变化情况。此外，第 4 节已经证明聚合结果可靠性取决于信任权重的设置是否准确，而这又依赖于交互满意度评估策略，因此本节重点对其性能进行实验分析。用于搭建 Powsharing 原型系统的实验机器参数为 Windows 11 23H2、Intel i7-10870H (2.2 GHz)和 16 GB RAM。本文实验中涉及的测试数据集参考典型电力数据格式（如电压、电流、功率、用电量等），通过程序随机生成具有相似统计特征的模拟数据。需要说明的是，本文方案虽然聚焦于电力数据共享场景，但对其他以数值型数据为主的应用领域具有较好的通用性，而对于非数值型的共享场景，由于无法进行有效的数据聚合操作，其通用性相对有限。

鉴于影响智能合约运行时间 T_{SC} 的主要因素是数据共享平台中区块链的共识周期，第一组实验测试了不同共识算法和不同共享平台成员规模下共识

周期的变化情况，实验结果如图7所示。一方面，在相同成员规模下，RAFT的共识周期显著高于PBFT。另一方面，随着共享平台成员规模的增加，PBFT共识周期呈指数级增长，当规模小于30时，PBFT共识周期约为250 ms；当规模大于50时，共识周期增加到670 ms。

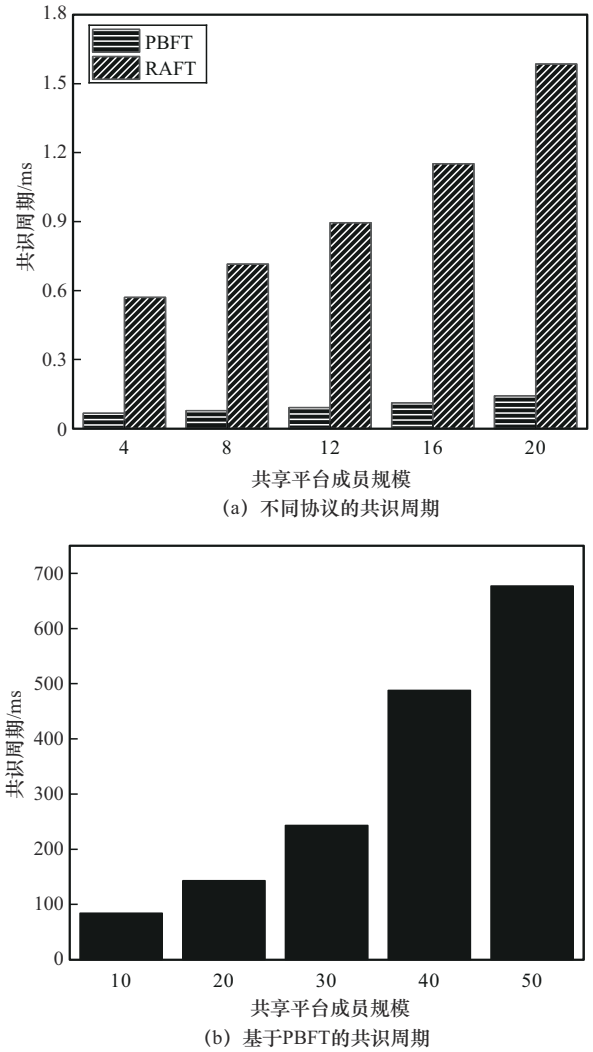

图7　不同成员规模下共识周期的变化情况

鉴于数据加密时间$T_{\text{VD-E}}$取决于本文采用基于CKKS的电力数据加密策略，第二组实验用于说明随着共享数据数量的增多加密时间的变化情况。此外，为了证明其高效性，本实验还与2种常见同态加密技术（BFV和BGV）进行了比较，结果如图8所示。相比于其他方法，本文方法的整体性能明显占优。具体来说，当数据量达到325 KB时，时间开销仅为23 ms。此外，CKKS方案无须额外优化，可直接支持电网常见的浮点数运算。

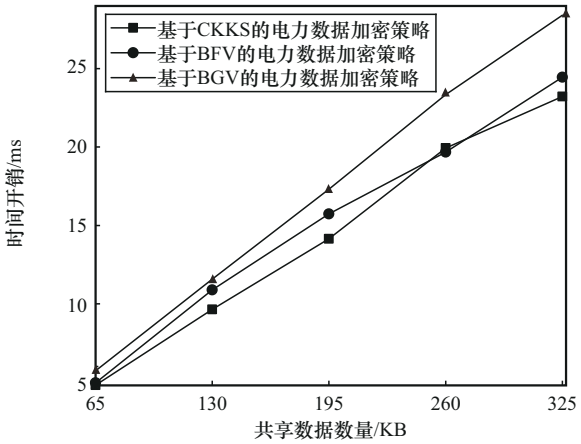

图8　不同共享数据规模下加密时间的变化情况

鉴于数据聚合时间T_{AGG}也取决于基于CKKS的电力数据加密策略及常见的电网数据聚合操作（包括加法、均值、方差和协方差运算），第三组实验用于说明随着数据提供方的增多不同数据聚合时间的变化情况。与第二组实验相似，本实验也与BFV和BGV进行比较，具体结果如图9所示。由图9可知，无论哪种聚合操作，本文方法都明显占优；随着运算复杂度的增加，时间开销也在明显地增大。就方差聚合来说，通常至少需要60 ms。

交互满意度评估旨在验证基于信任证据的OSP选择策略能否有效提升数据共享服务质量。满意度指标反映了用户对OSP服务响应时间、数据准确性和可靠性的综合评价。鉴于交互满意度评估策略以OSP信任证据为基础，本文参考了chainlink的预言机数量（约为1 000个节点），然而考虑到chainlink的预言机为大多数公有链及各行业Dapp提供服务，本文方案的OSP聚焦于电力数据共享场景，本文认为OSP数量在百级时的性能可以代表大规模下的真实性能，故第四组实验模拟了120个性能不同的OSP，共执行60次请求服务。每次请求随机选择多个OSP执行任务且在一个时间片后及时更新OSP信任度。为了证明评估策略的高效性，本实验还设计了一种随机的交互满意度评估策略，二者比较结果如图10所示。实验结果表明：前者通过动态更新OSP信任度，能够筛选出高质量的服务提供商，使满意度稳定在65~75的较高水平；随机选择策略由于无法区分OSP性能差异，满意度始终维持在45~60的较低水平。这证明了信任机制在提升数据共享服务质量方面的有效性。

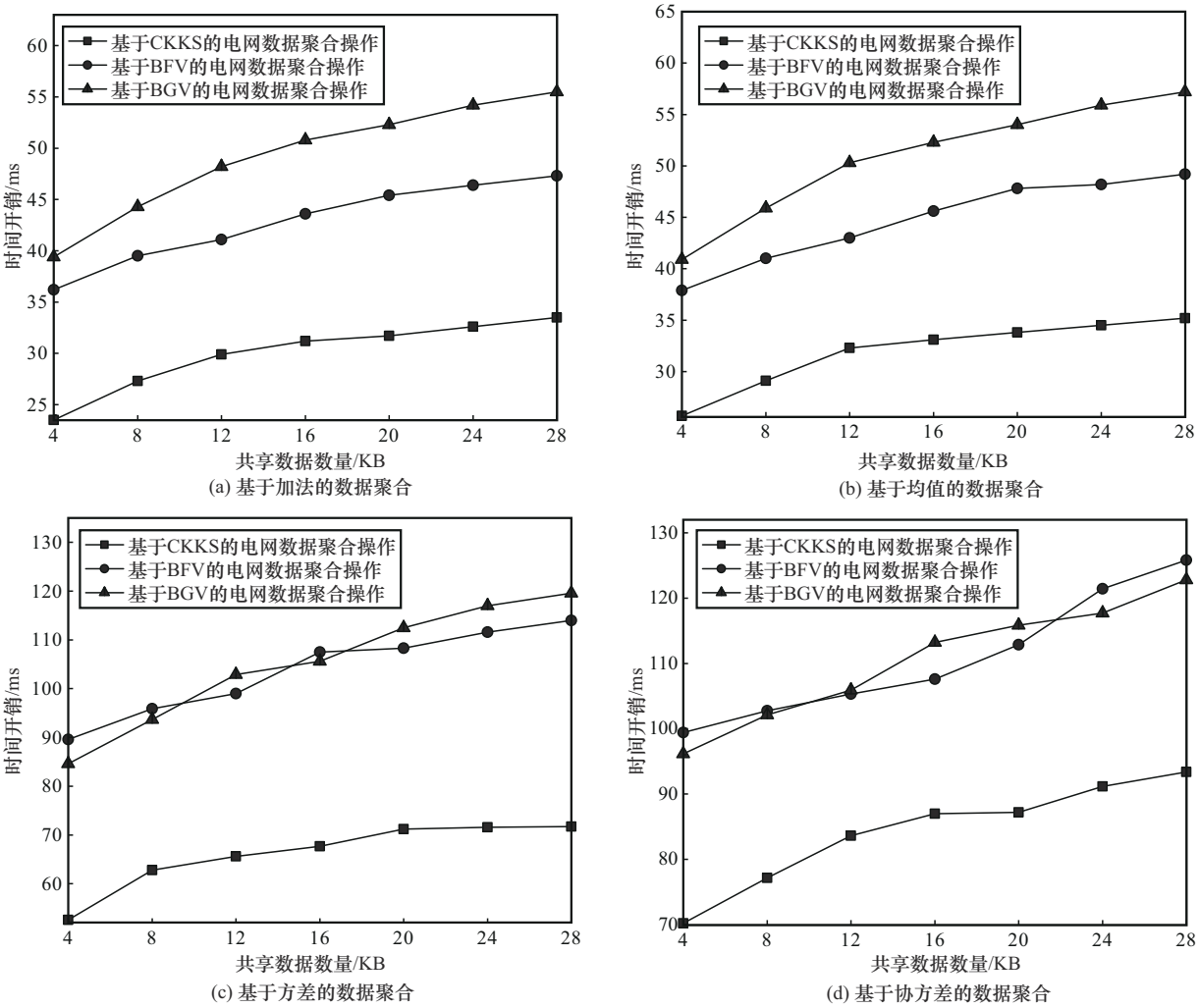

图9　不同数据提供商数量下聚合时间的变化情况

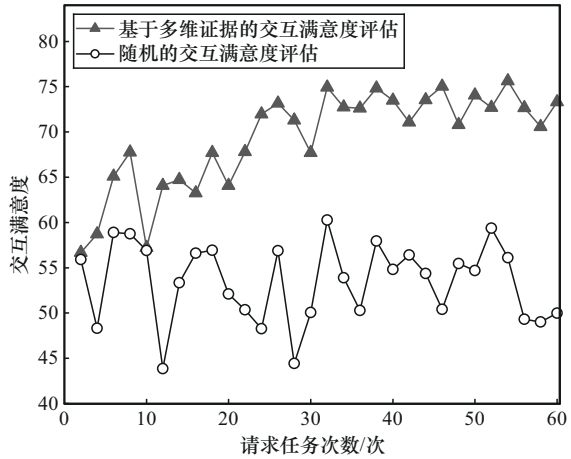

图10　不同评估策略下满意度随请求任务次数的变化情况

第五组实验结合实际电力场景的需求，测试了本文方案在不同数据规模、请求频率（包括高频率大规模数据请求、低频率大规模数据请求、高频率小规模数据请求、低频率小规模数据请求以及大小规模混合的数据请求）下的性能，以验证本文方案在不同电力场景下的适应性。适应性评估旨在验证方案在实际电力系统多样化应用场景下的性能表现，体现了方案的功能可扩展性。测试结果如图11所示。随着共享频率增高，各场景下数据共享的时间开销呈线性增长趋势，在高容量数据共享场景下，每分钟能够处理大约500次数据共享任务；在低容量数据共享场景下，每分钟能够处理大约12 000次数据共享任务；在复杂混合容量数据共享场景下，每分钟能够处理大约1 000次数据共享任务。实验结果表明，本文方案在低容量和复杂混合容量场景下均展现出良好的性能表现。鉴于高容量场景（如历史电力数据分析）通常对处理频率要求较低，本文方案的处理能力能够有效满足此类需求。因此，本文方案通过灵活调节处理能力以适应不同应用需求，在实际电力系统中展现出较强的适应性。

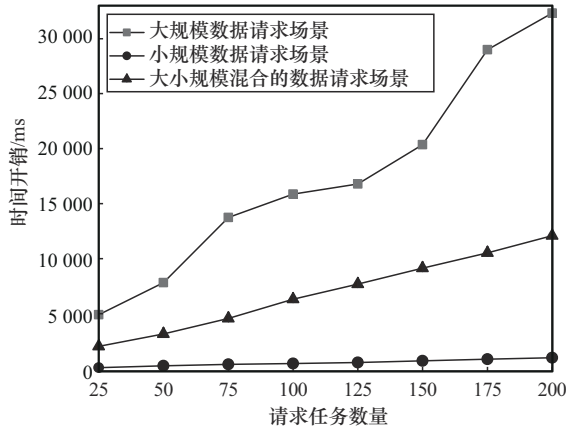

图 11　不同场景下本文方案的共享频率的变化情况

5.4　方法比较

为了体现基于垂直切分的分布式预言机数据共享方法 Powsharing 的优越性，本节将其与经典的区块链直接数据共享 Blksharing[10]、集中式预言机数据共享 Consharing[18]、基于水平切分的分布式预言机数据共享 Hrzsharing[20]、基于 SGX 的数据共享[19]以及基于 MPC[22]的数据共享进行性能比较。此外，为了能够获得更全面的结果，实验被设计为 2 组：单任务下共享时间开销对比和多任务下共享时间开销对比。

第一组实验用于说明随着共享数据数量的增多，不同方法的时间开销变化情况，结果如图 12 所示。从图 12 中不难看出：Powsharing 与 MPCsharing 的性能差别不大；Hrzsharing 性能优于 PowSharing 和 MPCsharing，但其性能不够稳定；Blksharing 必须先将所有源数据上链后才能完成分享，因此消耗时间最多；Consharing 无须中间处理过程，因此所需时间较少，但存在单点故障问题；SGXsharing 在聚合运算时可以在安全区中将密文解密后，通过明文聚合再将聚合结果加密，聚合时间大大降低，因此所需时间最少，但成本相对较高。

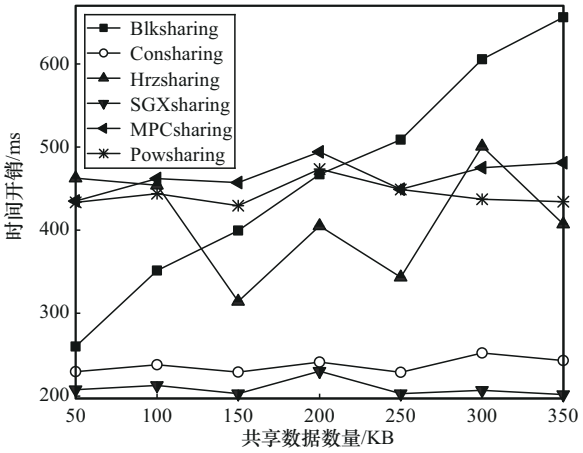

图 12　不同共享数据量下聚合时间的变化情况

第二组实验分别进行了均值聚合任务和方差聚合任务的对比，用于说明随着共享任务数量增多不同方法的时间开销变化情况，结果如图 13 所示。从图 13 中不难看出，随着任务数量增多，所有方法的时间开销都在增大。因为均值聚合较为简单，所以比较方案的性能相差不大。在执行复杂的方差聚合任务时，Powsharing 可采用流水线工作方式，因此时间开销整体较小，相较于 Consharing 和 Hrzsharing，效率至少提升 15%；BlkSharing 需要大量数据上链，因此时间问题非常严重；MPCsharing 需要将数据的多个份额分别上链，链上时间开销较大，故共享频率相对较低；SGXsharing 通过明文聚合方式缩短了聚合时间，且不存在单点故障问题，因此时间开销最小，但需要额外的硬件支持，成本

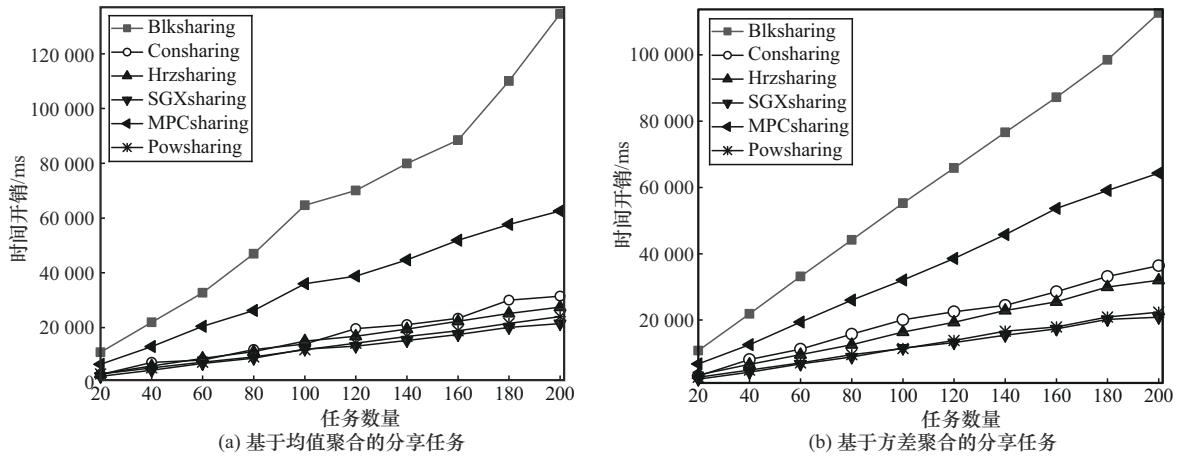

图 13　不同共享任务数量下聚合时间的变化情况

较高，以阿里云 8 核 CPU、32 GB 云服务器为例，支持 Intel SGX 的安全增强通用型云服务器比普通云服务器的月租金高约 200 元人民币。

综上所述，Powsharing 在不同实验设置下均展现出优异且稳定的性能，具备良好的性能可扩展性。同时，其无须依赖高成本硬件，更易在实际环境中部署使用。

6　案例讨论

为验证 Powsharing 在实际应用中的可行性与优势，本文以一个典型的电力数据共享场景为例，展示平台的整体部署架构及其在真实环境下的数据获取流程，并对比传统云存储方案，说明本平台在数据安全性、可追溯性和自动化程度方面的优点。

如图 14 所示，基于 Powsharing 的电力数据共享平台共分为 4 层：采集层、数据层、平台层和应用层。采集层负责从实际电力用户侧采集电量数据，覆盖高压用户和低压用户，分别通过采集终端和集中器连接至大用户电表和居民电表，实现数据的定时或召测采集。数据层是平台的数据源，主要接入国家电网部署的新一代用电信息采集系统。通过前置服务器、主站服务器和接口服务器形成数据汇聚通路，确保不同区域数据的可获取性和统一管理。平台层是核心的数据共享与处理模块，包括电力数据共享区块链、预言机服务提供商、上链预言机、聚合预言机等组件。该层实现数据请求任务的解析、处理、聚合和上链，确保数据处理过程的可信与透明。应用层为最终数据消费者提供服务支持，包括 GDP 估算、电力市场交易、能源预测规划和社会事件治理等多种应用场景。

以某能源供应商 *D* 为例，其希望获取 2025 年 1 月 1 日至当前时间内，秦皇岛市电力公司 *A* 与唐山市电力公司 *B* 所管辖区域的分钟级用电量数据（如商业用电、居民用电、工业用电等），以支持发电厂选址及容量规划的科学决策。数据共享过程如下所述。

1)请求发布：*D* 向区块链提交数据请求。

2)任务生成与分发：预言机服务提供商的监听预言机监听到请求后，生成任务并通过接口服务器向 *A* 与 *B* 的数据服务端发送数据调用请求。

3)数据调度：接口服务器将任务解析后转发至新一代用电信息采集系统的主站服务器，由主站服务器生成数据召测任务。任务经前置服务器向 *A* 与 *B* 所有低压与高压采集终端发送数据召测请求，采

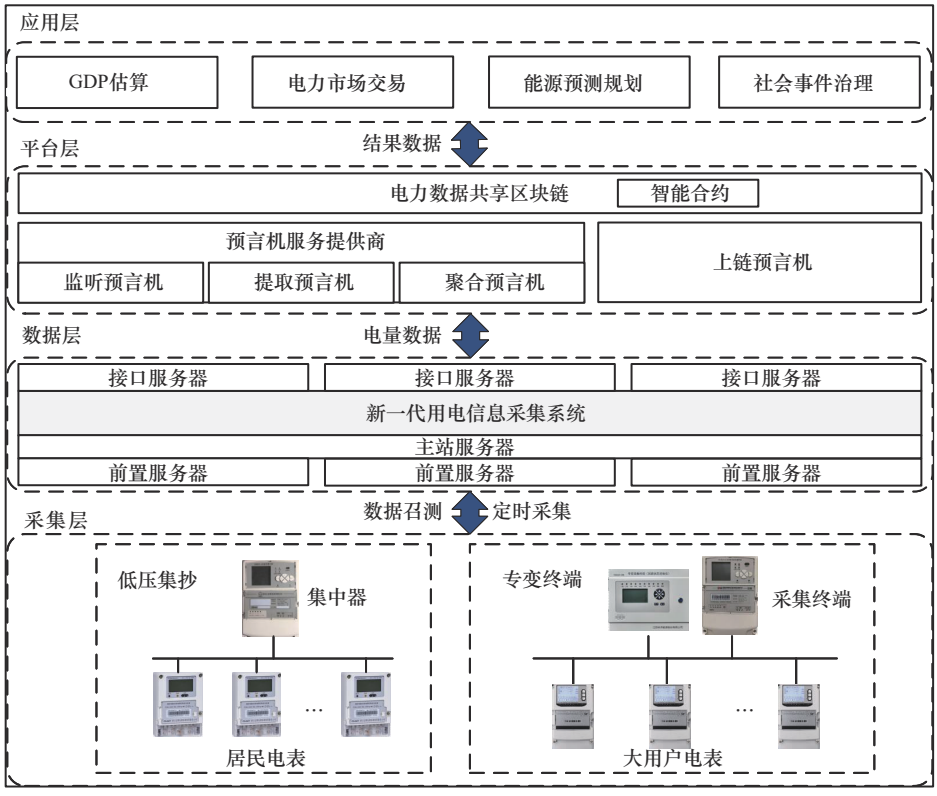

图 14　基于 Powsharing 的电力数据共享平台架构

集当前所有智能电表的表号及其对应正向有功总电量Fd_A和Fd_B。采集层的集中器获取此时所有电表的正向有功总电量，经前置服务器返回给主站服务器。主站服务器清除电量数据的异常值后，计算此次召测任务中所有智能电表的正向有功总电量差值，并将数据传递给提取预言机。

4)数据聚合：由聚合预言机计算A与B各自总用电量T_A和T_B，求和得出T_t，并发送给上链预言机进行数据融合。

5) 融合与上链：上链预言机将多个预言机服务提供商提供的T_t融合后上传至区块链。

6) 结果获取：D通过区块链获取请求结果，完成数据共享闭环。

当请求时间范围为历史日级数据时，由于主站服务器已定时采集并存储相应数据，因此数据层无须向采集层下发召测任务，而是直接从数据库中提取冻结数据，提升响应效率。

相较于传统基于云存储的数据共享模式，基于Powsharing的电力数据共享平台具有如下优点。

1) 共享过程可溯源。借助区块链的公开性与不可篡改性，平台能够实现电力数据从请求生成到结果反馈的共享过程溯源，有助于厘清数据所有权，维护数据提供方的权益。

2) 可靠数据处理：分布式预言机能够满足数据请求方对数据处理的需求，同时保证处理结果的可靠性。此外，提供服务的预言机在链上留痕，可用于事后审核与责任追踪。

3) 跨域协同：通过平台统一的数据请求接口与调度机制，打破区域电力数据壁垒，实现多城市、多系统数据的有效互通。

4) 隐私保护：平台仅返回结果数据而非原始信息，同时结合同态加密等密码技术，有效减少数据泄露风险，满足用户数据隐私需求。

7 结束语

本文设计了一种基于区块链预言机的安全高效电力数据共享平台。它具备以下特征：采用基于多区块链预言机协作的共享平台系统模型，提高可扩展性；采用安全的电力数据共享协议，保护数据隐私的同时提高聚合结果可靠性。与已有方案相比，本文方案在保证安全性的同时，共享效率至少提高了15%。

参考文献：

[1] XIA X F, XIAO Y, LIANG W, et al. Detection methods in smart meters for electricity thefts: a survey[J]. Proceedings of the IEEE, 2022, 110(2): 273-319.

[2] MITRA S, CHAKRABORTY B, MITRA P. Smart meter data analytics applications for secure, reliable and robust grid system: survey and future directions[J]. Energy, 2024, 289: 129920.

[3] SUN J F, XU G W, ZHANG T W, et al. Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(7): 7527-7540.

[4] DENG H, QIN Z, WU Q H, et al. Achieving fine-grained data sharing for hierarchical organizations in clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(2): 1364-1377.

[5] SUN J F, XU G W, ZHANG T W, et al. Share your data carefree: an efficient, scalable and privacy-preserving data sharing service in cloud computing[J]. IEEE Transactions on Cloud Computing, 2023, 11(1): 822-838.

[6] FUGKEAW S. Secure data sharing with efficient key update for industrial cloud-based access control[J]. IEEE Transactions on Services Computing, 2023, 16(1): 575-587.

[7] GE C P, SUSILO W, BAEK J, et al. A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 2907-2919.

[8] XU Y L, CHENG H, LIU X M, et al. PCSE: privacy-preserving collaborative searchable encryption for group data sharing in cloud computing[J]. IEEE Transactions on Mobile Computing, 2025, 24(5): 4558-4572.

[9] WANG H, WANG J, GE C P, et al. ADSS: an available-but-invisible data service scheme for fine-grained usage control[J]. IEEE Transactions on Services Computing, 2025, 18(1): 43-56.

[10] HU C C, LI C, ZHANG G G, et al. CrowdMed-II: a blockchain-based framework for efficient consent management in health data sharing[J]. World Wide Web, 2022, 25(3): 1489-1515.

[11] HUANG J Q, KONG L H, WANG J W, et al. Secure data sharing over vehicular networks based on multi-sharding blockchain[J]. ACM Transactions on Sensor Networks, 2024, 20(2): 1-23.

[12] HASSIJA V, CHAMOLA V, GARG S, et al. A blockchain-based framework for lightweight data sharing and energy trading in V2G network[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5799-5812.

[13] GARCIA P S R, KLEINSCHMIDT J H. Sharing health and wellness data with blockchain and smart contracts[J]. IEEE Latin America Transactions, 2020, 18(06): 1026-1033.

[14] TAN L, YU K P, SHI N, et al. Towards secure and privacy-preserving data sharing for COVID-19 medical records: a blockchain-empowered approach[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(1): 271-281.

[15] ZHANG L, OU Z R, HU C H, et al. Data sharing in the metaverse with key abuse resistance based on decentralized CP-ABE[J]. IEEE Transactions on Computers, 2025, 74(3): 901-914.

[16] 施建锋, 吴恒, 高赫然, 等. 区块链智能合约交易并行执行模型综述[J]. 软件学报, 2022, 33(11): 4084-4106.
SHI J F, WU H, GAO H R, et al. Overview on parallel execution models of smart contract transactions in blockchains[J]. Journal of Soft-

ware, 2022, 33(11): 4084-4106.
[17] HASSAN A, MAKHDOOM I, IQBAL W, et al. From trust to truth: Advancements in mitigating the Blockchain Oracle problem[J]. Journal of Network and Computer Applications, 2023, 217: 103672.
[18] SHI P C, WANG H M, YANG S Z, et al. Blockchain-based trusted data sharing among trusted stakeholders in IoT[J]. Software: Practice and Experience, 2021, 51(10): 2051-2064.
[19] WOO S, SONG J, PARK S. A distributed oracle using intel SGX for blockchain-based IoT applications[J]. Sensors, 2020, 20(9): 2725.
[20] LIN Y J, GAO Z P, SHI W S, et al. A novel architecture combining oracle with decentralized learning for IIoT[J]. IEEE Internet of Things Journal, 2023, 10(5): 3774-3785.
[21] PASDAR A, LEE Y C, RYAN P, et al. A blockchain oracle-based API service for verifying livestock DNA fingerprinting[C]//International Conference on Service-Oriented Computing. Berlin: Springer, 2023: 80-91.
[22] MANOJ T, MAKKITHAYA K, NARENDRA V G. A trusted IoT data sharing and secure oracle based access for agricultural production risk management[J]. Computers and Electronics in Agriculture, 2023, 204: 107544.
[23] ZHANG C, ZHU L H, XU C, et al. PRVB: achieving privacy-preserving and reliable vehicular crowdsensing via blockchain oracle[J]. IEEE Transactions on Vehicular Technology, 2021, 70(1): 831-843.
[24] WANG J X, GAO F, ZHOU Y Z, et al. Data sharing in energy systems[J]. Advances in Applied Energy, 2023, 10: 100132.
[25] ABDULLAH S, ARSHAD J, KHAN M M, et al. PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle[J]. Complex & Intelligent Systems, 2023, 9(3): 3023-3041.
[26] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Advances in Cryptology — EUROCRYPT'99. Berlin: Springer, 2007: 223-238.
[27] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.
[28] CHEN L, LU R, CAO Z, et al. MuDA: multifunctional data aggregation in privacy-preserving smart grid communications[J]. Peer-to-Peer Networking and Applications, 2015, 8: 777-792.
[29] LI X L, WENG C K, XU Y X, et al. ZKSQL: verifiable and efficient query evaluation with zero-knowledge proofs[J]. Proceedings of the VLDB Endowment, 2023, 16(8): 1804-1816.
[30] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
[31] DUCAS L, DURMUS A, LEPOINT T, et al. Lattice signatures and bimodal Gaussians[C]// Advances in Cryptology – CRYPTO 2013. Berlin: Springer, 2013: 40-56.
[32] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.

[作者简介]

鲁宁（1984– ），男，内蒙古包头人，博士，东北大学教授、博士生导师，主要研究方向为网络安全。

陈芳玉（1998– ），男，辽宁抚顺人，东北大学硕士生，主要研究方向为区块链、数据共享等。

刘增辉（1998– ），男，山东淄博人，东北大学博士生，主要研究方向为区块链、数据共享等。

王庆豪（1995– ），男，江苏盐城人，东北大学博士生，主要研究方向为区块链、隐私计算等。

史闻博（1980– ），男，河北唐山人，博士，东北大学教授、博士生导师，主要研究方向为信息安全。

马建峰（1963– ），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为应用密码学等。