计算机科学
COMPUTER SCIENCE

数据交易模式对比与交易难点分析

崔金甲, 曾琛, 王璐, 彭晓晖

引用本文

崔金甲, 曾琛, 王璐, 彭晓晖. 数据交易模式对比与交易难点分析[J]. 计算机科学, 2026, 53(4): 121-133.

CUI Jinjia, ZENG Chen, WANG Lu, PENG Xiaohui. Analysis of Data Trading Models and Transaction Challenges [J]. Computer Science, 2026, 53(4): 121-133.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250900002

数据交易模式对比与交易难点分析

崔金甲[1]　曾　琛[1]　王　璐[2]　彭晓晖[1]
1 中国科学院计算技术研究所　北京 100190
2 中国人民解放军 91977 部队　北京 100036
(mundotsui@qq.com)

摘　要　在数字化加速的趋势下,数据要素成为各行业的核心资源,推动了市场的不断发展。然而,目前的数据交易市场发展并不完善,其原因主要有两点:一是个人用户的行为数据交易门槛过高;二是企业间数据交易的合规审查机制不健全,数据交易规则尚未完善,市场活力受到制约。数据交易困难的根本原因在于数据本身区别于传统意义上“一手交钱一手交货”的商品,存在定价难、确权难、质量保证难、交易非否认难和保障数据主权难的问题。对此,搜集整理了现有较为完善的数据交易框架,从交易模式的视角对现有框架进行分类对比;针对上述 5 个难点,详细介绍了现有文献的解决方案;针对现有数据交易市场的发展情况,提出了对未来发展的建议。

关键词:数据交易难点;数据确权;数据定价;数据主权;数据质量保证;数据交易非否认
中图分类号　TP399

Analysis of Data Trading Models and Transaction Challenges

CUI Jinjia[1],ZENG Chen[1],WANG Lu[2] and PENG Xiaohui[1]
1 Institute of Computing Technology,Chinese Academy of Sciences,Beijing 100190,China
2 Troops 91977 PLA,Beijing 100036,China

Abstract　With the acceleration of digitalization,data have become a core resource across industries,driving continuous market growth. However,the current data trading market remains underdeveloped,mainly due to two reasons. Firstly,the high barriers for individuals to trade behavioral data. Secondly,the lack of sound compliance review mechanisms for inter-enterprise data transactions,with incomplete trading rules that restrict market vitality. The fundamental difficulties in data trading lie in the unique characteristics of data,which differ from traditional “cash-and-carry” goods,leading to challenges in pricing,data rights confirmation,data quality assurance,non-repudiation of transactions,and the safeguarding of data sovereignty. This paper collects and organizes relatively mature data trading frameworks,classifies and compares them from the perspective of trading models,and provides a detailed introduction to the solutions proposed in the literature for the five major challenges mentioned above. Finally,in light of the current development of the data trading market,this study puts forward suggestions for future development.

Keywords　Challenges in data trading,Data rights confirmation,Data pricing,Data sovereignty,Data quality assurance,Non-repudiation in data trading

1　引言

根据全国数据资源统计调查工作组发布的《全国数据资源调查报告》[1],2024 年全国年度数据生产总量为 41.06 ZB,人均年度数据生产量约为 31.31TB。数据要素市场正经历快速增长阶段,其规模扩张速度远超传统生产要素市场。这一现象不仅源于技术迭代,更得益于各地区的政策推动,例如欧盟《数据治理法案》(*Data Governance Act*)[2]和我国“数据二十条”[3]均明确将数据列为生产要素,并通过立法确立其权属框架。与此同时,我国加速布局算力基础设施,推动数据资源开发利用,进一步激活数据要素市场。数字化转型背景下,数据要素已成为各行业的核心资源,驱动着市场持续扩张。云计算、大数据分析和人工智能技术的崛起也为数据要素市场提供了强大的技术支持。以生物与医学领域为例,可穿戴设备采集的健康数据能够帮助医生追踪患者生命体征的动态变化。通过跨行业数据流通,医生可整合患者的病史、遗传背景

到稿日期:2025-09-01　返修日期:2025-12-04
基金项目:国家自然科学基金(62072434,U23B2004)
This work was supported by the National Natural Science Foundation of China(62072434,U23B2004).
通信作者:曾琛(zengchen@ict.ac.cn)

与药物反应等信息，结合大数据技术为患者制定个性化医疗方案，实现精准医疗并降低药物副作用。同时，生物学数据能帮助医药研究者深入了解药物作用机理，加速新药研发进程；临床实验数据的共享能够助力科研人员评估药物的安全性与有效性，缩短药物研发周期。

欧盟实施的《通用数据保护条例》(*General Data Protection Regulation*，GDPR)[4]明确了个人数据的“可携带权”，我国《个人信息保护法》也明确赋予了个人主动流转其数据的权利，这些法案为个人数据交易和企业数据的合规流通提供了法律依据。在法律允许的范围内，企业在取得用户同意后可以合法地商用用户数据，并支付用户相应的报酬，实现数据价值的流通。尽管数据要素价值显著，但数据要素市场化配置水平仍待提升[5]。

1)个人用户的行为数据交易门槛过高。现有的数据交易多以企业打包售卖数据集或数据访问接口为主，个人缺乏一个完善的、准入门槛低的数据交易平台以出售其私人行为数据，大量用户数据滞留于用户设备本地，形成数据孤岛，数据要素无法充分发挥其经济价值。BAT，GAFAM 等头部企业常以“改进用户体验”的名义将用户数据传输至云端，无偿使用用户的行为数据，以实现商业目的。这些企业往往不向用户提供完整的数据导出功能，限制用户对自身数据的访问和迁移能力，最终导致普通用户既无法从数据流通中获益，也难以在不同平台间迁移数据，形成显著的数据锁定效应。这也解释了为何现有的数据交易平台[6-7]多以企业间 B2B 数据流通为主。

2)企业间数据交易的合规审查机制不健全，数据交易规则尚未完善，市场活力受到制约。企业在数据交易前很难确认用户行为数据的所有权归属，数据涉及个人隐私或商业敏感信息，缺乏统一的脱敏、匿名化标准。除此之外，不同行业与地区的法律规范不一，导致企业难以把握合规边界，面临“合规成本过高”和“违规风险过大”的难题，进而发展成“不敢共享、不愿共享”的现象[8]。

数据交易困难的根本原因在于数据本身区别于传统意义上“一手交钱一手交货”的商品，具体表现如下。

1)数据复制的边际成本近乎为零，这是数据交易确权难与交易非否认难的核心原因之一。与实体商品复制需额外投入原材料、人力等成本不同，数据复制仅需依托存储与网络资源，增量成本可忽略不计；此外，硬盘读写、网络传输速度的提升及云存储的普及，使得一份数据能被快速复制到全球各地，因此极易被盗版复制与未授权访问。这使得数据买方获取数据后，可轻易删除交易记录、私下留存副本，甚至违规转售后否认接收或使用过数据；而复制副本与原始数据完全一致，缺乏物理标识，数据卖方难以追溯复制轨迹、固定关联证据，最终加剧了非否认困境。

2)数据难以通过部分样例进行“验货”，因为发挥价值的往往是数据整体而不是数据个例。有的数据买家期望能够从大量的长期数据中获得洞察，而有的数据买家则对数据的时效性有额外的要求，更看重数据的实时性。因此，数据价值的衡量不应局限于数据量的大小，这样会导致难以对数据进行合理定价。

3)数据并不像实体商品一样能够被买断，一些隐私信息即便在被合法售卖后也应当受到监管，其中包括数据使用主体、方式、范围和用途等，即保障数据持有者的数据主权(Data Sovereignty)。数据主权指数据持有者在数据交易后对数据使用方式、使用范围的持续掌控权，即数据流通过程中的可追踪性与授权边界控制能力[4]。

综上所述，数据交易存在定价难、确权难、质量保证难、交易非否认难和保障数据主权难的问题。现有的数据定价方案根据待交易数据的类型分为按贡献定价、基于隐私牺牲定价、招标和拍卖等方式；数据确权方案多基于数据相似性检测的方法，也有方案要求数据卖家自证其对数据的所有权；数据质量保证则通过评价机制或数据中介来辅助买卖双方的交易匹配；交易非否认多通过密码学与区块链不可篡改的特性实现，也有部分方案选择基于硬件实现原子交换协议完成数据交付；保障数据主权方面，现有方案通过加密技术、可验证协议和记录操作日志等方式监督交易后的数据使用情况。本文将在第 4 章详细阐述这些交易难点现有的解决方案。

本文的工作总结如下：

1)分析了数据作为商品的特征，明确了数据主权与数据确权的概念，并介绍了构建数据交易市场所需的关键技术。

2)调研了现有的数据交易市场和较为完善的数据交易框架，将数据交易模式归类为数据集交易、数据处理即服务和众包交易，结合常见的交易依托(区块链、中介、可信执行环境)对数据交易框架进行了对比，阐述每种方案的优劣。

3)根据对数据交易框架调研的结果，将数据交易难点归结为 5 点：定价难、确权难、质量保证难、交易非否认难和保障数据主权难。针对每个难点，讨论了现有文献中的解决方案，旨在为完善数据交易市场提供参考。

4)从“数据流通的标准化与基础设施的建立”“重视数据的差异化与交易方法的实用性”和“把握 Web 3.0 机遇”3 个方面，对未来数据交易市场的发展提出建议。

2 背景知识与相关技术

2.1 数据作为商品的特征

1)数据复制的边际成本近乎为零[9]。随着工业技术的发展，硬盘、服务器等存储介质也变得不再昂贵，数据复制成本几乎可忽略不计。现代分布式存储架构与云计算服务也使数据副本的创建与分发成本趋近于零。数字水印技术虽然能够声明版权，但并不能从根源上杜绝侵权行为的发生。传统的数据加密技术也只是防止数据被未授权地访问，随着交易的进行，数据最终还是要暴露给买方。

2)数据价值的衡量不应局限于数据量的大小[10]。数据定价应遵循价值导向原则(Value-based Pricing)，其核心参数包括信息熵(数据中有效信息的密度)和场景适配度等。定价

模型应该更注重数据的实际洞察和价值，而非仅仅以存储或传输的数据量为依据，这有助于确保客户更精准地支付与数据真实价值相符的费用，实现更有效的数据利用。对于商业分析而言，一份包含深度见解和关键趋势的小型数据集比冗长而一般的大数据集更具价值。如果仅仅以数据量来定价且数据匹配不准确，将导致客户支付大量费用，却得到相对较少的实际洞察。因此，以信息量为基础的定价模型更能反映数据的实际贡献，满足客户对高质量、高价值数据的需求。但在实际应用中，信息量通常难以客观衡量，同一份数据对于不同的买家来说信息量也不同，存在主观性。此外，数据价值遵循边际效用递减规律：同一组临床实验数据，对首个购买的药企可支撑其新药申报（高价值），但对后续购买者仅具验证价值（低价值）。

3）数据的时效性要求。在数据交易中考虑数据的时效性至关重要，因为不同业务场景对信息的实时性有着不同的需求。对于需要及时决策的应用，例如金融市场的实时交易或紧急网络安全事件的响应，及时、实时的数据是至关重要的。在这些情况下，过时的数据会导致决策不准确，甚至造成损失。对于历史趋势分析或长期战略规划来说，时效性要求较为灵活，但仍然需要确保数据在一定时间内的准确性和完整性。如果数据更新不及时，将会错过关键的市场变化，无法准确评估历史事件的影响。此外，在实时数据交易场景（如 IoT 传感器数据流）中，交易标的实为数据访问权而非数据本体[11]。在没有收集数据时，如何说服买方购买访问权限也是数据作为商品进行交易时面临的问题之一。因此，综合考虑数据时效性是确保数据交易成功的关键因素之一，这有助于确保数据满足特定业务需求，为数据买方提供有针对性的洞察，并在不同行业和应用中实现更有效地利用数据。

2.2 数据主权与数据确权

数据主权是一个多层次概念，既包括个人对其数据的合理控制权（如决定数据是否被分享、使用方式及范围等），也涵盖国家对境内数据的管辖、监管与保护权（如数据安全保障、跨境传输规制等）。欧盟实施的《通用数据保护条例》（*General Data Protection Regulation*，GDPR）[4]在个人数据权利保护层面集中体现了数据主权的个体维度理念。GDPR 通过赋予个人知情权、访问权、删除权等一系列数据控制权利，强化数据处理的透明度，并对数据跨境传输设置严格限制，确立了个人对自身数据的主导性权利，这与数据主权中“个人对数据的合理控制”高度契合。因此，GDPR 不仅是个人数据保护领域的重要立法实践，体现了数据主权在个体层面的核心精神，也成为全球数据治理与个人数据保护立法的重要范式。

数据确权与数据主权在数据交易中密切相关，但各自关注重点不同。数据确权指的是通过法律或技术手段明确数据的归属与使用权边界，为数据的流通与交易奠定基础；而数据主权则更侧重于数据拥有者对数据的全面掌控，包括是否分享、是否持久保存等决策权。前者强调“谁拥有、收益归谁”，后者强调“能否掌控、如何使用、是否授权”。两者相辅相成，数据确权是实现数据主权的前提和手段，数据主权则是确权的目标和价值体现。

为明确研究范畴，本文对关键术语进行特定定义：“数据确权”在本文中并非指法律意义上的权属确认，而是指从计算机科学角度出发，基于技术手段（如文本相似度检测、指纹提取等）对数据的原始来源进行判别，用于识别是否存在非法转售或重复交易行为；“数据主权”则特指数据卖家在数据交易后对数据使用方式、使用范围的持续掌控权，即数据流通过程中的可追踪性与授权边界控制能力。此处的“确权”更偏重于数据真实性与归属的技术判别逻辑，而“主权”则强调数据主体在交易后全生命周期的控制能力，两者共同构成数据交易信任与合规的基础。

2.3 数据交易基本技术

2.3.1 哈希函数与 MinHash 技术

哈希函数（Hash Function）是一类将任意长度输入映射为固定长度摘要（哈希值）的单向函数，其满足特定性、抗碰撞性并具有雪崩效应。在同一个哈希函数下，相同的输入永远产生相同的输出，且难以找到两个不同输入产生相同输出的情况。此外，即便两个输入仅有一个字符的差别，最终生成的哈希值也会有很大的不同，即雪崩效应。哈希值是固定长度的字符串，这意味着可以非常快速地对原始输入进行比较。对于需要比较大量文本是否相同时，这种方法尤其有效。如果两个文本的哈希值相同，那么理论上可以立即认为这两个文本相同，可以用来快速验证数据交易过程中所交付数据的真实性与完整性，即最终交付的数据与交付前声称的数据是否一致，时间复杂度仅为 $O(1)$。基于哈希函数的雪崩效应，传统的哈希函数可以用来快速比较两个文本是否相同，但不能检测文本是否相似。然而在数据交易过程中，数据确权应该考虑到数据整体的相似度，而不是简单地考虑数据整体是否相同，显然传统的哈希函数无法满足这一需求。

文本相似度检测通常通过 Jaccard 系数[12]来完成。给定两个集合 A 和 B，Jaccard 系数为 A 和 B 交集的大小与 A 和 B 并集的大小的比值。Jaccard 系数越大，样本相似度越高，表达式如下：

$$J(A,B)=\frac{|A\cap B|}{|A\cup B|},A,B\neq\emptyset$$

Jaccard 系数可以衡量两个数据样本间的相似度。Jaccard 相似度在小型数据集上表现良好，但在大规模数据集上则需要大量的计算资源，因为每两个数据集之间都需要计算一次相似度，时间复杂度为 $O(n^2)$。若能缩短两两比较的文本长度，便可以大大减少计算量。MinHash 技术采用了此思想。MinHash 算法是一种局部敏感哈希算法（Locality Sensitive Hashing）[13]，用于高效估计集合之间的 Jaccard 相似度。MinHash 的大致流程为：先选取 K 个独立哈希函数$\{h_1,\cdots,h_k\}$；对集合 S 中的每个元素 x，计算 $h_i(x)$；记录最小值 $m_i=\min\{h_i(x)\mid x\in S\}$，最后生成签名向量 $\boldsymbol{Sig}(S)=[m_1,\cdots,m_k]$。在该算法中，数据集会被表示为一个特征集合，通过多

个独立哈希函数对集合中的元素进行哈希，记录每个哈希函数下的最小哈希值，从而为每个集合构建一个签名向量（也称“数据指纹”），该向量的长度远小于原始集合的大小。对任意两个集合，其 MinHash 签名向量之间相同位置值的重合比例，即为它们的 Jaccard 相似度的近似值。由于哈希函数具备局部敏感性，相似集合更可能映射到相同签名，因此该方法可大幅减少计算开销。

MinHash 技术在数据交易过程中可用于数据确权与非法转售检测。其通过对原始数据生成短小的“数据指纹”，高效评估样本间的相似度。在数据确权中，MinHash 可作为权属标识；在数据交易中，平台可比对指纹，以识别重复出售与泄露风险。相比全文比对，MinHash 在大数据环境下具有更高的计算效率。

2.3.2 区块链技术与共识算法

区块链技术由中本聪（Satoshi Nakamoto）在 2008 年发表的《比特币：一种点对点电子现金系统》[14]中首次系统阐述，其本质是融合密码学、哈希链、分布式共识机制与 P2P 网络技术的多层级可信数据架构。在区块链中，每个数据块都链接到前一个块，最终形成连续的链。这种结构保证了区块链能够追溯交易历史的完整性，其可追溯与不可篡改的特性，使交易过程更加透明，提升了数据流通过程中的可信度与安全性。区块链通过哈希指针（Hash Pointer）的级联效应实现数据的不可篡改性：任何区块数据的修改都会引发该区块哈希值变更，导致后续所有区块的父哈希引用失效，这种链式反应会被全网节点通过定期默克尔根（Merkle Root）验证机制检测并拒绝。任何试图篡改数据的行为都需要重新获得网络中大多数节点的认可，这在实际计算上是不可行的。这些特点保证了区块链的不可篡改性，可以用于确保数据交易过程中所传输数据的一致性与完整性。

智能合约（Smart Contract）作为图灵完备的链上程序（如以太坊 EVM 字节码），通过预置的确定性状态转换逻辑实现自治执行，其代码部署、调用过程及状态变更均被永久记录在区块链上，形成可审计的执行轨迹，具有去中心化、不可篡改、自动执行和可审查等特点。在数据交易中，智能合约可用于自动管理交易流程，包括数据访问授权、付款结算、使用权限控制等操作，有效防止交易欺诈与违约行为，提高交易的可信度、效率与可追溯性。通过智能合约，数据提供方与需求方可建立更加安全、自动化和可验证的数据交易机制。

共识算法作为区块链的底层安全支柱，需解决分布式环境下的拜占庭容错（Byzantine Fault Tolerance）问题，即在允许部分节点故障或恶意行为的情况下，仍能保证网络状态的全局一致性。共识算法的发展伴随着区块链技术的演进，形成了多种经典机制，常见的包括工作量证明（Proof of Work，PoW）[14]、权益证明（Proof of Stake，PoS）[15]、委托权益证明（Delegated Proof of Stake，DPoS）[16]以及拜占庭容错算法（Practical Byzantine Fault Tolerance，PBFT）[17]等。PoW 通过哈希算力竞赛实现 Sybil 攻击防御，但其能耗较高（比特币网络年耗电超 100 TWh），造成社会资源的浪费；PoS 则根据节点所持代币数量分配记账权，提升了能效；DPoS 引入投票机制，由选出的代表节点进行记账，提高了性能和可扩展性；PBFT 适用于许可链，在少量节点间高效达成一致，广泛用于联盟链环境中。这些算法各有优劣，适配于不同的区块链场景需求。在缺乏中心机构的情况下，共识机制还可作为自动化仲裁工具，记录各方操作并达成统一结论，为交易争议提供可信依据，从而增强数据交易的透明性与公正性。

2.3.3 数据安全与隐私保护技术

同态加密（Homomorphic Encryption）[18]是允许在加密数据上直接执行特定运算的加密方法，无需事先解密数据。同态加密的核心特性满足函数一致性原则：对于任意允许的运算 f 及明文 $\{m_i\}_{i=1}^{n}$，始终存在 $Decrypt(f(Encrypt(m_1),\cdots,Encrypt(m_n)))=f(m_1,\cdots,m_n)$，即密文空间上的运算结果解密后与明文空间直接运算的结果严格等价。在数据共享与交易过程中，数据持有方通常需要将数据上传至第三方平台（如数据中介或数据市场），但也会担心平台非法访问、分析或泄露其数据。同态加密可以保障数据在“加密可计算”的状态下进行处理，防止平台获得明文内容，从而保护数据隐私。

可信执行环境（Trusted Execution Environment，TEE）是一种硬件层面隔离出的安全区域，可确保运行时数据的保密性与完整性不受主操作系统或其他特权实体影响。TEE 可以确保在该环境中运行的程序免受外部系统（包括操作系统、管理员，甚至主机所有者）的干扰与窥探。TEE 的典型实现包括 Intel SGX[19]，ARM TrustZone[20]等。在数据交易场景中，TEE 常用于构建受信任的中介平台，使数据持有方可以将加密或明文数据上传到 TEE 中执行算法分析，而无需担心中介平台作弊、泄露数据或篡改结果。这样既实现了对数据使用的可控、可信执行，又保护了数据隐私。因此，TEE 被广泛应用于隐私计算、数据确权、联合建模、非法转售检测等数据交易环节。

数字签名（Digital Signature）[21]是一种基于非对称加密的电子认证机制，广泛应用于数据安全与身份验证领域。其基本原理是：首先对原始数据使用哈希函数计算生成固定长度的摘要信息，然后由发送方使用其私钥对该摘要进行加密，生成数字签名。接收方收到数据和签名后，使用发送方的公钥对签名解密得到摘要 A，同时对收到的数据再次进行哈希计算得到摘要 B，若两者一致，即可确认数据未被篡改且确实来自合法发送者。在数据交易过程中，数字签名可用于验证数据持有者的身份、防止数据在传输过程中被篡改，并可作为交易的凭证，在争议仲裁中提供有效支撑。

3 数据交易模式对比

本章从数据交易模式的视角对现有较为成熟的数据交易框架进行归类，如表 1 所列，从交易模式与交易依托两个视角，分析数据交易过程中存在的各种难点。

表 1 数据交易框架对比

Table 1 Comparison of data trading frameworks

交易模式	交易依托	文献	框架特点
数据集交易	可信执行环境	[22]	利用区块链、远程认证协议和可信执行环境确保数据交易的去中心化、公平性和安全性
	区块链	[23]	链上只传输少部分关键数据，解决了区块链平台交易效率问题
		[24]	通过智能合约设计了有效的投票机制及内置的共识与惩罚功能
	中介	[25]	引入数据指纹帮助数据确权，中介可充当交易经纪人也可充当经销商
		[26]	提出唯一性指数，高效量化数据集独立性，实现数据交易的问责制
		[27]	引入声誉机制评估数据卖家和买家的信誉，识别和惩罚数据交易中的不当行为
数据处理即服务	可信执行环境	[28]	卖家的原始数据始终处于保护状态，原始数据不暴露给买家，仅在安全硬件环境中处理数据
	区块链	[29]	通过信号集和概率矩阵传递信息，买方基于信息调整决策以提升效用，卖方则通过定价实现收益，且全程不涉及原始数据的交易
		[30]	卖家仅需提供基于本地数据训练的模型更新(数据效用)，买家通过聚合这些模型更新来提升全局模型性能，实现数据价值的合法合规交易
	中介	[31]	中介先训练最优模型，再通过注入噪声生成不同精度的模型实例，实现“版本化”销售
众包交易	区块链	[32]	数字水印确保数据版权，语义相似性算法保障数据质量
		[33]	利用众包感知与真相发现技术，从不可靠的传感器数据中挖掘可靠知识，根据数据质量分配众包利润
		[34]	基于同态加密的真相发现技术和可靠性评级机制，计算卖方数据质量，同时监督消费者根据数据真实地对卖方的可靠性进行评级
		[35]	学习买卖双方交互历史动态，提升众包数据匹配精准度
		[36]	通过计算任务集相似度和账号轨迹相似度对卖家进行分组，识别恶意卖家并弱化恶意数据影响
	中介	[37]	买家上传数据特征，中介根据买家样例特征与预算代替买家选择数据集
		[38]	依据数据的不确定性和复杂相关性，以条件熵为量化指标，结合市场中数据买家的多样化需求，将数据质量分为不同质量级别的版本

3.1 交易模式

数据集交易模式下，数据卖家通常拥有稳定的数据来源(如合作机构授权、公开数据爬取、自有业务积累)，且具备数据清洗、结构化、标准化处理能力。通过批量生产标准化数据集，“一次制作、多次销售”以降低边际成本并进行版本化、时间维度等维度的差异化定价。然而，标准化与可复用性的提升，也使得已经打包的数据更易被复制、传播，从而显著增加了非法转售、数据滥用和隐私泄露等风险。因此，该模式亟需在交易机制中引入数据确权，使用控制与溯源审计等手段，以有效保障数据资产的合法流通与权益归属。此外，此类数据通常以静态形式交付，更新频率相对较低，难以满足对高时效性与动态性数据的需求。

相比之下，数据处理即服务(Data-as-a-Service，DaaS)模式强调以“处理结果”为核心交付物，买方无需接触原始数据即可获取如模型预测、数据分析报告、风控评分或推荐结果等服务成果。该模式的显著优势在于：原始数据始终不对外暴露，在源头上规避了数据泄露与非法转售的风险。然而，DaaS 模式也面临一系列挑战：首先，数据处理任务的工作量往往难以量化，导致定价机制缺乏统一标准；其次，在不直接获取原始数据的前提下，买方难以客观评估处理结果的准确性与有效性，容易产生“结果未达预期”的争议，进而引发信任问题与责任归属纠纷。

在众包交易模式中，数据的提供不再依赖于少数集中式机构，而是通过激励机制广泛动员个体用户、终端设备或小微组织提交数据。这类模式适用于分布式、碎片化的数据采集需求，如城市交通照片、环境传感数据、用户行为记录、商品评论等，具有强烈的实时性与地域性特征。买方通常是需要海量、多样、实时数据的组织，如地图服务平台、市场调研公司或人工智能模型开发者；卖方则是通过移动端、IoT 设备和在线平台等参与数据贡献的众多个体。该模式的优势在于，数据来源广泛、覆盖面广，特别适合难以通过集中式方式获取的场景。然而，该模式也面临诸多挑战：首先，数据质量难以保障，提交者之间存在显著异质性，可能出现冗余、错误或欺诈性数据；其次，动态数据则需要持续众包更新，平台需通过补贴、激励机制保持提供者活跃度，否则数据时效性会下降；再次，参与方可信度难以验证，平台需设计激励与声誉机制以提升参与积极性与数据可靠性；此外，众包模式下的数据确权与责任归属界定更为复杂，如何平衡个体隐私保护与买方效用最大化，仍是当前研究与实践中的重要议题。

3.2 交易依托

可信执行环境(TEE)提供了基于硬件隔离的安全执行环境，使得数据在处理过程中始终处于保护状态，即使在中介平台或云服务器上运行，数据本身也不会暴露。该机制能够有效防止数据泄露与篡改，特别适用于“数据不出域”的交易场景，如数据处理即服务。然而，TEE 的部署依赖特定硬件，可扩展性有限。

区块链通过去中心化的账本结构和共识机制，实现了交易过程的公开透明、不可篡改与可追溯，特别适合需要强可验证性和溯源能力的数据交易场景。智能合约进一步实现自动化权限管理、收益分配等功能。区块链机制强化了交易的问责制和非否认能力，有利于降低交易双方的信任成本。然而，

性能瓶颈(如 TPS 限制)、链上存储开销仍是其面临的主要挑战,尤其在大规模、高频交易中表现受限。

中介平台依托中心化运营机制提供数据对接、质量评估、定价撮合等交易服务,具备良好的业务灵活性和用户体验,特别适合异构数据聚合与服务定制场景。中介能够主动承担信任桥梁角色,并通过引入声誉机制、水印技术或数据指纹实现确权与质量控制。但其可信度高度依赖平台本身,存在"中介作恶"风险;在无透明监督机制的情况下,平台可能滥用交易数据或歪曲评价体系,降低交易公正性。系统安全性上,中心化平台也存在单点故障的风险。

3.3 小结

总体来看,上述交易模式与交易依托虽各具优势,但在实际交易中均面临一系列难点:1)数据确权与溯源困难,标准化数据易被复制、非法转售,权益归属难以界定;2)数据质量难以保证,特别是在买卖双方信息不对称的情况下,难以验证处理结果的真实性或数据质量的可靠性;3)数据定价难,数据信息量通常难以客观衡量,同一份数据对于不同的买家来说信息量也不同,进而难以定价;4)数据交易的非否认,涉及到数据和资金交付的原子性与不可否认性;5)保障数据主权,数据交付后的使用方式应该遵从事先约定的规则,如数据的使用方式、用途和范围等。上述问题共同制约了数据资产的安全流通与价值实现。

4 数据交易难点解决方案

4.1 数据确权

数据确权的目的是保证数据原始卖家的利益,否则会出现转售者恶意低价转售的行为,从而损害数据原始卖家的利润,破坏数据交易市场秩序。文献[25]通过提取数据的多维度特征(如图像的颜色直方图、平均哈希值、结构相似度指数等)组合生成数据指纹,每个待售数据绑定唯一智能合约,合约中记录数据指纹、描述信息及所有者公钥,存储在区块链上。平台维护"数据-合约表",记录历史合约地址、指纹及所有者账户,确保所有权可追溯。卖家上传数据时,平台会将其指纹与"数据-合约表"中已有指纹进行比对,若相似度超过阈值,则拒绝上架。文献[32]将卖家的"版权指纹"和消费者的唯一指纹嵌入数据中,生成带水印的数据。若发现盗版数据,则提取其中的指纹并与区块链中存储的消费者指纹进行比对即可定位非法转售者;同时,卖家可验证其他卖家数据中是否包含自己的版权指纹,识别盗用行为。文献[27]将数据的 MinHash 值上传至区块链"索引链",链中记录数据摘要、数字签名、卖家信息等,作为所有权凭证。文献[39]提出的框架要求数据卖家在交易前必须提供基于 MinHash 的所有权证明。文献[26]提出了 AccountTrade——一个通过中介进行数据交易的可问责协议,它通过计算唯一性指数来衡量数据独特性,并根据唯一性指数是否介于限定区间来判断数据的原创性,还可通过数据经纪人辅助数据确权。但该方案需要将原始数据集暴露给交易平台或数据经纪人,仍然存在数据被恶意泄露或非法分析的可能。在文献[40]提出的方案中,数据买家将所需的数据资源广播到整个网络时,数据卖家响应并声称拥有数据资源,然后执行挑战响应机制(Challenge Response Mechanism),用于验证响应者是否真的是包含该数据集的以太坊地址的所有者。

上述数据确权方案大多依赖于提取数据的特征信息并将其上链或公开,以实现所有权标识与非法转售检测。然而,这些特征信息通常仅在特定数据交易系统内部有效,缺乏跨平台的通用性与互认机制。若非法转售者绕过原系统,将数据转移至另一个交易平台进行出售,由于该平台无法访问或验证原平台中的确权信息,转售者可能被错误地识别为"数据原始持有者",非法转售者则规避了监管与责任追溯。这一局限性反映出当前确权机制在跨系统协同与互信方面的不足。文献[41]提出的方案允许数据买家合法转售数据,并确保数据原始卖家在授权转售中获得收入。该方案将问题建模为两阶段斯塔克伯格博弈(Stackelberg Game),使用经济学和博弈论的理论来分析定价方案,确定了数据生产者和转售者之间的收入分享比例,可以为数据原始卖家和转售者带来更高的利润。数据原始卖家通过监听网络中的验证请求来检测非法转售,如果原始卖家发现数据被未经授权的转售者出售,他们会展示数据所有权证据,绕过非法转售者并创建新的智能合约直接与数据买家交易。"允许转售"的方案从动机上抑制了非法转售的行为,但要求数据原始卖家持续监听验证广播,否则可能导致部分非法转售行为未被及时识别和追踪。

4.2 数据质量保证

在数据交易过程中,数据作为非实体商品,其质量往往具有高度的信息不对称性。买家在未获取数据内容前难以全面评估其准确性、完整性与实用性,导致交易决策面临不确定性风险。尤其在缺乏标准化评估机制与可信验证手段的情况下,数据质量难以被客观衡量,成为制约数据交易效率与信任建立的关键障碍。

文献[22]中的可信交换节点会提取一小部分加密数据发送给买家,买家解密后可以直接验证这部分数据是否符合自身需求,以达到"验货"的目的,避免"货不对板"。文献[35]通过学习买卖双方的历史交互行为,动态更新双边偏好序列,从而提升偏好表达的准确性。在此基础上,引入扩展的稳定匹配算法,即任意一方均无法通过单方面更换匹配对象而获得更优结果。方案整体采用"匹配筛选-动态偏好优化-稳定匹配"的三阶段流程,实现数据供需双方的高质量匹配,有效提升数据交易的匹配效率与满意度。文献[36]通过计算任务集相似度和账号轨迹相似度对卖家进行分组,识别恶意卖家并弱化恶意数据影响。文献[37]提出的 CrowdBuy 协议则允许数据买家先提供数据特征与购买预算,然后由中介在预算内来匹配最符合样例特征的众包数据集。尽管更安全的 CrowdBuy++协议保障了用户的数据隐私不被泄露,但是此模式下买家丧失了自由选择数据卖家的权利,平台仍有偏袒作弊的可能。文献[42]设计了一种激励机制,鼓励数据提供者如实报告数据与质量,在投入必要努力的情况下获得最大收益,从而实现真实性与个体理性。具体而言,该机制确保个体选择诚实报告并付出预期努力时,其收益将高于误报或懈怠的策略,从而促使"真实报告并努力投入"成为其最优响应策略,达到纳什均衡(Nash Equilibrium),有

效提升数据质量与市场稳定性。文献[43]要求数据卖家自我估计数据质量，通过计算每个数据卖家的相对贡献，帮助其主动校准感知偏差，提升自我估计数据质量的准确性，从源头改善数据质量。数据买家则在有限预算内优先招募高质量卖家，并通过优化任务分配激励卖家提供高质量数据。数据交易中，买家通常会对数据提出具体要求（如数据格式、取值范围、无重复项、满足特定统计属性等），这些要求可抽象为“合规谓词”（Compliance Predicate）。文献[44]中提出的协议的核心是让每个数据卖家证明其提交的数据满足该谓词，同时不泄露数据归属或具体内容，从而达到买家的数据要求。

当涉及隐私数据交易时，数据卖家通常不愿向买家泄露敏感的个人数据和真实身份。此时，验证数据真实性与隐私保护的目标相互矛盾。文献[45]利用同态加密构建密文空间，支持数据卖家开展数据服务、数据买家进行结果验证，同时保障数据机密性；其采用的新型基于身份的签名方案在密文空间中执行（不同于传统在明文空间操作的数字签名方案），每个数据卖家的签名均衍生自其真实身份，这一特性可使数据买家确信数据卖家真实收集并处理了数据。文献[46]引入诚实但好奇（Honest-but-Curious）的交易服务器，帮助生成带验证位的盲化扰动噪声，数据卖家将独特扰动印记嵌入数据以保证可验证性，交易服务器监督交易过程，实现对数据扰动和来源真实性的验证，在不泄露隐私的前提下确保交易数据真实可靠。

文献[30]专门针对于联邦学习场景，数据买家先初始化一个全局模型并分发给各数据卖家，卖家无需共享原始数据，仅需提供基于本地数据训练的模型更新（数据效用），买家通过聚合这些模型更新来提升全局模型性能，基于本地模型更新的质量间接评估其背后数据的质量，实现数据价值的合法合规交易。除此之外，文献[22,24,27-28,34,47-48]都引入了评价系统或声誉系统，辅助买家与卖家双向选择。

4.3 数据定价

数据定价是完成一笔数据交易的前提之一。数据的价值通常难以确定，同一份数据对于不同的用户具有不同的价值。因此，客户定制化交易模式应该被考虑到数据交易过程中。此外，高质量、易访问的数据通常比质量低、难以批量分析处理的数据更具有价值，数据的定价也需要考虑到市场需求和供给，遵循市场交易规律。如表2所列，现有主流数据定价方案可以归类为：按贡献定价、拍卖定价、招标定价、混合定价、基于隐私牺牲的定价、灵活定价以及按查询定价。

表2 数据定价方案对比

Table 2 Comparison of data pricing schemes

定价方式	文献	亮点	局限性
贡献	[30]	按数据卖家的实际贡献（即模型聚合权重）分配奖励，解决了公平计费的核心问题	聚合权重受模型评估偏差影响
	[49]	学习买家的估值信息来设定价格，满足不同买家对数据准确性的不同需求，通过博弈论量化卖家贡献	基于贪婪算法，计算量大
拍卖	[38]	以中介的视角采购并出售数据集，实现收益近似最大化	数据中介很难准确获取或验证成本分布的真实性
	[50]	强调数据独占性，通过时间敏感性来激励买家出高价	牺牲了卖给多个买家从而获得更多收益的可能
招标	[32]	基于语义相似度的拍卖，保障定价合理、价格诚实与收益非负	语义相似度依赖特征向量准确性
	[34]	通过反向拍卖中的临界支付机制，平衡了成本效率与卖家激励	当参与的卖家或任务增多时，计算开销显著增加
	[37]	在预算内从多个卖家中根据价格和数据特征匹配多个数据集	买家没有权利选择卖家，数据匹配服务由中介完成
混合定价	[11]	根据市场上的买家类型差异化定价，旨在最大化数据卖家的收入，同时考虑了买家类型的多样性	真实市场上的买家类型难以估计
	[51]	基于时间、数量与订阅制推出不同的定价方案，凸显了低复杂度订阅方案的实用价值	难以完全适配复杂多变的实际数据交易场景
隐私牺牲	[52]	马尔可夫链模型量化时间戳级别的隐私损失，能更精细地补偿不同时间戳的隐私损失	实际数据的复杂性远超模型假设
	[53]	将定价建模为椭球体，定价根据模型当前的认知和市场反馈来确定报价	依赖于隐私补偿的准确量化
	[54]	定价函数直接依赖于隐私损失	难以实现数据所有者隐私估值的真实性
	[55]	即使数据所有者未直接参与数据统计，若其关联数据被使用，也能因隐私损失获得补偿	实际可能缺乏依赖关系的先验知识
灵活定价	[31]	对基于数据训练的机器学习模型实例定价	适用的模型型类型受限
	[56]	学习用户支付意愿，据此调整公布价格	计算量大
	[57]	将定价视为非平稳的多臂老虎机问题，引入衰减因子，衡量历史的重要性	实际市场条件难以假设
	[58]	基于上下文动态定价机制和改进的随机梯度下降算法学习数据所有者的成本模型，动态调整价格	对不符合线性成本特征的真实世界数据适应性有限
查询定价	[59]	支持复杂查询的灵活定价，同时解决无套利、重复收费、多卖家收益分配问题	对于大规模集，当前框架的定价效率不足

基于贡献的定价方案中，数据的价格不再由卖家单方面定价或完全依靠市场拍卖决定，而是根据数据对模型效果或决策结果的“边际贡献”进行定价。按贡献定价可以体现数据的真实价值，激励高质量数据供给，非常适合联邦学习场景[30]。文献[49]也通过动态学习数据买家的估值信息来设定价格，为了满足不同买家对数据准确性的不同需求，将数据商品划分为多个版本的多种定价出售，通过计算每个数据提供者的Shapley值来确保奖励的公平性。Shapley值是一种在博弈理论中用来量化个体对整个团队贡献的方法，它确保了每个数据卖家获得的奖励与其对数据整体所做的贡献成正比。此类贪婪算法虽然在理论上提供了近似最优解，但在实际应用中可能需要大量的计算资源。基于拍卖的数据定价是

目前数据市场中另一类重要的定价机制。与按贡献定价相比,它更强调基于市场供需博弈来决定价格。通过设计合理的拍卖机制,数据买方在市场上进行竞价,价格由市场行为动态形成,而非由数据特征或模型贡献预先决定。文献[38]除了基于拍卖模式之外,还通过计算数据提供者的虚拟成本以实现最低成本采购数据。数据中介将原始数据转换为基于统计模型的“信息商品”,并按质量划分为多个版本,为每个版本设定固定价格,简化交易流程。该方案基于公开已知的成本分布计算虚拟成本和最优支付,但这一假设在实际场景中可能难以满足,因为数据买家的成本是私有信息,数据中介很难准确获取或验证成本分布的真实性。除此之外,买家感知的数据价值可能随时间推移而变化。文献[50]的拍卖方案中,数据只会出售给一个买家,从而确保每个买家参与拍卖时至少有非负的预期收益,通过时间敏感性来激励买家在数据价值较高时出价。

与传统拍卖(正向拍卖)相对应的交易模式是逆向拍卖(反向拍卖),也称为招标模式,是一种以买方为主导的定价与交易方式。卖方通过竞相报价,逐步降低价格,最终由买方择优成交。文献[32]以语义相似度作为数据质量的衡量标准,通过计算消费者和卖家数据描述的特征向量差异得出衡量标准,通过计算消费者和卖家数据描述的特征向量差异得出语义相似度,且该相似度会直接影响卖家在拍卖中的竞争力。在赢家选择阶段,采用贪心策略,每次选择边际效用与报价比值最高的卖家,意在满足数据质量阈值的同时最小化总支付成本。拍卖机制能激励卖家诚实报价,因为其赢家选择规则具有单调性且支付为临界值,使得卖家诚实报价时收益最大,同时能确保赢家获得的收益不低于其成本,保障卖家收益非负。在数据交易中,存在卖家虚报数据收集成本以获取更多收益的问题。文献[34]的反向拍卖机制采用两步投标策略,第一步卖家提交加密投标,第二步提交未加密投标并进行验证。这种方式使得卖家无法监听他人投标,且投标会被加密验证,无法谎报,从而保证卖家如实报告数据收集成本。文献[37]方案中的竞标由框架平台来完成,数据买家声明数据需求后,多个卖家参与竞标出价,在买家预算内选取一或多个符合要求的卖家。此方案下,数据买家只能声明数据需求,不具备卖家选择权,因为最终的入围卖家由平台来决定。

混合定价考虑了数据市场和买家类型的多样性,根据不同的买家偏好提供多种不同的定价方案。在文献[11]中,MSimple 机制适用于市场中只有一种类型的买家,即所有买家具有相同的需求和支付能力;MGeneral 机制适用于市场中存在多种类型的买家,每种买家可能有不同的需求和支付能力,通过解决一个凸规划问题,卖家可以找到最优的定价策略;MPractical 机制适用于买家理性有限的情况,即买家可能无法完全理解或评估复杂的定价策略,或者渴望卖家提供一个简单、易于理解的定价菜单的情况。上述 3 种定价机制旨在最大化数据卖家的收入,同时考虑了买家的类型多样性、有限理性以及数据的独特经济属性。文献[51]基于时间、数量与订阅制推出不同的定价方案。时间依赖型定价是指每次数据更新的价格由请求该更新的具体时间决定的定价方式;数量依赖型定价是指每次数据更新的价格依据已请求的更新次数而定(例如通过累计折扣),以此吸引更多更新请求的定价方式;订阅型定价是指每次更新收取固定费用并额外收取一次性订阅费,是一种实现复杂度较低的定价方式,凸显了低复杂度订阅方案的实用价值。

基于隐私牺牲的定价是指在数据交易过程中,根据数据主体所承受的隐私泄露风险对数据价值进行补偿定价的机制。由于隐私数据的暴露可能带来潜在的安全威胁、身份风险或未来的经济损失,因此,隐私牺牲定价模型试图通过合理的经济激励,衡量并补偿数据主体的隐私风险,确保数据交易的公平性和可持续性。文献[52]从数据中介视角,通过马尔可夫链模型量化时间戳级别的隐私损失,能更精细地补偿不同时间戳的隐私损失,同时保证中介的盈利能力和对数据买家的无套利性,但参数设置不当可能导致隐私保护过度或不足、定价不合理等问题。文献[53]的定价过程利用当前和历史数据查询的信息,通过椭球知识集等方式动态估计查询的市场价值,结合保留价确定发布价格,并根据交易反馈不断更新对市场价值模型的认知。文献[54]的定价函数直接依赖于隐私损失:噪声越小(隐私损失越大),价格越高;噪声越大(隐私损失越小),价格越低;每个数据查询都由数据消费者自定义分析方法和可接受的隐私噪声水平。因此,不同消费者的查询差异很大,数据经纪人也无法对这些查询进行统一控制。文献[55]结合自上而下和自下而上两种数据定价方法。自上而下方法先确定服务价格,再按隐私损失比例分配补偿给数据所有者;自下而上方法先计算每个数据所有者的隐私补偿,再汇总确定服务价格(确保总价格覆盖补偿)。除此之外,该方案还充分体现了“依赖公平性”:即使数据所有者未直接参与统计,若其关联数据被使用,也能因隐私损失获得补偿。隐私补偿的计算依赖于数据项的域和依赖关系的先验知识,但在实际场景中,这些信息难以精确获取。

灵活定价是指根据数据交易市场的实时供需关系、数据特征(如稀缺性、时效性、隐私敏感度)、用户偏好或交易环境动态调整价格的机制。文献[31]的方案不直接对原始数据定价,而是对基于数据训练的机器学习模型实例进行定价。价格由模型实例的精度决定,而非底层数据集的规模或内容。精度越高的模型,价格越高;反之,则价格越低。该方案主要聚焦于结构相对简单、误差函数严格凸的机器学习模型,模型类型相对受限。文献[56]和文献[57]都将定价问题建模为多臂老虎机(Multi-armed Bandit)问题。文献[56]采用了一种基于线性回归的算法,观察用户对不同价格的反应来学习买家估值分布,并据此调整公布价格。文献[57]通过引入衰减因子来调整历史信息的重要性,每个“臂”(即候选价格)的奖励分布随时间变化,使得算法能够更好地适应估值随时间变化的情况。该算法依赖于对买家估值(即买家愿意支付的价格)分布和时间折扣函数的特定假设,如果实际市场条件与这些假设不符,策略就无法达到预期的性能。文献[58]基于上下文动态定价机制和改进的随机梯度下降算法学习数据所有

者的成本模型，并基于学习到的成本模型动态调整价格，实现买家收益最大化与卖家非负收益的平衡。其核心算法设计仍基于线性假设，这导致模型对不符合线性成本特征的真实世界数据适应性有限。尽管灵活定价看似能够更加适应多种类型的数据交易，但文献[60]认为灵活定价为卖家带来的经济收益低于固定定价，因为固定定价通过捆绑销售整体数据集，能更好地捕获消费者剩余(Consumer Surplus)。

查询定价主要用于数据查询或数据分析接口的按需计价，而不是直接售卖完整数据集，这种交易模式较为普遍。例如，阿里云、AWS、Google Cloud 等主流云服务商的数据市场，广泛采用了 API 按查询计费的方式，用户可以按需调用接口获取天气数据、金融行情、地图信息、舆情监测结果等，每次调用都根据查询范围、数据维度和响应复杂度计费，这种模式典型地体现了查询定价机制的实际应用。基于查询的定价需要做到无套利，即查询价格不得高于能推导出该查询结果的一组视图的总价格，否则买家会选择购买视图自行推导，存在套利空间。在一些查询方案中，买家有时需要组合多个数据源的复杂查询，被迫购买远超需求的数据集。文献[59]提出 QueryMarket 系统，旨在支持复杂查询的灵活定价，同时解决重复收费、数据库更新、多卖家收益分配等实际问题。

4.4 数据交易非否认

数据交易过程中的非否认是指交易双方无法否认其参与交易的行为。例如，数据买家在收到数据集后不能否认其购买行为或拒绝打款，数据卖家不能向买家交付与声称数据不一致的数据，数据买家不能恶意声称其收到的数据与卖家声称的数据不一致等。此外，非否认机制还应该保证最终交付数据的完整性，如果数据在传输过程中被恶意篡改，买方将收到不完整或被恶意修改的数据，进而影响数据分析或商业决策。

文献[26]与文献[37]基于可信第三方来保障数据交易流程的完整性。文献[26]要求买方在平台维护的公告板上发布购买声明，买方在声明后不可否认其购买行为，打款和数据传输则由数据中介介入。文献[37]的方案包含一个验证机制，允许买家在收到图像后验证其与卖家上传的特征向量是否一致，以确保数据一致性。文献[22]则基于可信执行环境来保证数据的交付，避免了数据中介在数据交易过程中作弊的可能。

除此之外，智能合约[23-33]能保证数据交易过程的公开透明与自动化执行，原子交换协议[61-62]的应用也能保证数据交付与资金结算的原子性，均为普遍采用的数据交易非否认方案。

4.5 保障数据主权

数据是新型社会生产要素，保证数据主权是数据自由规范流通的前提，同时，数据主权也反对利用技术手段限制数据的自由流通以达到数据垄断的目的。文献[63]提出的平台通过区块链的智能合约实现了对 GDPR 合规性的支持，允许数据主体轻松行使访问、更正和删除其个人数据的权利。数据主体可以通过用户界面发起请求，智能合约随后自动触发相应的操作，如更新数据记录或从数据集中删除个人信息。这些操作都会被记录在区块链上，确保了过程的透明性和可追踪性。文献[64]支持去中心化环境中数据共享的操作级日志记录，这种细粒度的个人数据来源历史使数据所有者能够跟踪其数据与第三方共享后发生的情况，保障了 GDPR 中的“知情权”。文献[65]参考公钥基础设施中的证书透明化机制，提出了透明日志机制。该机制允许持续向数据所有者报告其数据的活动，使得数据所有者可以验证数据使用者是否按照约定使用数据，从而监督数据使用者遵守约定好的使用条款。文献[66]的方案中，用户可以通过定义隐私偏好(如数据可被使用的目的、保留时间、是否允许第三方使用等)，明确规定自己的数据如何被处理和利用。该框架通过区块链上的智能合约执行这些隐私偏好，检查消费者的隐私政策是否符合用户意愿，只有符合要求的消费者才能获取数据。同时，用户还能对隐私偏好的执行情况进行审计，验证数据是否按自己的规定被使用，进一步强化了对数据使用的掌控权。类似 GDPR 中的“被遗忘权”(Right to be Forgotten)，保障数据主权也应该给予用户从存储和处理其个人信息的系统中删除其数据的权利。需要注意的是，这里的删除指的是根据合约的“拒绝使用”，比如合约限制数据只能用一段时间而非永久使用，并非是数据卖家可以随意删除自己的数据。文献[67]提出将删除作为一种控制方法(Deletion as Control)来保障用户的“被遗忘权”。这种方法允许用户在数据被删除之前自由使用数据，但在数据被删除后，数据控制器的未来行为和内部状态不应再依赖于已删除的数据。简言之，数据被删除后，数据使用方的后续行为不应再与被删除的数据有相关行为。文献[68]借助可穿刺加密(Puncturable Encryption)技术，使用户可以使用现有密钥和相应标签对密钥进行穿刺操作，生成新的穿刺密钥。拥有穿刺密钥的主体无法解密带有特定穿刺标签的加密数据，即使用户的属性满足数据的访问策略也无法访问，从而实现对特定数据的自主删除控制。这意味着用户能够独立、精准地删除特定数据，无需依赖第三方的协助。

4.6 小结

本文介绍的数据交易框架大多依托区块链技术实现交易的透明化与可追溯性，但区块链系统的性能瓶颈，尤其是吞吐量的限制，仍是制约大规模数据交易落地的重要挑战之一。文献[23]将数据分割成两部分：较大的部分 S1 和较小的部分 S2，数据买家只有完全收到 S1 和 S2 时才能访问数据，比如 S2 可以是 S1 的加密密钥。S1 通过安全的离链通道发送给数据买家，S2 则在链上传输，智能合约只需处理较小的数据量，从而降低了计算和存储成本。基于区块链的数据交易框架也有潜在的双重支付攻击，即买家恶意尝试用同一笔钱购买多份数据。使用未花费的交易输出(UTXO)、工作量证明、网络共识与交易确认可以解决双重支付的问题。不基于区块链的交易平台则存在数据中介作弊、单点故障与数据泄露等风险。

本章主要围绕数据确权、数据质量保障、数据定价、交易非否认性与数据主权等核心问题，梳理并分析了现有的数据

交易解决方案。然而,数据交易的挑战远不止于此。由于数据本身具有多样的形式与复杂的属性,不同类型的数据交易面临各自特有的技术难题和风险。现有框架仍需根据数据的具体特征与应用场景,设计更具针对性的机制与策略,以完善数据交易的全流程保障体系。

5 未来研究方向

1)数据流通的标准化与基础设施的建立。要做好数据要素市场,首先要保证数据能够正常流通。现阶段数据流通仍然存在许多难点:首先是数据格式与标准不一致,不同行业和组织可能使用不同的数据格式和编码标准,这使得数据在不同系统间传输和解析变得复杂;其次,不同领域使用不同的软件平台和系统架构也可能导致数据在不同平台间无法直接交换,阻碍数据的有效流通。因此,需要开发相关平台或中间件来实现数据的无缝对接,如数据空间项目。数据空间项目中引入了"自我描述"机制[69],"自我描述"是指数据集的元数据(Metadata),元数据提供了数据集的内容、结构、来源、质量、使用条件和访问权限等关键信息。"自我描述"的目的是确保数据的可发现性、可理解性和可重用性,使数据买家能够清楚地了解数据的特性和适用性,进而做出有效的数据选择决策。数据空间通过采用统一的数据标准和协议,如开放的 APIs、数据模型和数据交换格式,从而保证不同系统之间的互操作性。这有助于简化数据格式和编码标准的不一致问题,使得数据能够在不同平台和应用之间无缝传输。数据空间也提供了数据治理框架,允许数据所有者定义数据的使用规则和访问权限。同时,通过数据质量管理工具,可以监控和维护数据的准确性和一致性。数据空间通过集中管理和优化资源分配,降低了数据流通的总体成本。数据空间建立在强大的技术基础设施之上,为大规模数据处理提供了必要的支持,同时也降低了单个组织建立和维护这些基础设施的成本。

2)重视数据的差异化与交易方法的实用性。尽管现有研究在数据交易定价、确权及隐私保护等方面提出了多种方法,但与实际应用场景相比,数据交易平台所能提供的功能仍然较为有限。一方面,部分理论方法在实践中面临较高的部署成本,或过度依赖于对市场结构的先验假设,因而难以在真实交易环境中落地;另一方面,现有平台在功能设计上缺乏对不同类型数据的差异化支持,未能建立与数据特征相匹配的交易机制。这种方法与平台之间的脱节导致了"研究成果丰富但平台功能单一"的矛盾,也限制了数据要素市场的活力与发展空间。因此,未来的研究与实践需要更加关注数据交易难点解决方案的可操作性,并探索面向多样化数据类型的分类指引与平台功能集成,以推动数据交易市场的健康、可持续发展。

3)把握 Web 3.0 机遇。随着 Web 3.0 时代的到来,数据交易市场面临新的发展机遇与技术变革。Web 3.0 倡导的去中心化理念,将进一步推动数据资产的个人掌控与可信流通。去中心化身份(Decentralized Identifier,DID)[70]技术和可验证凭证(Verifiable Credential,VC)[71]技术,为数据确权提供了新的解决思路。个人或组织可以通过 DID 绑定其生成或收集的数据,利用可验证凭证对数据来源、质量、授权范围进行链上声明,实现数据的"自带确权",并支持跨平台迁移和复用,打破数据割据现状。此外,未来的数据交易平台可探索将去中心化自治组织(Decentralized Autonomous Organization,DAO)机制引入数据市场治理。DAO 可以通过社区共治的方式协商数据定价、质量评估、收益分配等规则,降低平台作恶风险,增强透明度与公平性。例如,数据价格的形成可以结合多方共识、链上历史交易数据及供需博弈动态,通过 DAO 机制动态调整,替代中心化平台单方面定价。这种机制有望激发数据市场参与者的积极性,实现更具弹性的价值发现过程。同时,结合多方安全计算、零知识证明、可验证计算等 Web3.0 技术,可以构建更加完善的数据交易协议,实现隐私保护与数据可用性的兼容,缓解当前"隐私与数据价值冲突"的核心难题。例如,数据卖家可在不暴露原始数据的前提下,证明数据符合买家的质量要求或用途需求,降低信任门槛。未来的数据交易研究需要紧密结合 Web 3.0 生态技术,构建更加开放、可信、自治的数据市场,推动数据资产的自由流动与公平收益分配,最终实现以"数据为要素"的数字经济可持续发展。

结束语 数字化转型背景下,数据要素已成为各行业的核心资源,驱动市场持续扩张。尽管现有研究在技术应用与机制设计上取得了一定进展,但已实际落地的数据交易市场的功能依然单一。本文系统梳理了数据交易的背景特征、技术基础与现有成熟框架,将数据交易模式归类为数据集交易、数据处理即服务,以及众包交易,结合常见的交易依托(区块链、中介、可信执行环境)对数据交易框架进行了对比,对比并介绍了数据交易难点的主要解决方案,最后得出结论:现有数据交易平台的现实发展与理论研究脱轨显著,部分理论方法在实践中面临较高的部署成本,或过度依赖于对市场结构的先验假设,难以在真实交易环境中落地;数据交易平台在功能设计上缺乏对不同类型数据的差异化支持,未能建立与数据特征相匹配的交易机制。因此,建议未来研究聚焦三方面:1)推进数据流通标准化与基础设施建设,实现数据流通的标准化操作;2)数据交易平台应当充分考虑到数据的差异化,提供多样化的数据交易难点解决方案;3)借力 Web 3.0 技术构建去中心化可信体系,强化跨平台确权与数据主权保障,助力数据要素市场高质量发展。

参 考 文 献

[1] National Data Administration [EB/OL]. https://www.nda.gov.cn.

[2] Data Governance Act[EB/OL]. https://eur-lex.europa.eu/eli/reg/2022/868/oj.

[3] Opinions of the Communist Party of China Central Committee and the State Council on Establishing a Basic Data System to Better Give Play to the Role of Data Elements[EB/OL]. https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

[4] General Data Protection Regulation[EB/OL]. https://gdpr-info.eu/.

[5] National Development and Reform Commission [EB/OL]. ht-

tps://www.ndrc.gov.cn/wsdwhfz/202209/t20220913_1335479_ext.html.

[6] Shanghai Data Exchange [EB/OL]. https://www.chinadep.com/.

[7] Guiyang Big Data Exchange [EB/OL]. https://www.gzdex.com.cn/.

[8] Research Report on Consumer Data Circulation Model Based on the Right to Data Portability[EB/OL]. http://www.sic.gov.cn/sic/93/552/622/0529/20240529080857 1136847956_pc.html.

[9] XIONG Q, TANG K. Research Progress on the Right Delimitation, Exchange and Pricing of Data[J]. Economic Perspectives, 2021(2):143-158.

[10] JIANG D, YUAN Y, ZHANG X, et al. Survey on Data Pricing and Trading Research[J]. Journal of Software, 2022, 34(3): 1396-1424.

[11] MAO W, ZHENG Z, WU F. Pricing for Revenue Maximization in IoT Data Markets: An Information Design Perspective[C]// IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019: 1837-1845.

[12] TIAN X, ZHENG J, ZHANG Z. Jaccard Text Similarity Algorithm Based on Word Embedding[J]. Computer Science, 2018, 45(7): 186-189.

[13] WU W, LI B, CHEN L, et al. A Review for Weighted MinHash Algorithms(Extended abstract)[C]// 2023 IEEE 39th International Conference on Data Engineering (ICDE). IEEE, 2023: 3785-3786.

[14] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. https://bitcoin.org/bitcoin.pdf.

[15] Peercoin—The Pioneer of Proof-of-Stake[EB/OL]. https://www.peercoin.net/read/papers/peercoin-paper.pdf.

[16] Delegated Proof of Stake Consensus [EB/OL]. https://bitshares.org/delegated-proof-of-stake-consensus/.

[17] CASTRO M, LISKOV B. Practical Byzantine fault tolerance [C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation. USENIX Association, 1999: 173-186.

[18] GENTRY C, BONEH D. A fully homomorphic encryption scheme[EB/OL]. https://crypto.stanford.edu/craig/craig-thesis.pdf.

[19] Intel Software Guard Extensions [EB/OL]. Intel. https://www.intel.com/sgx.

[20] Building a Secure System using TrustZone Technology [EB/OL]. https://documentation-service.arm.com/static/5f21279 6500e883ab8e74531.

[21] 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.

[22] SU G, YANG W, LUO Z, et al. BDTF: A Blockchain-Based Data Trading Framework with Trusted Execution Environment[C]// 2020 16th International Conference on Mobility, Sensing and Networking(MSN). IEEE, 2020: 92-97.

[23] CHEN F, WANG J, JIANG C, et al. Blockchain Based Non-repudiable IoT Data Trading: Simpler, Faster, and Cheaper[C]// IEEE INFOCOM 2022-IEEE Conference on Computer Communications. IEEE, 2022: 1958-1967.

[24] LIU Y, HAO X, REN W, et al. A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things[J]. IEEE Transactions on Computers, 2023, 72(2): 501-512.

[25] WU Z, ZHENG H, ZHANG L, et al. Privacy-friendly Blockchain Based Data Trading and Tracking[C]// 2019 5th International Conference on Big Data Computing and Communications (BIGCOM). IEEE, 2019: 240-244.

[26] JUNG T, LI X Y, HUANG W, et al. AccountTrade: Accountable protocols for big data trading against dishonest consumers [C]// IEEE INFOCOM 2017-IEEE Conference on Computer Communications. IEEE, 2017: 1-9.

[27] HE Y, ZHU H, WANG C, et al. An Accountable Data Trading Platform Based on Blockchain[C]// IEEE INFOCOM 2019—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019: 1-6.

[28] DAI W, DAI C, CHOO K K R, et al. SDTE: A Secure Blockchain-Based Data Trading Ecosystem[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 725-737.

[29] ZHENG Z, MAO W, XING Y, et al. On Designing Market Model and Pricing Mechanisms for IoT Data Exchange[J]. IEEE Transactions on Mobile Computing, 2024, 23(11): 10202-10218.

[30] LI Q, LIU Z, LI Q, et al. martFL: Enabling Utility-Driven Data Marketplace with a Robust and Verifiable Federated Learning Architecture[C]// Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2023: 1496-1510.

[31] CHEN L, KOUTRIS P, KUMAR A. Model-based Pricing for Machine Learning in a Data Marketplace [J]. arXiv: 1805.11450, 2018.

[32] SHENG D, XIAO M, LIU A, et al. CPchain: A Copyright-Preserving Crowdsourcing Data Trading Framework Based on Blockchain[C]// 2020 29th International Conference on Computer Communications and Networks (ICCCN). IEEE, 2020: 1-9.

[33] CAI C, ZHENG Y, ZHOU A, et al. Building a Secure Knowledge Marketplace Over Crowdsensed Data Streams[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2601-2616.

[34] AN B, XIAO M, LIU A, et al. Secure Crowdsensed Data Trading Based on Blockchain[J]. IEEE Transactions on Mobile Computing, 2023, 22(3): 1763-1778.

[35] DENG Q, ZUO Q, LI Z, et al. Privacy-Preserving Stable Data Trading for Unknown Market Based on Blockchain[J]. IEEE Transactions on Mobile Computing, 2025, 24(7): 5615-5631.

[36] WANG E, CAI J, YANG Y, et al. Trustworthy and Efficient Crowdsensed Data Trading on Sharding Blockchain[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3547-3561.

[37] ZHANG L, LI Y, XIAO X, et al. CrowdBuy: Privacy-friendly Image Dataset Purchasing via Crowdsourcing[C]// IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018: 2735-2743.

[38] ZHENG Z, PENG Y, WU F, et al. Trading Data in the Crowd: Profit-Driven Data Acquisition for Mobile Crowdsensing[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(2): 486-501.

[39] CHENLI C, TANG W, GOMULKA F, et al. ProvNet: Networked bi-directional blockchain for data sharing with verifiable provenance[J]. Journal of Parallel and Distributed Computing, 2022, 166: 32-44.

[40] XIONG W, XIONG L. Smart Contract Based Data Trading Mode Using Blockchain and Machine Learning[J]. IEEE Access, 2019, 7: 102331-102344.

[41] HUANG Y, ZENG Y, YE F, et al. Fair and Protected Profit Sharing for Data Trading in Pervasive Edge Computing Environments[C]// IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020: 1718-1727.

[42] ZHAO Y, GONG X, CHEN X. Privacy-Preserving Incentive Mechanisms for Truthful Data Quality in Data Crowdsourcing [J]. IEEE Transactions on Mobile Computing, 2022, 21(7): 2518-2532.

[43] ZHAO C, YANG S, MCCANN J A. On the Data Quality in Privacy-Preserving Mobile Crowdsensing Systems with Untruthful Reporting[J]. IEEE Transactions on Mobile Computing, 2021, 20(2): 647-661.

[44] ZHOU M, FANTI G, SHI E. Conan: Distributed Proofs of Compliance for Anonymous Data Collection[C]// Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 914-928.

[45] NIU C, ZHENG Z, WU F, et al. Trading Data in Good Faith: Integrating Truthfulness and Privacy Preservation in Data Markets[C]// 2017 IEEE 33rd International Conference on Data Engineering(ICDE). 2017: 223-226.

[46] ZHANG M, LI X, MIAO Y, et al. Privacy-Preserved Data Disturbance and Truthfulness Verification for Data Trading[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 5545-5560.

[47] ZHENG S, PAN L, HU D, et al. A Blockchain-Based Trading Platform for Big Data[C]// IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops(INFOCOM WKSHPS). IEEE, 2020: 991-996.

[48] CHEN W, YANG W, XIAO M, et al. LBDT: A Lightweight Blockchain-Based Data Trading Scheme in Internet of Vehicles Using Proof-of-Reputation[J]. IEEE Transactions on Mobile Computing, 2025, 24(4): 2800-2816.

[49] ZHENG Z, PENG Y, WU F, et al. ARETE: On Designing Joint Online Pricing and Reward Sharing Mechanisms for Mobile Data Markets[J]. IEEE Transactions on Mobile Computing, 2020, 19(4): 769-787.

[50] XUE S, DING H, ZHANG L, et al. Online Competitive Posted-Pricing Mechanism for Trading Time-Sensitive Valued Data [C]// 2022 8th International Conference on Big Data Computing and Communications(BigCom). IEEE, 2022: 44-53.

[51] ZHANG M, ARAFA A, HUANG J, et al. Pricing Fresh Data [J]. IEEE Journal on Selected Areas in Communications, 2021, 39(5): 1211-1225.

[52] NIU C, ZHENG Z, TANG S, et al. Making Big Money from Small Sensors: Trading Time-Series Data under Pufferfish Privacy[C]// IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019: 568-576.

[53] NIU C, ZHENG Z, WU F, et al. Online Pricing with Reserve Price Constraint for Personal Data Markets[C]// 2020 IEEE 36th International Conference on Data Engineering (ICDE). 2020: 1978-1981.

[54] LI C, LI D Y, MIKLAU G, et al. A Theory of Pricing Private Data[J]. ACM Transactions on Database Systems, 2014, 39(4): 1-28.

[55] NIU C, ZHENG Z, WU F, et al. ERATO: Trading Noisy Aggregate Statistics over Private Correlated Data[J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 33(3): 975-990.

[56] XU A, ZHENG Z, LI Q, et al. VAP: Online Data Valuation and Pricing for Machine Learning Models in Mobile Health[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 5966-5983.

[57] MAO W, ZHENG Z, WU F, et al. Online Pricing for Revenue Maximization with Unknown Time Discounting Valuations [C]// Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence. Stockholm: International Joint Conferences on Artificial Intelligence Organization, 2018: 440-446.

[58] XIAO M, LI M, ZHANG J J. Locally Differentially Private Personal Data Markets Using Contextual Dynamic Pricing Mechanism[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 5043-5055.

[59] KOUTRIS P, UPADHYAYA P, BALAZINSKA M, et al. Toward practical query pricing with QueryMarket[C]// Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2013: 613-624.

[60] LI Q, LI Z, ZHENG Z, et al. Capitalize Your Data: Optimal Selling Mechanisms for IoT Data Exchange[J]. IEEE Transactions on Mobile Computing, 2023, 22(4): 1988-2000.

[61] CHENLI C, TANG W, JUNG T. FairTrade: Efficient Atomic Exchange-based Fair Exchange Protocol for Digital Data Trading[C]// 2021 IEEE International Conference on Blockchain(Blockchain). IEEE, 2021: 38-46.

[62] TAS E N, SERES I A, ZHANG Y, et al. Atomic and Fair Data Exchange via Blockchain[C]// Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 3227-3241.

[63] UROVI V, JAIMAN V, ANGERER A, et al. LUCE: A Blockchain-based data sharing platform for monitoring data license accountability and compliance[J]. arXiv: 2202.11646, 2022.

[64] JU C, TANG W, CHENLI C, et al. Monitoring Provenance of Delegated Personal Data with Blockchain[C]// 2022 IEEE Inter-

national Conference on Blockchain(Blockchain). 2022:11-20.
[65] LOHMÖLLER J,VLAD E,DAHLMANNS M,et al. Poster: Bridging Trust Gaps: Data Usage Transparency in Federated Data Ecosystems[C]// Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. New York:ACM,2023:3582-3584.
[66] DAIDONE F,CARMINATI B,FERRARI E. Blockchain-Based Privacy Enforcement in the IoT Domain[J]. IEEE Transactions on Dependable and Secure Computing,2022,19(6):3887-3898.
[67] COHEN A,SMITH A,SWANBERG M,et al. Control,Confidentiality,and the Right to be Forgotten[C]// Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. ACM,2023:3358-3372.
[68] MEI Q,YANG M,CHEN J,et al. Expressive Data Sharing and Self-Controlled Fine-Grained Data Deletion in Cloud-Assisted IoT[J]. IEEE Transactions on Dependable and Secure Computing,2023,20(3):2625-2640.
[69] Gaia-X:A Federated Secure Data Infrastructure [EB/OL]. https://gaia-x.eu/.
[70] Decentralized Identifiers v1.0[EB/OL]. https://www.w3.org/TR/did-1.0/.
[71] Verifiable Credential 2.0[EB/OL]. https://www.w3.org/TR/vc-data-model-2.0/.

CUI Jinjia, born in 2001, postgraduate, is a member of CCF(No. U1835G). His main research interests include decentralized identity and data trading.

ZENG Chen, born in 1987, Ph.D, assistant researcher. Her main research interests include distributed systems and trust management.

（责任编辑：何杨）

凝心聚力谋新篇 笃行致远启新程——CCF 会员活动中心工作计划会在广州召开

2026 年 3 月 21—22 日，2026 年 CCF 会员活动中心工作计划会在广州召开。本次会议由 CCF 广州会员活动中心承办，华为技术有限公司作为金牌合作伙伴支持了会议。CCF 监事长金芝、CCF 秘书长唐卫清、全国 47 个城市会员活动中心代表、会员与分部工委执委等 130 余人齐聚一堂，共同回顾 2025 年会员与分部工作，共话新一年度工作，共谋发展新局。会议由 CCF 会员与分部工委主任李贝主持。

CCF 会士、秘书长唐卫清针对分部工作的目标和未来发展方向做了讲解。他强调，2026 年是 CCF 高质量发展的一年，各分部要坚守合规化运营底线，深耕会员服务，不断优化服务模式，助力学会高质量发展迈上新台阶。

CCF 会士、监事长金芝对 CCF 监事会工作进行了介绍，为会员活动中心的监委会工作梳理了思路、明确了履职方向，推动监委会监督职责规范落地。

CCF 副秘书长王新霞就学会运营管理制度与相关规范进行全面解读。

CCF 会员部富蕾就分部条例修订及活动计划的提交进行了介绍。

CCF 会员与分部工委主任李贝介绍了 2025 年会员与分部工作情况。总结了过去一年学会在会员服务、会员发展、会员活动中心建设等方面取得的成效与经验，为后续工作奠定基础。随后 2025 年获得优秀会员活动中心的代表进行了分享，结合自身运营实践，分享会员服务提质、特色活动打造、分部高效管理等方面的经验。

CCF 会士、常务理事、公益工委主任卜佳俊对 CCF 公益日及相关品牌活动做了介绍。倡导广大会员践行技术向善理念，积极参与公益事业，持续提升学会的社会影响力与公信力。

围绕“分部服务会员新模式、智能化手段的探讨”、“监委工作职责如何落实、监委与执委如何配合工作”“执行层面如何做好分部工作中的合规、如何更好激励会员“三个议题主席、秘书长、监委主席分别展开了热烈的研讨与交流。各位发言人积极献言献策，立足工作实际提出一系列针对性强、可落地的思路举措，为优化学会工作、强化会员服务凝聚了集体智慧。

通过两天的研讨与交流，进一步明确了 2026 年会员活动中心重点工作与目标，为后续工作的有序开展奠定了坚实基础。CCF 各会员活动中心将更有针对性地开展丰富的活动、持续提升会员归属感与满意度，为 CCF 高质量发展注入源源不断的强劲动力。

据 CCF 微信公众号