



北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

基于数据空间的金融数据可信流通 研究报告

北京金融科技产业联盟

2025年4月

版权声明

本报告版权属于北京金融科技产业联盟，并受法律保护。转载、编摘或利用其他方式使用本报告文字或观点的，应注明来源。违反上述声明者，将被追究相关法律责任。



编制委员会

编委会成员：

何 军 聂丽琴 徐晓剑

编写组成员：

张洪鹏 陈雨薇 郅军利 田 璞 杨 华 沈蓓瑾

徐 祎 周雍恺 戚文彬 王 琪 陈钟正 靳 晨

杨天雅 王慧敏 王 超 陈 曦 昌文婷 吴昌泉

王立冬

编 审：

黄本涛 国 钰 魏中宣

参编单位：

中信银行股份有限公司

华为技术有限公司

中国工商银行股份有限公司

中国银联股份有限公司

华控清交信息科技（北京）有限公司

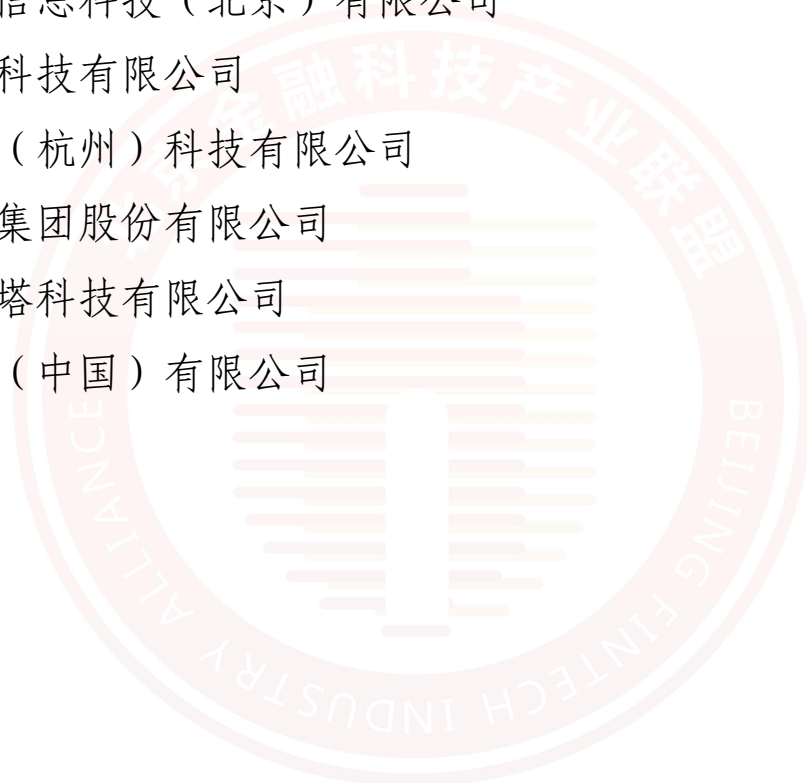
上海富数科技有限公司

蓝象智联（杭州）科技有限公司

蚂蚁科技集团股份有限公司

杭州金智塔科技有限公司

亚信科技（中国）有限公司



目 录

一、总体概述	3
(一) 发展背景	3
(二) 研究目标	5
(三) 研究方法	6
二、金融数据流通现状及挑战	8
(一) 涵义理解	8
(二) 发展现状及趋势	9
(三) 发展需求	15
(四) 面临挑战	16
三、数据空间发展	18
(一) 数据空间定义	18
(二) 国际数据空间发展及实践	19
(三) 我国数据空间发展及实践	26
四、金融数据可信流通方案研究	31
(一) 金融数据可信流通典型场景	31
(二) 金融数据可信关键角色	32
(三) 数据资源流通模式	34
(四) 金融数据可信流通方案架构	37
(五) 金融数据可信流通方案关键技术	38
五、典型场景应用与技术验证	49
(一) 中信银行总分行数据流通管控实践场景	49
(二) 工银金租数据流通场景	52
(三) 银联安全生物特征支付场景	54
(四) 金智塔小微企业智能授信风控创新实践场景	57
(五) 华为公司与伙伴数据流通实践场景	60
(六) 富数科技基于多源数据的金融风控数据空间场景	62
(七) 蚂蚁科技三农普惠金融服务场景	64
六、总结及建议	68
(一) 主要结论	68
(二) 相关建议	69

一、总体概述

（一）发展背景

数据成为新型生产要素，释放数据要素价值成为国家战略。在金融行业，随着金融数字化转型的加速，数据在金融行业中扮演的角色越来越重要。数据不仅支撑日常业务操作，还是推动创新、提升效率的关键要素。然而，伴随这种趋势，数据安全和隐私保护成为了一个重大挑战。金融机构依赖于大量数据来开展业务，包括但不限于个人信用信息、交易数据和市场分析，数据使用场景也更加多样化，数据使用从单域延伸到跨域甚至跨组织，数据泄漏、数据滥用成为主要风险。这些数据的安全管理和高效利用对于维护金融稳定、提升服务质量、增强竞争力至关重要。随着金融科技的发展，如何对数据存储、流通、使用进行安全管理，保障数据安全和隐私，成为了业界面临的一个重大挑战。

目前，数据保护领域已经发展出多种技术和方法。其中一类是常规的数据加密、数据访问控制、数据脱敏等数据安全技术，用以保障数据在存储、处理、传输过程中的安全。例如，传统基于角色的访问控制（RBAC）模型被广泛应用于 IT 系统中，以管理用户对敏感数据的访问权限。另外一类是隐私计算技术，主要包括多方安全计算、联邦学习、机密计算等，这类技术通常用于针对高敏感数据保护，实现类似“可用不可见”的效果。然而，当前业界普遍采用的上述技术受使用场景等约束，已经难以满足

数据要素流通新时代对数据保护的要求，可信数据空间为数据安全保护提供了新的选择。

数据空间理念和架构来源于国际数据空间协会（IDSA, International Data Spaces Association），其作为数据空间理念的启动者和赋能者，聚焦数据主权，提出了去中心化、数据主权可控的“数据空间”理念及架构。当前，该组织已经汇聚了来自 30 多个国家的 180 多名成员，其国际数据空间参考架构模型（IDS RAM, International Data Spaces Reference Architecture Model）已具备广泛的业界影响力。2023 年数据空间正式进入欧盟立法《数字法案》，已经成为欧盟数据战略中数字基础设施的重要组成部分。

在国内，可信数据空间已经成为实现数据资源共享共用的数据流通利用基础设施。国家数据局成立后，多次提出要积极推进数据空间等数据流通技术研发和集成应用，实现数据在不同主体间“可用不可见”“可控可计量”，布局建设数据基础设施，为数据可信、高效流通提供有力的基础支撑。2024 年 11 月，国家数据局发布《可信数据空间发展行动计划（2024—2028 年）》，明确可信数据空间发展的总体思路、目标和计划。其中，提出以建设可信可管、互联互通、价值共创的数据空间为重点，分类施策推进企业、行业、城市、个人、跨境 5 类可信数据空间建设运营，为充分释放数据要素价值，激发全社会内生动力和创新活力，构建全国一体化数据市场提供有力支撑。并明确提出到 2028 年，

可信数据空间标准体系、技术体系、生态体系、安全体系等取得突破，建成 100 个以上可信数据空间，形成一批数据空间解决方案和最佳实践，基本建成广泛互联、资源集聚、生态繁荣、价值共创、治理有序的可信数据空间网络。

在金融行业，如何引导和支持可信数据空间发展，推动金融机构积极参与可信数据空间建设，促进金融数据要素合规高效流通使用，充分释放数据要素价值，已成为一个重要课题。

(二) 研究目标

可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。

本课题围绕金融行业数据要素价值释放，研究基于可信数据空间如何促进数据资源有效共享流通。本课题围绕金融数据流通的行业现状、数据空间理念及其技术发展、金融数据可信流通场景及方案、可信数据空间验证及实践等方面开展研究，并给出结论和政策建议。具体目标包括：

- ✓ 分析金融数据流通的行业现状，识别发展趋势和潜在挑战。研究金融数据的理论和内涵，以及其在金融行业中的重要性。
- ✓ 研究可信数据空间理念和技术发展趋势，总结重点行业数据流通实践经验，分析其在金融数据流通中的应用潜力。

- ✓ 研究总结可信数据空间在金融行业落地场景，设计金融可信数据空间的方案架构，识别关键技术。
- ✓ 通过技术验证，展示金融数据可信流通方案的实际效果和可行性。
- ✓ 给出实践验证结论，提出促进金融数据可信流通的政策建议，以支持金融数据的可信流通和数据价值的释放。

(三) 研究方法

本课题采取政策分析、文献分析、定量分析、实地调研、专家座谈、集中讨论等方式进行课题研究分析。通过制定研究计划、资料研究、定期例会、现场调研、专家研讨，完成研究，给出总体路径和重要举措。必要时，联合厂商搭建数据空间技术平台开展场景验证、技术指标分析等方式配合课题工作开展。

1. 制定计划

讨论制定课题方向及研究框架，并将任务进行分解，制定调研提纲并列出具体的任务清单，明确各阶段研究工作重点。

2. 资料研究

各成员单位充分利用国内外研究机构的专业书籍、专业研究报告和数据库等研究成果，按照数据空间政策制度、数据空间技术、数据产品与服务、数据空间厂商企业、数据空间落地场景、数据空间生态等构成维度，分门别类收集、整理、研究数据空间相关案例资料。

3. 现场调研

根据需要进行现场调研，掌握数据产业发展最新动态，理论与实践保障课题输出质量。

4. 专家研讨

项目组将组织专家调研会。请与会专家为课题研究内容、阶段成果进行讨论，给出建议。

5. 实验验证

邀请数据空间相关企业、研究院所搭建验证平台与环境，组织金融等行业机构进行方案功能验证和测试等，以获得数据空间技术第一手资料，为研究报告内容提供依据。

6. 编撰报告

根据研究团队成员在资料研究、现场调研、专家研讨等工作成果，编写报告并组织汇报。

二、金融数据流通现状及挑战

（一）涵义理解

金融数据的可信流通，是推动金融行业数字化转型的重要保障和必然趋势。在中共中央、国务院《数字中国建设整体布局规划》及《“数据要素×”三年行动计划（2024-2026年）》政策的指引下，金融作为重点领域，将加速推动数字技术创新应用，提升服务水平。

金融行业作为信息化建设起步较早、成熟度较高的行业之一，长期以来积累了庞大的数据量和丰富的数据类型，金融数据不仅具备一般数据的特性，更包含了国民个人信息、企业资金流转、社会经济活动等内容，在业务运营中涉及大量的客户信息、交易数据和市场信息。随着数据治理体系的完善，使金融数据具有体量大、质量好、价值高，敏感性强等特点，金融数据融合应用具备了天然优势。

金融数据应用场景丰富，涵盖客户风险评估、反欺诈、精准营销、智能投顾等多个领域。然而，金融行业的数据具有高度敏感性，且其行业具备金融强监管属性，如何使金融数据在严格遵守《中华人民共和国数据安全法》、《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《银行保险机构数据安全管理办法》等法律法规的前提下，合法合规地释放数据价值，避免数据成为“孤岛”成为当下行业探讨热题。

金融数据的可信流通，实质上是在保障数据安全与隐私的前提下，探索数据价值最大化的过程。这要求金融行业不仅要加强内部数据治理，提升数据质量与安全防护能力，还需与外部监管机构、技术服务商等紧密合作，共同构建数据流通的信任机制与合规框架。通过技术创新保护数据主体的权益，促进数据的合规共享与价值释放。

（二）发展现状及趋势

1. 政策指引

（1）美国数据强国战略：战略性的安全防护、制度化的数据开放和市场化的数据交易

美国正通过一系列战略部署和技术革新，不断强化其数据治理体系，推动数据资源的防护、共享、开放和商业化流通。美国的数据战略不仅聚焦于安全防护，还积极促进数据的开放利用和市场培育，展现出其在数据资源流通技术发展上的决心和前瞻性。

一是数据安全防护体系的强化。美国通过发布零信任战略，转变传统的网络安全观念，以数据为中心构建安全攻防体系。同时，成立网络空间与数字政策局，强化政府治理能力，并建设高安全基础设施，确保重要数据的安全。

二是政府数据开放的深化。美国实施《开放政府数据法案》，推动非敏感数据的最大限度开放，并通过 Data.gov 等统一数据开放平台，向社会提供了大量的政府数据集，促进了数据的开放利用。

三是数据商业化流通交易的推进。美国培育成熟的数据经纪市场，提供数据集查询和交易撮合服务，形成了多元化的数据交易模式。同时，通过《数据经纪人责任制与透明法案》等政策法规，加强了行业监管和自律，提高了数据交易的透明度和规范性。

美国在数据资源流通技术领域的发展现状和趋势表现为战略性的安全防护、制度化的数据开放和市场化的数据交易。通过这一系列措施，美国正不断巩固其在全球数据治理和流通技术领域的领先地位，为数据驱动的创新和经济增长提供坚实的基础。

（2）欧盟构建数字堡垒：制定全面的制度规则、建立统一的基础设施和推动建设行业数据空间

欧盟正致力于构建一个统一的数据市场，通过制定全面的制度规则、建立统一的基础设施和推动行业数据空间的建设，以增强其数字产业的实力和在数字时代的全球竞争力。欧盟的数据资源流通技术发展现状和趋势体现了其对数据安全与隐私保护的坚定承诺，以及对数据共享和流通的积极推动。

一是建立数据安全“欧盟规则”。欧盟通过《欧洲数据战略》和《2030 数字罗盘》等战略文件，确立了数据治理的框架，并以 GDPR 为核心，建立了严格的隐私保护法规体系，同时制定《数据法案》和《数据治理法案》，推动数据的可信共享。

二是构建统一基础设施。欧盟推进 Gaia-X 体系的建设，旨在实现数据和服务的自由、安全整合和共享，采用创新的“1+2+3”

架构，促进各类主体的参与，并辅以量子通信基础设施 EuroQCI，增强数据传输和存储的安全性。

三是搭建行业数据空间。以 Gaia-X 为支撑，欧盟在关键行业领域打造公共数据空间，促进行业内数据的流通和创新应用，同时通过数据空间连接各个数据源和使用者，形成一个开放、安全、可信的数据共享环境。

欧盟在数据资源流通技术领域的发展现状和趋势表现为对数据安全与隐私保护的高标准要求，对统一基础设施的创新建设，以及对行业数据空间的积极推进。这些措施不仅加强了欧盟的数据治理能力，也为数字经济的发展和 innovation 提供了坚实的基础，推动了其数字化转型的进程。

（3）日本：构建安全与创新并重的数据流通新纪元

日本正通过其国家综合数据战略，积极塑造一个既注重个人信息安全又促进数据驱动创新的数据资源流通环境。该战略以数据安全保护为基础，统一数据生态架构为支撑，数据银行模式为创新点，展现了日本在数据资源流通技术发展上的战略布局和未来趋势。

日本在个人信息保护方面虽然起步较晚，但通过《个人信息保护法》的实施与修订，不断强化对人脸识别信息和数据跨境传输的监管，体现了其在保护个人信息方面的坚定立场和适应数字化发展需求的灵活性。同时，日本通过构建全国性的数据共享生

态架构，明确了数据产业链各环节的整合作用和各类数据参与者的角色，旨在解决数据分散治理的难题。

此外，日本在培育数据银行方面采取了创新措施，以信托机构为起点，推动数据信托服务的发展，进而促进数据交易市场的成熟，为日本数字信任体系的建设奠定了基础。通过“数据流通环境整備研究会”的工作，日本政府正致力于通过官民合作，实现跨领域数据流通，以数据银行为基础，推动数字社会的发展和数据的高效利用。

日本的国家综合数据战略不仅反映了其对数据安全和个人信息保护的重视，也显示了其在构建数据生态和推动数据流通方面的前瞻性和创新力，预示着日本在数据资源流通技术领域将迎来更加安全、高效、协同的发展未来。

（4）中国：将可信数据空间视为实现数据资源共享共用的数据流通利用基础设施

为促进我国数字经济健康发展，确保数据资源作为国家战略性资产的有效流通，我国正积极应对数据流通面临的法律法规滞后、技术安全风险等多项挑战。为此，国家高度重视数据安全保护体系建设，不断加强相关法律法规的制定和完善，旨在打造一个全面的数据安全保护框架。

当前中国数据要素流通产业发展已经完成顶层设计，各地都在积极开展创新实践，发展新型数据产业，包括数据交易所、行业数据空间、数据跨境流通等。在激发数据价值发挥的同时，中

国数据安全立法进程在加快完善。《中华人民共和国数据安全法》（2021）、《中华人民共和国个人信息保护法》（2021）相继落地施行，与《中华人民共和国网络安全法》（2017）共同构成了数据安全治理法律领域的“三驾马车”。在法律框架下，各地方性数据安全条例政策不断涌现，以数据流通关键环节和主体为中心，明确数据流通安全规则。

国家数据局发布《可信数据空间发展行动计划（2024—2028年）》，将可信数据空间定义为实现数据资源共享共用的数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。计划提出，到2028年，可信数据空间标准体系、技术体系、生态体系、安全体系等取得突破，建成100个以上可信数据空间，形成一批数据空间解决方案和最佳实践，基本建成广泛互联、资源集聚、生态繁荣、价值共创、治理有序的可信数据空间网络，各领域数据开发开放和流通使用水平显著提升，初步形成与我国经济社会发展水平相适应的数据生态体系。

2. 行业规划

金融行业正处于数字化转型的重要阶段，数据作为新型生产要素，对推动经济社会的高质量发展具有重要意义。安全可控的金融数据流通共享是释放数据价值的关键前提，然而隐私泄露、数据滥用等安全风险仍制约着数据要素的深度应用。

从金融行业来看，人民银行及相关机构颁布的一系列金融行业数据安全规范，支撑起金融数据安全的体系框架，为金融数据能力和安全建设提供了依据和指引。2021年人民银行印发《金融科技发展规划（2022—2025年）》，明确指出在保障安全和隐私前提下，推动数据有序共享与综合应用，激活数据潜能，有力提升金融服务质效。

2024年11月，中国人民银行等七部门联合印发《推动数字金融高质量发展行动方案》，提出夯实数据治理与融合应用能力基础，加强数据资产积累，全面整合内外部数据，实现全域数据的统一管理、融合共享。强化数据挖掘分析和数据可视化能力建设，形成对业务经营、风险管理、内部控制的基础数据支撑。推进金融领域“数据要素×”试点，运用大数据、隐私计算等科技手段，融合应用多维数据，优化金融产品和风控模型，提升金融服务和风险管控质效。行动方案同时提到，要培育高质量金融数据市场，加强金融领域数据资源开发利用，探索开展金融行业数据空间建设。在依法安全合规前提下，支持客户识别、信贷审批、风险核查等多维数据在金融机构间共享共用和高效流通，建立健全数据安全可信共享体系。

金融机构作为数据要素市场的核心参与主体，在营销获客、风险管控等业务场景中深度依赖内外部数据资源。随着国家法律法规和金融行业相关规范、指南的陆续出台和落实完善，金融行业数据安全保护及合规审查的要求日趋严格。需要强调的是，数

据安全治理并非追求绝对化管控，而应构建隐私保护、安全可控与价值释放的动态平衡机制。在满足合规要求的前提下，坚持“敏感数据安全优先，非敏感数据效率优先”原则，促进数据要素流通，提升数据要素流通效能，充分激活数据资产价值。

（三）发展需求

1. 完善数据全流程合规治理与监管体系。为了保障金融数据的安全流通，需着眼数据全生命周期，建设依法合规、高效贯通的数据流通规则标准体系，覆盖采集、整理、聚合、存储、分析、流转等环节。同时，严格遵守相关法律法规，确保数据来源合法、交易主体资质明晰，并兼顾安全保护。监管机构应加强对金融机构数据安全管理的监督和指导，利用技术手段提高监管效能，确保市场主体在法律法规约束下开展数据资源处理及交易活动，实现数据高效流动与数据安全保护的平衡。

2. 加强金融数据分类分级保护与流通。金融数据作为关键生产要素，其使用场景和用途用量千差万别。随着数据流通范围、期限及使用场景的变化，金融数据的安全保护和流通模式需相应调整。数据的分类分级授权使用是保障金融数据安全流通的关键。针对不同类别和级别，应建立差异化的授权使用规范，明确数据资源持有者、数据加工使用者、数据产品经营者等各方在数据流通过程中的权利与义务，规范数据交易行为，健全产权保护制度。

3. 构建完善市场生态。为了推动金融数据流通的健康发展，需要构建完善的市场生态和流通规则。规范数据流通行为、打击

数据泄露和滥用等违法行为。同时，推动场内化、标准化的大型金融数据交易生态的形成，拓宽数据流通渠道和种类。

（四）面临挑战

金融数据的流通与共享对于提升金融机构的经营效率、客户服务水平以及实现业务创新和产品创新具有重要意义。然而，金融数据流通也面临着诸多挑战，需要业界各方共同努力加以解决。

1. 严法律带来强要求。国家通过《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》等法律法规，对金融数据的采集、使用、存储和传输设定了高标准，确保了数据的合规性和安全性。然而，这些法律法规的实施增加了金融机构的管理成本和合规难度。同时，行业监管机构如银保监会、证监会等不断提升监管力度，发布了一系列数据安全管理办法，要求金融机构建立健全的数据安全管理体系，进一步提升了金融机构的管理成本。

2. 高标准带来严要求。随着金融数据的重要性日益凸显，业内提出了多项数据安全治理标准，如《金融业数据能力建设指引》、《金融数据安全数据生命周期安全规范》等。这些标准虽然有效完善了安全保障体系，但也提高了金融机构的管理成本，并增加了合规难度。金融机构需要投入更多精力，从而限制了金融数据的有效流通。

3. 风险防控加剧封闭性。金融机构对数据的高敏感、高价值认识导致其“不愿流通”、“不敢流通”以及“不会流通”，使

得金融数据被封闭在“孤岛”中，限制了金融数据在市场中的流通。另一方面，数据泄露和滥用等问题的频发，加剧了金融机构对数据流通的谨慎态度，为了避免潜在的法律风险和声誉损失，金融机构在数据流通方面采取了更加严格的管控措施，这进一步加剧了数据的封闭性，使得数据流通的难度进一步加大。



三、数据空间发展

(一) 数据空间定义

早在 2016 年前后，德国弗劳恩霍夫协会提出了“数据空间”这一概念，随后成立了工业数据空间协会（Industrial Data Space Association, IDSA）。随着数据空间理论架构和实践的不断探索和完善，这一理念逐步从专注工业领域的“工业数据空间”（Industrial Data Space）升级为覆盖各个行业的“国际数据空间”（International Data Space），跨越国界，连接全球。2022 年，中国信息通信研究院两化所在国际数据空间参考架构的基础上，携手多家机构和厂商，结合本土实践，提出了“可信数据空间”（Trusted Data Matrix, TDM）的概念。TDM 不仅继承了 IDS 的核心理念，即在数据主权原则下构建安全、受保护的数据流通环境，还进一步强化了数据流通的安全性、透明度和效率。TDM 通过体系化的技术安排，如数据使用控制、数字身份认证、数据合约数字化等，确保数据流通协议的确认、履行和维护，解决了数据提供方、使用方、服务方、监管方等主体间的安全与信任问题。数据空间概念提出情况及发展情况详见表 1。

表 1 数据空间概念提出及发展情况

概念名称	概念提出	定义	发展现状
国际数据空间 (IDS)	2016 年 德国弗劳恩霍夫协会	在数据主权原则下，通过安全数据交换和可信数据共享的政策和机制 连接不同公有云平台的体系结构 ，旨在构建受保护的数据生态系统。	从制造业起步逐渐覆盖其他行业：共计数据空间 134 个，其中公共数据空间 17 个，行业数据空间 46 个，测试床 71 个。

可信数据空间 (TDM)	2022年3月 信通院两化所	在现有信息网络上搭建数据集聚、共享、流通和应用的 分布式关键数据基础设施 ，通过体系化的技术安排确保数据流通协议的确认、履行和维护，解决数据提供方、使用方、服务方、监管方等主体间的安全与信任问题。	发布及牵头多项规范标准： 《可信工业数据空间系统架构 1.0 白皮书》、 《可信数据空间系统测试规范》 《可信数据空间互联互通技术规范》 IEEE P3158《可信数据空间系统架构国际标准》 ITU-T SG20 TR《数据共享控制模型》
-----------------	-------------------	---	--

在国家数据局的发文中，对可信数据空间给出如下定义：

可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的数据流通利用基础设施，是数据价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。

可信数据空间具备数据可信管控、资源交互、价值创造等关键能力。可信数据空间的核心价值在于通过加密技术、访问控制等手段，确保数据在传输、存储、处理各环节中的安全，防止数据泄露与篡改，同时采用隐私计算、数据脱敏等技术，实现数据“可用不可见”，保护个人隐私与商业机密。

（二）国际数据空间发展及实践

国际数据空间（IDS）是一个以促进安全可信业务生态系统中的标准化数据交换和数据链接为目标的研究项目，旨在建立一个去中心化的数据共享平台，允许不同规模和领域的独立合作伙伴信任外部各方如何管理其数据，同时促进合作构建创新数据服务。

IDS 的核心是创建一个安全的数据环境，其中数据所有者可以定义对其数据的使用限制，并且这些限制可以在数据共享之前被数据消费者接受。这种以数据为中心的交换方式，不仅保障了数据主权，还通过标准化互操作性，支持了不同数据生态系统之间的数据交换。

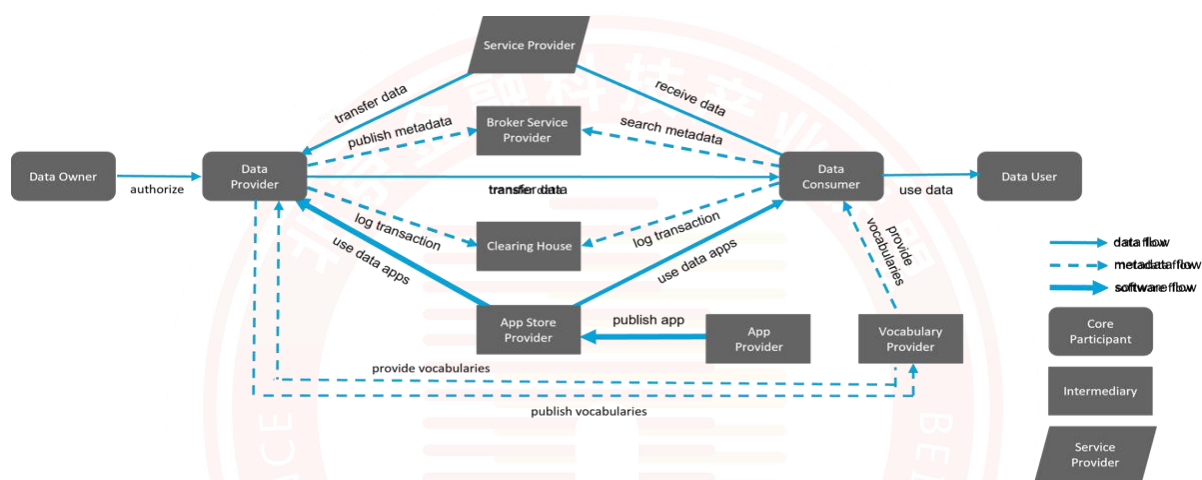


图1 国际数据空间参与角色

如图所示，IDS 参与角色包含：

- ✓ 核心参与者包含数据提供方、数据需求方；
- ✓ 中间机构包含身份认证机构、数据中介、应用商店、词汇中介、票据交换所等；
- ✓ 软件开发者包含应用开发者和连接器开发者；
- ✓ 空间治理机构包含认证机构和评估设施以及标准化组织。

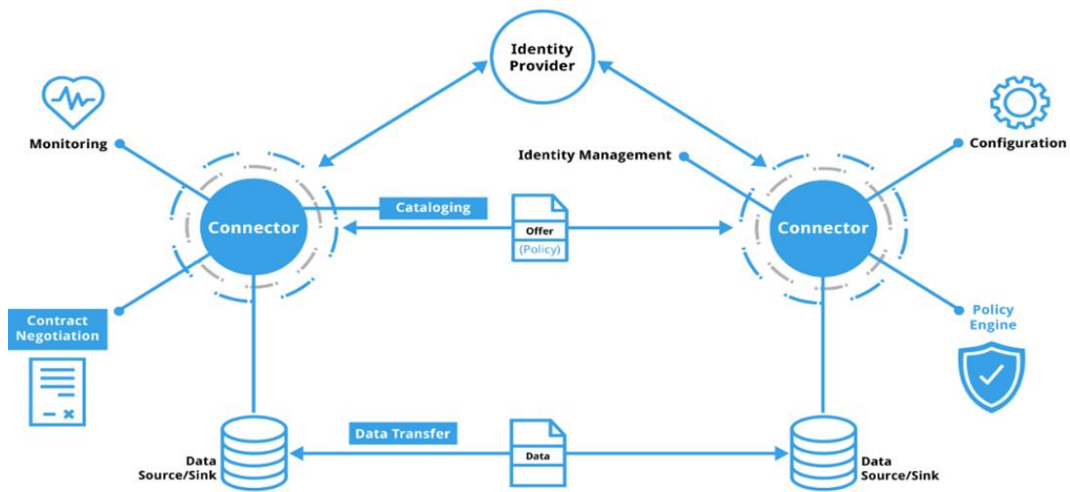


图2 国际数据空间核心组件

IDS 核心组件包含：

- ✓ 连接器（Connector）是数据空间中联通数据与服务的网关，也为各应用程序（App）和软件提供可信任的运行环境。
- ✓ 身份提供组件（Identity Provider）创建、维护和管理一个数据空间内参与者的身份信息及其有效期。
- ✓ 合约磋商组件（Contract Negotiation）提供包含创建和协商在内的合约管理服务。
- ✓ 策略引擎组件（Policy Engine）负责按数据合约条款执行数据使用策略。
- ✓ 策略监测组件（Monitoring）负责跟踪并反馈策略执行情况。

在实践方面，IDS 倡议已被多个国际研究机构和工业企业所接受，他们共同努力建立一个跨越国界的数据共享生态系统。2020 年 2 月，欧盟委员会发布“欧洲数据战略”，首次提出构

建九大类数据空间（后增至 17 类），例如欧洲健康数据空间（European Health DataSpace），并提出“单一数据市场”理念，强调巩固“数据主权”。随后，英国推出国家数字孪生体原则形成数据空间实施理念，德国联盟协会构建参考架构，推动数据空间技术标准落地，日本以互联产业开放框架为核心推动分布式数据共享模式发展。

1. 欧盟委员会发布《欧洲数据战略》形成工业数据空间顶层规划

2020 年 2 月，欧盟委员会发布《欧洲数据战略》明确提出创建一个单一的欧洲数据空间-一个真正的单一数据市场，向来自全球的数据开放。其中围绕数据主权和开放共享的立法将成为工业数据空间建设的主要抓手，在 2020 年第四季度针对数据开放及使用方式、行业内及跨行业的数据互操作性等开展立法研究。在 202 年第四季度的数据法案中解决共同生成的工业数据使用权问题，并探索企业愿意共享数据和促进数据生成方面的商业模式。另一方面，基础设施建设将成为工业数据空间建设的主要推进手段，将加强对云基础设施的投资，投资时间跨度将从 2021 年到 2027 年，投资金额将达到 40 亿到 60 亿欧元。

基于研究学界对“欧洲开放科学云”不断增长的经验，欧盟委员会将支持建立以下九个欧洲公共数据空间：

欧洲工业（制造业）公共数据空间，以支持欧盟工业的竞争能力和表现，允许挖掘制造业的非个人数据使用的潜在价值（2027 年预计达 1.5 万亿欧元）。

欧洲绿色协议公共数据空间，通过挖掘数据的巨大潜力，支持绿色协议在以下几个方面的优先行动，包括气候变化、循环经济、零污染、生物多样性、森林滥伐、合规保证等。“绿色数据为人”（GreenData4all）和“拯救地球”（地球数字孪生）两项计划将涉及具体措施部署。

欧洲出行数据公共空间，确立欧洲在智能交通系统发展领域的领先地位，既包括车联网，也包括其他交通工具的数据联网。此项数据空间将方便当前和未来交通和出行数据库的数据获取、归集和共享。

欧洲健康数据公共空间，这一方面对预防、诊断、治疗疾病方面的领先非常必要，另一方面也是作出有依据、基于证据的医疗决策以促进医疗保健系统数据的可获得性、有效性和可持续性的必要措施。

欧洲金融数据公共空间，通过加强数据共享、创新、提高市场透明度、促进可持续发展刺激金融，为欧洲商业和更加一体化的市场提供金融准入。

欧洲能源数据公共空间，采用以客户为中心的安全和令人信赖的方式，更有力地推动数据获取和跨行业共享，因为这将促进技术创新和支持能源系统的去碳化进程。

欧洲农业数据公共空间，通过处理和分析农业生产及其他数据来强化农业部门的可持续产能和竞争力，使得能在农场级别上实现精细和定制的生产方法的应用。

欧洲公共管理数据公共空间，一是在欧盟和成员国层面提高公共支出、支出质量、反腐败的透明度和问责力度，二是满足执法需求、保障欧盟法律有效执行和确保技术创新，涉及“监管科技”、“备案科技”和“法律科技”等支持从业人员和公共利益服务的应用。

欧洲技能数据公共空间，旨在减少教育培训系统与人力市场需求方面的技能错配。

2. 英国推出《国家数字孪生体原则》形成数据空间实施理念

英国数字建造中心发布了《英国国家数字孪生体原则》，旨在通过颁布国家级的数字孪生体构建原则，统一各个独立行业开发数字孪生体的标准，达成孪生体之间高效、安全的数据共享，释放出数据资源整合的价值，优化传统英国在社会、经济、环境方面的发展模式。

原则着重指出，数据空间必须依据合理的质量数据来进行构建，确保各参与主体能够依照一定的规范展开数据的集成处理，保证参与共享的数据资源质量拥有高可靠性。将建立基于行业实践的数据开放接口当作主要的切入点。《原则》在遵循整体安全原则的基础之上，借助开放式应用程序编程接口（API）尽可能

地开放数据，并且支持运用一种通用的方法提高各数字孪生体之间数据集的互操作性。

3. 德国联盟协会构建参考架构，推动数据空间技术标准落地

2016年，德国工业4.0开启了工业数据空间子项目，此项目由德国弗劳恩霍夫应用研究促进协会负责推动。该项目旨在构建一个值得信赖的数据交易共享网络，为此建立了一整套工业数据空间参考架构模型。其综合考虑了数据使用者、数据提供者、认证中心、中间代理商等十种主体在数据共享流通中所发挥的作用，精心设计了涵盖数据主权、数据交易、数据定价等内容的完整商业模式、交易流程以及软件开发规范，并且为各个主体提供了标准化的软件接口“连接器”，从技术解决方案的层面保障了数据安全交换以及主权的完整性。后续，由工业数据空间项目衍生成立了国际数据空间协会，所涉及的数据范畴从工业制造延伸至整个数字经济领域。截至2024年，德国有23个案例发布在Data Spaces Radar上，占据案例总量的首位，充分反映了德国在全球数据空间建设方面的领先态势。

4. 日本工业价值链协会以互联产业开放框架为核心推动分布式数据共享模式发展

2019年，日本工业价值链协会发布了《互联产业开放框架》（以下简称“CIOF”），这一举措意味着日本工业数据空间布局正式拉开帷幕。与德国工业数据空间项目有所不同，日本模式聚焦于互联产业开放框架，规避数据主权问题，运用分布式平台的

方式推动数据共享。其通过数据流通合同的形式，对工业数据的使用许可范围、供需双方的权利和义务，以及数据使用过程中衍生出的其他问题予以明确界定。基于分布式平台，由数据的提供方和使用方直接进行对接，探索并形成双方均认可的数据字典，以此保障数据流通的独立性。与此同时，现场数据和相关数据资产由 CIOF 系统直接进行管理，并借助区块链技术确保数据按需加密和传输，从而有效防止数据伪造。当下，日本工业价值链协会正在积极推进一项涵盖日本 100 强企业的工业数据共享项目，将运用区块链技术来降低数据泄露的风险以及运营成本。

（三）我国数据空间发展及实践

中国不仅是制造大国，也是数据资源与应用方面的大国。预计到 2025 年，中国的数据总量会攀升至世界首位，在全球的占比有望超出 27%，进而成为数据规模最大、数据类型最为丰富的国家之一。当前我国的数据共享流通尚处在起始阶段，需要参考发达国家顶层设计、交易共享等方面的先进实践经验基础上，构筑契合我国发展现状的数据共享流通架构，从而更进一步推动数据要素的市场化进程。

我国在数据空间的发展和实践方面，也已经展现出了积极战略布局。在国家层面，数据空间被视为支撑经济社会数字化转型的关键新型基础设施。通过整合现有的政务云平台、数据资源平台和信息共享平台等，结合《“数据要素×”三年行动计划》的

实施，我国正加快金融、工业、农业、商贸、交通等多个行业的数据空间基础设施建设。

在区域层面，我国正推动构建以中心城市为核心的区域数据枢纽，如北京、上海、广州等，这些枢纽将覆盖不同的地理区域，形成跨层级、跨地域的数据流通架构。同时也在鼓励不同行业和区域数据空间的互联互通，构建起全国一体化的数据生产流通平台。

在政策和标准制定方面，我国也在积极推动。例如，工信部印发的《工业大数据发展指导意见》和《工业互联网创新发展三年行动计划》，都强调了探索建立工业数据空间、推动数据开放共享的重要性。同时，中国信息通信研究院发布的《可信工业数据空间系统架构》白皮书，为可信工业数据空间的初步架构和标准体系提供了指导。

总体来看，我国数据空间的发展和实践正处在一个快速起步推进的阶段，不仅在基础设施建设方面取得了成效，而且在政策支持、技术应用和标准制定等方面也展现出了清晰的方向。随着技术的不断成熟和应用场景的不断拓展，数据空间有望成为推动我国数字经济发展的关键力量。

1. 相关政策密集出台，引导数据有序利用

在 2017 年，国家《“十三五”先进制造技术领域科技创新专项规划》明确指明，要致力于研发企业智慧数据空间构建技术系统，并开展平台的典型应用。2020 年，《关于工业大数据发

展的指导意见》进一步强调，将通过探寻建立工业数据空间、加速区块链等技术于数据流通中的应用、健全工业大数据资产价值评估体系等途径，从技术手段、定价机制、交易规则等众多方面发力，激发工业数据市场的活力，推动数据的市场化配置。2021年11月，《“十四五”大数据产业发展规划》清晰提出要“率先于工业等领域构建安全可信的数据共享空间”。

2024年11月，国家数据局发布《可信数据空间发展行动计划（2024—2028年）》，将可信数据空间发展带到新阶段。其中提出以建设可信可管、互联互通、价值共创的数据空间为重点，分类施策推进企业、行业、城市、个人、跨境可信数据空间建设运营，为充分释放数据要素价值，激发全社会内生动力和创新活力，构建全国一体化数据市场提供有力支撑。并明确到2028年，可信数据空间标准体系、技术体系、生态体系、安全体系等取得突破，建成100个以上可信数据空间，形成一批数据空间解决方案和最佳实践，基本建成广泛互联、资源集聚、生态繁荣、价值共创、治理有序的可信数据空间网络。

2. 各区域及行业积极开展数据空间探索实践

2020年，北京印发《关于推进北京市金融公共数据专区建设的意见》，大力推动金融公共数据专区的建设。通过汇集多维数据，有效提升了金融服务的效率，为普惠金融的发展以及智慧城市的建设提供了有力支持。该专区主要聚焦于特定的领域或场景，推动政企数据的融合，提升数据开放的程度，促进数据资源

在社会层面的利用。其运营模式由市经信部门进行统筹协调，授权市属国有企业开展专业化运营，以此确保数据使用的公益性以及技术的安全性。此外，在北京的基础设施建设、技术应用层面，充分利用区块链隐私计算等技术，实现数据可用不可见，推动专区数据流通的科技创新。2023年11月，北京数据基础制度先行区启动运行，提出到2030年，完全建成北京数据基础制度先行区，打造数据要素市场化配置的政策高地、可信空间和数据工场。

2023年，深圳数字交易所联合多方成功达成了国内首笔基于数据空间技术的场内数据业务合作，塑造了我国首个在智能制造领域的可信数据空间应用范例。这一具有里程碑意义的事件，象征着可信数据空间技术在国产商业领域实现了实质性的落地。这不仅彰显了可信数据空间技术在国产商业化方向的可行性，还为行业数据要素的高效流通、合规使用提供了全新的解决办法。该案例运用自主可控的可信数据空间架构，通过构建产业数据要素的可信流通体系，达成了数据的安全流转和可信共享，切实解决了数据协同、监控和溯源的难题，为产业数据要素的交易给予了坚实的技术支撑，为数据驱动的实体经济发展注入了崭新的动力。

3. 围绕可信工业数据空间开展生态建设

由中国信息通信研究院联合多家单位在2021年发起成立可信工业数据空间生态链（TDMC），联盟成员单位包括国有企业、工业制造企业、互联网企业、技术公司、科研院校、数据交易服务机构等。联盟立足于搭建工业数据要素可信流通、共享的生态

合作与促进平台,开展可信工业数据空间技术、标准和产业研究,共同探索工业数据要素可信流通的新模式和新机制,推动技术落地应用、开展试点示范,推进可信工业数据空间发展,服务工业企业,为实施工业互联网相关政策提供必要支撑。自成立以来,联盟共发布《可信工业数据空间系统架构 1.0》、《可信工业数据流通关键技术研究报告》、《可信工业数据流通应用案例集》等成果,并推动 ITU、IEEE 等国内外标准组织中的技术标准研制工作,首个 IEEE 数据空间标准 IEEE 3158-2024《Standard for Trusted Data Matrix System Architecture》已于 2024 年 6 月 6 日发布。

2021 年中国工业互联网研究院联合相关部属事业单位、科研院所、工业互联网平台企业共同发起成立工业互联网平台创新合作中心,同年海尔卡奥斯发起工业数据空间技术组。技术组以促进工业数据空间行业高质量发展为目标,旨在推动共建统一标准下的可信数据生态系统,促进数据流动与数据共享,建设安全、开放、合作、有序的工业数据空间命运共同体,形成多个面向不同领域、行业的工业数据空间试点。技术组旨在促进工业数据空间安全与治理领域的技术研究及应用,提升工业企业数据治理能力,助力以数据为关键要素的数字经济发展。技术组已发布《工业数据空间场景案例集》等成果。

四、金融数据可信流通方案研究

(一) 金融数据可信流通典型场景

数据在银行业等金融行业都得到广泛的应用，数据流通价值体现在能够有效提升业务效能、优化资源配置、强化风险控制能力、促进业务创新发展。应用场景包括信贷风险评估、交易欺诈识别、精准营销、供应链金融、运营优化、智能投顾、量化投研、风险定价、金融反欺诈、反洗钱等多方面。例如，银行机构与运营商数据实现联合建模及可信数据流通，建立手机银行登录行为异常识别模型和电信反欺诈服务，极大提升银行电信反欺诈的效果和效率。

1. 赋能创新产品，精准贴合需求

由于数据壁垒能够在金融数据可信流通中得到解决，金融机构能够更全面进行风险评估，产品设计完全基于客户需求，真正向客户提供个性化金融产品，并把个性化产品的营销流程嵌入合作平台场景中。

2. 融合多方数据，提升营销效率

在金融数据可信流通架构下，金融机构数据、公共数据实现融合，避免公共数据涉及的用户数据及外部数据交互过程中出现隐私泄露风险。金融机构可提前对客户进行业务预核实，将平台算法自动与客户信息库进行匹配，并通过建模将符合初筛条件的对象信息和公共数据通过金融数据可信流通方式向营销部门进行反馈，快速匹配营销策略，提高营销效率。

3. 预测用户行为，实现营销预判

借助金融数据可信流通方式，金融机构将合规收集更多维度数据，以此来预测客户行为，推算用户购买能力、风险偏好、授信额度、承保概率等因素，并对用户进行有针对性触达。

4. 提升业务流程，优化客户体验

保险公司可以借助金融数据可信流通方式实现智慧理赔，客户进行理赔时，寿险公司通过隐私计算平台发送理赔数据请求，医疗机构、社保局、税务局分别将患者的就诊数据、结算单据、医保结算、电子发票等通过隐私计算节点同寿险公司理赔数据进行计算，全面提升赔案处理效能。

5. 全景化角度下的大数据风控升级

通过采用金融数据可信流通，在利用多维度的数据为客户做更精准的画像同时，可结合其他新兴技术有效解决“数据隐私”和“数据孤岛”问题，全景化提升金融机构的风控能力。

金融数据可信流通在提升金融服务效率和体验、降低金融风险 and 成本、创新金融产品和模式等方面有着显著作用，在金融领域的应用场景具有较大空间，随着金融数据可信流通与各个金融场景的深度融合，将进一步提升金融服务质效，为新质生产力“蓄势赋能”。

（二）金融数据可信关键角色

数据资源流通是一个复杂的多方参与和协作的过程，明确数据流通参与方角色职责对于构建有效的数据流通体系至关重要。从业务视角看，可信数据空间主要包含以下利益相关方：

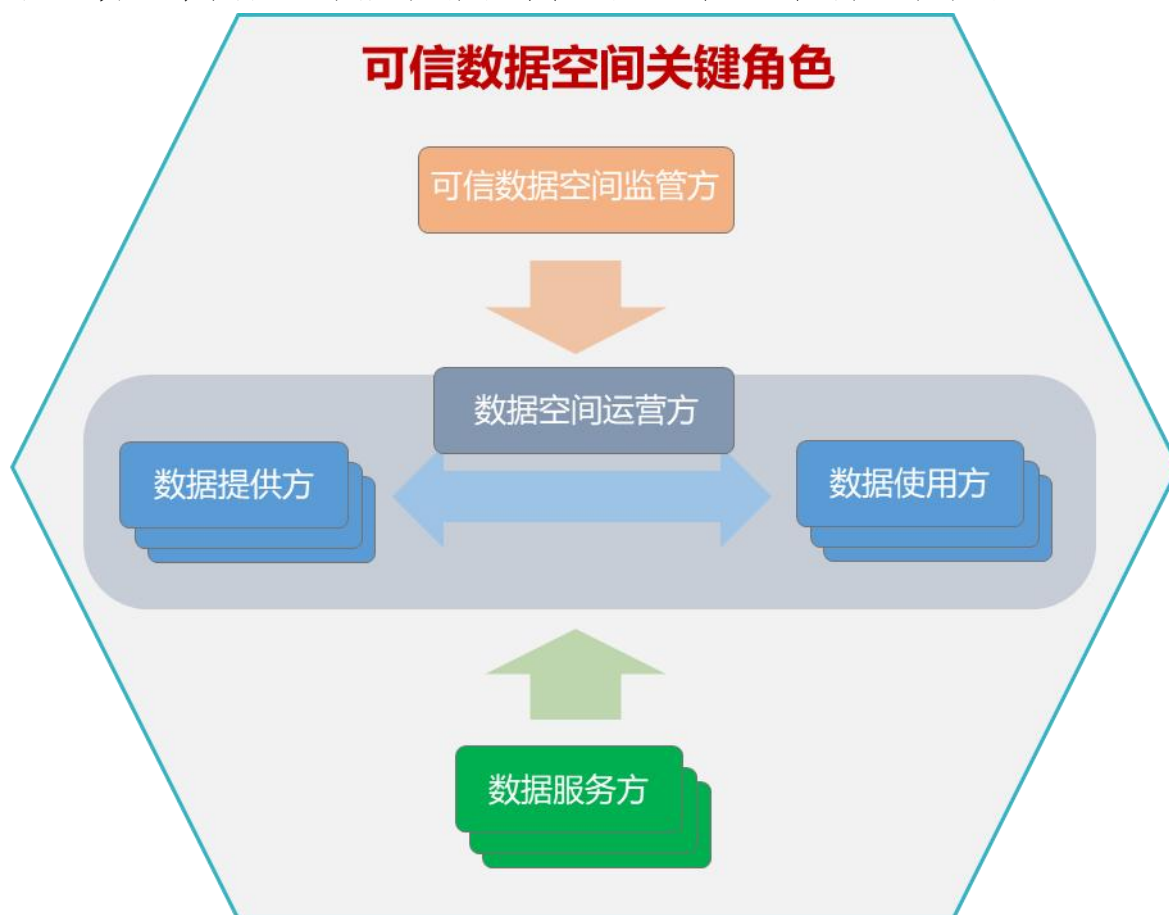


图3 可信数据空间关键角色

1. 数据提供方：提供在可信数据空间中流通交易的数据，并对数据使用策略进行授权；
2. 数据使用方：在可信数据空间中提出流通交易的需求，并按数据使用策略接收并使用数据；

3. 数据空间运营方：建立合规、互信、安全的技术体系，搭建和维护数据交易和流通平台，制定数据交易规则、流程、定价机制，促进数据供需双方的对接和交易流通，释放数据价值。

4. 数据服务方：支撑可信数据空间提供流通交易、可信合规、增值服务、基础设施等各类活动，为各利益相关方提供相应的中间服务，其可由数据交易所、数据商以及第三方专业服务机构等担任，辅助可信数据空间中各类业务的开展；

5. 可信数据空间监管方：在可信数据空间中，对各利益相关方的行为进行监督管理，保障国家数据安全和各参与方权益，推动数据要素市场健康发展。

在可信数据空间中，这些角色相互协作、相互制约，共同推动数据流通利用。数据提供方和数据使用方可直接开展数据流通交易，也可通过数据交易所等中间服务方进行集中流通交易。在实际操作中，角色之间关系并非一成不变，一个组织可能承担多个角色，并且随着市场发展还可能出现新的角色。

（三）数据资源流通模式

金融数据资源流通应用场景丰富，导致数据资源流通模式多样，本研究根据实际应用场景提炼出点对点流通、点对多流通、多点互联流通三种流通模式，可基本覆盖数据资源流通场景。用户根据具体情况选择合适的流通模式，或者同时采用多种流通模式，以实现数据资源最优流通模式选择。

模式一:点对点模式。该模式在数据共享流通场景中最为常见(如图 4 所示)。以银行风控数据流通为例,银行与数据提供方提前线下协商后,数据提供机构将银行所需数据交付给银行。在此过程中,数据提供方(机构或数据厂商)提供数据,数据使用方(银行)需要数据进行加工后支撑风控业务。

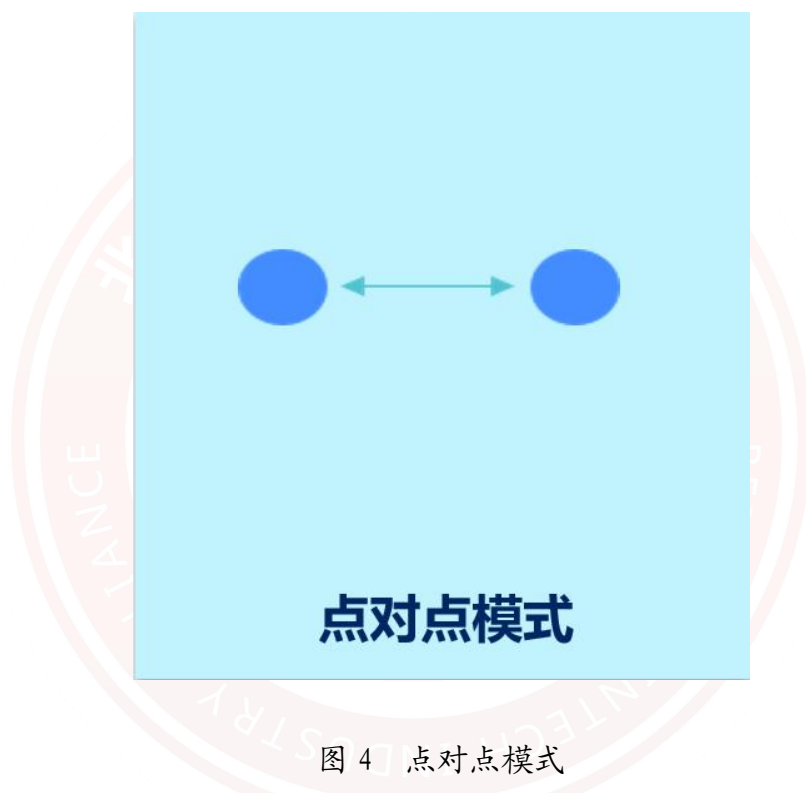


图 4 点对点模式

模式二:点对多模式。随着数据流通的普及,参与方数量增多,同一个数据资源往往出现多个数据使用方,每个使用方需求不同,点对点的数据共享流通方式给数据提供方带来较大不便,因此数据提供方将数据进行加工,形成标准化的数据产品或服务,同时提供给多个数据使用方(如图 5 所示)。例如:多家机构共享同一份客户数据样本,进行 AI 模型训练。点对多模式使得数据的共享与流通在效率上有较大提升。

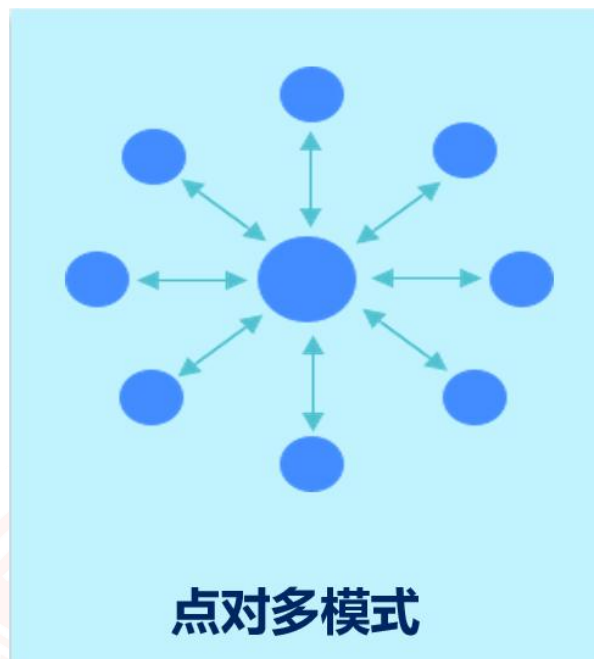


图 5 点对多模式

模式三:多点互联模式。随着数据流通参与方增多，各相关方对数据使用范围、深度和安全提出不同要求，出现了多点互联模式。在该模式中，各参与方通过数据市场进行数据的发布、检索，同时该类模式提供完整的覆盖各类角色的数据流通业务流程，构成数据可信流通模式（如图 6 所示）。



图 6 多点互联模式

以上三种金融数据可信流通模式各有特点，适用于不同的数据流通场景。在基于数据空间的数据可信流通方案中，通常可支持上述三种数据流通模式，在实际应用中，可根据业务需求选择合适的流通模式。

(四) 金融数据可信流通方案架构

金融数据可信流通的方案架构（如图 7 所示），自下而上分别为：数据流通支撑设施层、数据调度处理层、数据控制层以及数据运营服务层。



图 7 金融数据可信流通方案架构

流通支撑设施层是数据共享流通的基础与载体，包括计算资源、存储资源、网络资源等基础支撑设施。数据调度处理层实现数据可靠供给和合规流通，保障数据能够供得出、流得动。数据控制层实现了数据共享流通的安全可信与透明，保障数据生命周期安全可控。数据运营服务层实现了合规倍增的价值链，使数据能够用得好，充分释放数据价值。

（五）金融数据可信流通方案关键技术

1. 数据访问控制

● 数据访问控制定义

对具有价值的信息资源的访问都应该通过认证。用户在进行访问之前，通常会被要求提供正确的认证。最常见的认证方法是

提供用户名和密码的组合。然而用户名和密码是静态认证方式，很容易被破解。对于具有高价值的信息，应采用强度更高的认证方法。访问控制通过组合多种认证要素可以有效的提高认证强度。按用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。

- 数据访问控制的作用

通过对身份认证和确认，实现控制只允许哪些人可以访问数据和哪些人不可以访问数据。

2. 数据使用控制

- 数据使用控制技术定义

数据使用控制是对传统访问控制机制的扩展，支持复杂的策略控制要求，是实施数据流通后数据权益保护的关键机制。访问控制技术仅仅是在某个指令执行前发挥作用，一旦操作完该指令，访问控制便再也不会对数据有任何作用。数据使用控制是将数据控制权始终保持在数据提供方，使得数据提供方的控制策略能够在数据全生命周期进行执行。数据使用控制将数据使用控制延伸到数据使用方，例如控制数据在使用方使用一定时长或一定次数后自动执行删除。通过数据使用控制技术将数据控制权始终控制在数据提供方手中。

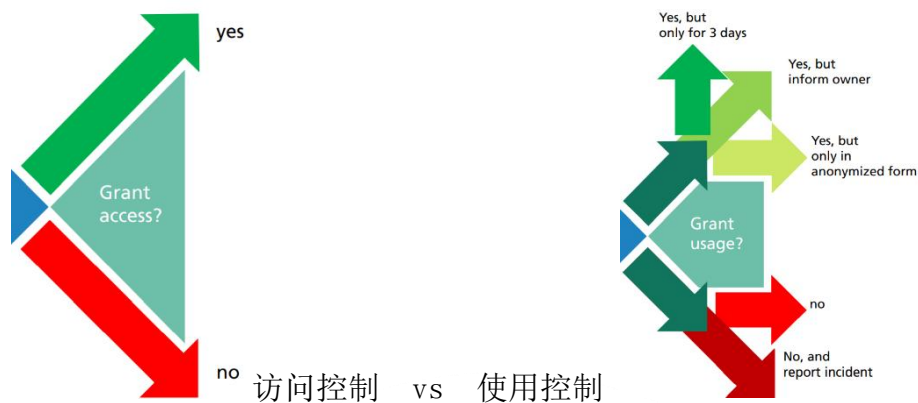


图 8 访问控制与使用控制的对比

通过 4W2H 的模型化描述可以更进一步体现使用控制的能力特性，使用控制策略可以控制使用方的目标角色（Who）在确定的时间（When）和位置（Where）通过何种应用（How To）以多大量级（How Many）访问和处理数据（Do What）。

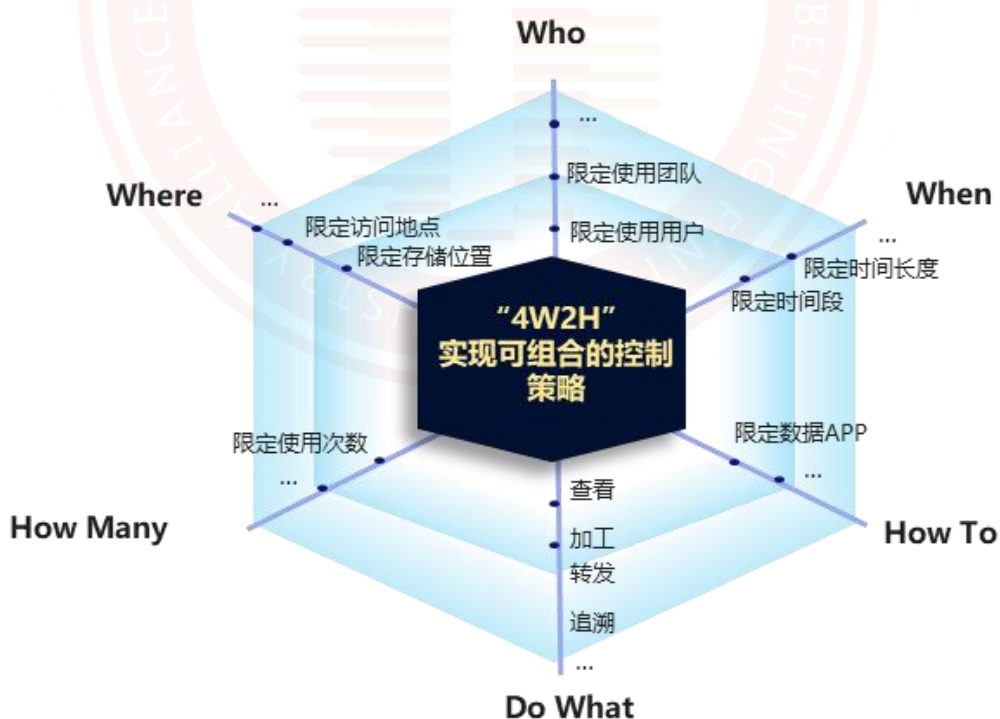


图 9 “4W2H” 控制策略

数据使用控制的典型能力如表 2 所示：

表 2 数据使用控制能力

编号	使用控制能力
1	基于时间段的使用控制
2	基于时长的使用控制
3	基于用户的使用控制
4	基于地域的使用控制
5	基于数据接收方安全级别的使用控制
6	基于应用的使用控制
7	基于数据使用次数的使用控制
8	要求数据流通加密的使用控制
9	要求数据流通前脱敏的使用控制
10	要求数据使用后发送日志的使用控制
11	要求数据使用后通知数据权益方的使用控制
12	要求数据使用超过一定期限后删除的使用控制
13	要求数据使用方落盘加密的使用控制
14	控制数据使用方能否转发数据

● 数据使用控制技术的作用

数据使用控制为数据提供方提供了在数据跨域流动场景中对数据权益的保护，在执行交换关键和敏感数据交易中，数据使用控制技术强制执行数据提供方制定的数据限制策略，始终将数据控制权限、知情权限和拒绝权限始终保持在数据提供方手里，打消了数据提供方数据流通利用的顾虑。

3. 数据空间连接器

● 数据空间连接器的定义

数据空间连接器是数据空间的核心组件，作为参与方接入数据空间的入口，负责数据空间中数据资源的安全可控交换。它是实现可信数据流通的关键基础能力模块。

● 数据空间连接器的作用

数据空间连接器提供数据接入、可控交换、数据消费能力，通过数据连接器可实现数据提供方和数据消费方之间数据的流通和可控使用，在数据空间连接器内执行数据访问和数据使用控制策略，确保数据交换过程的安全性和可追溯性。

4. 智能合约

● 智能合约技术的定义

将传统合约数字化，并以信息化方式传播、验证或执行的计算机协议。与传统合约相比，智能合约不依赖第三方执行合约，让合约验证和执行过程更加便捷。合约允许多方用户共同参与制定一份智能合约，通过 P2P 网络扩散并存入区块链，并自动执行，从而能够保证合约条款的安全可靠，让双方进行可信交易，并且这些交易可追踪且不可逆转。在金融数据交易过程中，通过智能合约技术能够缩短交易流程。

● 一体化智能合约技术的作用

智能合约不需要第三方执行，并且可以自动执行。另外智能合约可以实现自动化交易托管，减少交易流程中耗费的时间成本。

5. 数据脱敏

● 数据脱敏的定义

数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。目前数据脱敏较常见应用在涉及客户安全数据或者一些商业性敏感数据的情况下，在不违反系统规则条件下，对真实数据进行改造并提供测试使用，如身份

证号、手机号、卡号、客户号等个人信息都需要进行数据脱敏。数据脱敏类别可分为结构化数据脱敏和非结构化数据脱敏。

- 数据脱敏的作用

数据脱敏可以将数据漂白，抹去数据中的敏感内容，同时保持原有的数据特征、业务规则和数据关联性。保证开发、测试、培训以及大数据类业务不会受到脱敏的影响，达成脱敏前后的数据一致性和有效性。

6. 数据编织

- 数据编织的定义

数据编织是一种统一的数据管理架构，通过智能化和自动化的方式，将分布在不同位置、不同形态的数据资源进行统一集成和协同管理，实现数据的无缝连接、治理和服务。它为组织提供一个跨平台、跨环境的统一数据管理视图。

- 数据编织的作用

数据编织通过全局命名空间的打造，实现数据资产的可视、可管、可用。数据编织技术实现数据的无缝连接和协同，提供统一的数据访问接口，支持跨平台数据集成，并具备智能化的数据治理能力。通过数据编织，组织可以降低数据管理的复杂度，提升数据质量和可用性，加速数据价值实现。提供统一的数据视图和访问接口，使用户能够跨多个系统和平台访问数据。

7. 数据加密技术

● 数据加密的定义

数据加密技术原理是将一个信息（或称明文）经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密钥匙还原成明文。加密技术是实现网络安全技术的基石，其中加密钥匙是确保数据安全性的关键。

● 数据加密的作用

数据加密技术的主要目标是保护数据的机密性和完整性，防止未经授权的访问和篡改。通过使用强加密算法和密钥管理策略，数据加密可以确保数据在传输和存储过程中的安全性。

数据加密技术可以应用于各种场景和平台，包括云服务、网络传输等。它可以根据不同的安全需求，选择不同的加密算法和加密强度，以适应各种应用环境。

数据加密技术通常与数字签名等验证机制结合使用，可以确保数据的完整性和真实性。数字签名可以验证数据在传输过程中是否被篡改，并验证数据的来源是否可靠。

在数据加密技术中，密钥的管理至关重要。密钥是加密和解密数据的核心，因此必须采取严格的密钥管理措施，包括密钥的生成、分发、存储、销毁等，以防止密钥泄露和滥用。

8. 可信执行环境

● 可信执行环境的定义

可信执行环境（以下简称 TEE）是主处理器内的安全区域。它运行在一个独立的环境中且与操作系统并行运行。这个并行系统相对于传统系统更加安全，它确保加载的代码和数据的机密性和完整性都得到保护。在 TEE 中运行的受信任应用程序可以访问设备主处理器和内存的全部功能，而硬件隔离保护这些组件不受主操作系统中运行的用户安装应用程序的影响。TEE 通过加密和隔离保护不同的受信任应用程序。

- 可信执行环境的作用

可信执行环境在中央处理器上构建一块受保护的计算执行空间与其他区域隔离，保证在该环境下所加载的数据和执行的程序的安全性、完整性。在可信执行环境内部，应用运行也是相互独立的，不能无授权互访问。

9. 安全多方计算

- 安全多方计算定义

安全多方计算问题是在一个分布式网络上计算基于任何输入的函数，每个输入方在这个分布式网络上都拥有一个输入，而这个分布网络确保输入的独立性，计算的正确性，而且除了各自的输入外，不透露任何可用于推导其他方输入和输出的信息。主要有混淆电路、同态加密、秘密分享三种形式。安全多方计算主要面向的是在多个参与方的环境下，每一个参与方都拥有自己的私密信息，同时又希望利用其他的信息来共同完成计算一个函数的过程。

- 安全多方计算的作用

安全多方计算提供了一种基于密码学的解决方案，重点解决金融数据在计算过程中的隐私安全问题，在不泄露原始数据的前提下，实现多方协同计算，使得参与方无法得到除计算结果之外的其他信息，保障金融数据的安全共享、流通、计算和交易。

10. 联邦学习

- 联邦学习定义

联邦学习是一个机器学习框架。在多参与方或多计算结点之间开展高效率的机器学习。联邦学习做到各个参与方的自有数据不出本地，而后通过加密机制下的参数交换方式，在保障数据隐私的情况下，建立一个虚拟的共有模型。这个虚拟模型相当于聚合在一起建立的最优模型。在建立模型的过程中，各个参与者的身份和地位相同，而联邦系统帮助大家建立了安全共享的策略。另外根据原始数据的分布规律，常用的联邦学习模式主要有横向联邦学习、纵向联邦学习和迁移联邦学习。

- 联邦学习的作用

能够保证参与各方在保持独立性的情况下，进行信息与模型参数的加密交换，并同时让各自的模型获得成长。

11. 区块链存证

- 区块链存证定义

区块链数据存证，就是把数据标识（哈希值）存到区块链上，达到防篡改、可追溯、数据来源可信任的目的。一般情况下，通

过链上链下协同工作，采用文件与哈希值分离的方式，链上只保存文件的哈希值，原文件保存在链下。只要计算出文件的哈希值，与链上的哈希值比对，就知道文件是否被篡改。

- 区块链存证的作用

区块链存证最大作用就是防篡改。尤其针对电子合同，区块链存证功能加强了智能合约存证期间的不可篡改性。

12. 数据沙箱

- 数据沙箱定义

数据沙箱是一种可信管控技术，通常通过硬件或软件技术实现代码和数据的隔离，例如虚拟机、容器等技术。它提供了一个隔离的环境，用于在安全的边界内执行外部代码和数据，确保应用程序不会对主机系统或数据造成损害，允许数据使用方在安全和受控的区域内对数据进行分析和处理。

- 数据沙箱的作用

数据沙箱通过隔离技术实现数据的防泄漏，能够保障数据在安全环境中使用和分析，不会被泄露到沙箱外部。

13. 密态计算

- 密态计算定义

密态计算是一类在数据加密状态下直接进行处理和计算的技术，能够在保护数据隐私的同时实现数据的分析和利用。数据在全生命周期中始终处于“看不见”的加密状态，实现“可用不可见”。

- 密态计算的作用

通过密态计算旨在实现从数据进入系统到计算完成，再到输出结果的全生命周期保护。无论是在数据存储、传输，还是在多步骤、多算子的复杂计算中，密态计算都能够保证数据在整个流程中始终保持密态化。这种全链路加密的特性，显著降低了流通和加工等中间环节的数据泄露风险。



五、典型场景应用与技术验证

(一) 中信银行总分行数据流通管控实践场景

1. 场景及需求

在中信银行内部，为了满足分行经营管理、绩效管理等系统使用数据的需求，总行定期按照预设规则给各分行下发分行所辖范围内的数据，其中包括敏感数据和非敏感数据，同时分行按照外部机构或内部合规管理要求，按需向总行申请使用数据，其中部分场景涉及客户敏感数据。

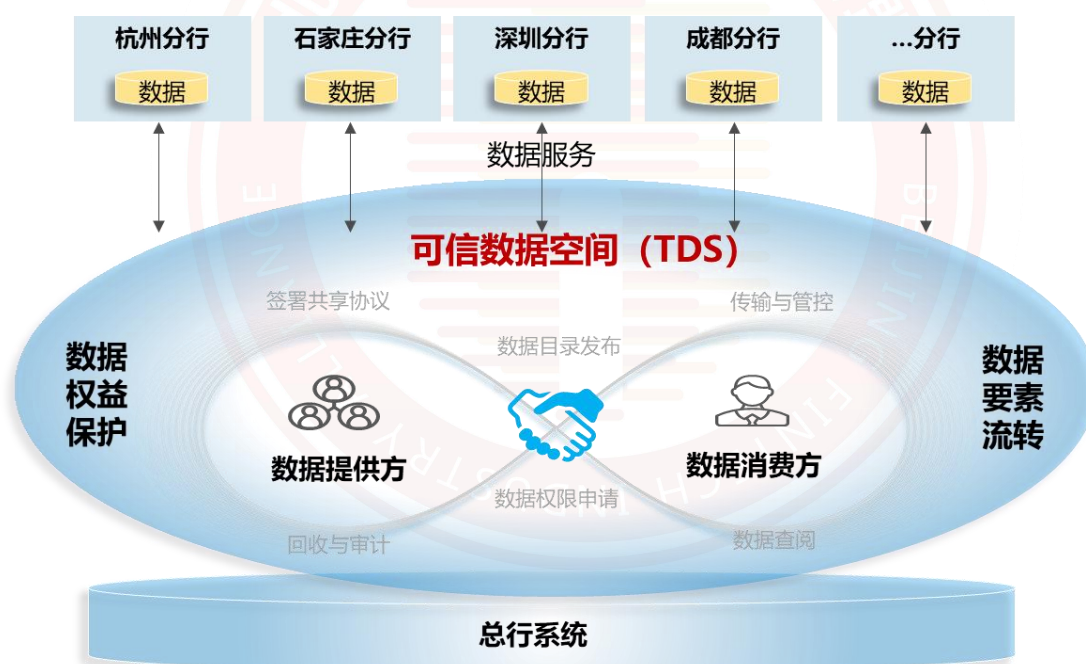


图 10 总分行数据可信流通

数据在总、分行流通过程中，有明确的数据安全策略，并在数据流通前采取了严格事前审批、数据流通过程中对数据进行加密、对数据使用过程中进行隔离管控等技术措施保护敏感数据。但当前对于数据申请方获取数据后的使用策略，缺少精细化的技

术管控手段，对于数据流通、使用全过程难以做到最小必须、可感知、可管控、可审计。亟需探索一种数据可信流通方案，支撑总分支行数据高效流通，统一安全隐私策略管控，在保证数据权益的前提下，建立信任，提升数据流通效率。

2. 技术验证方案

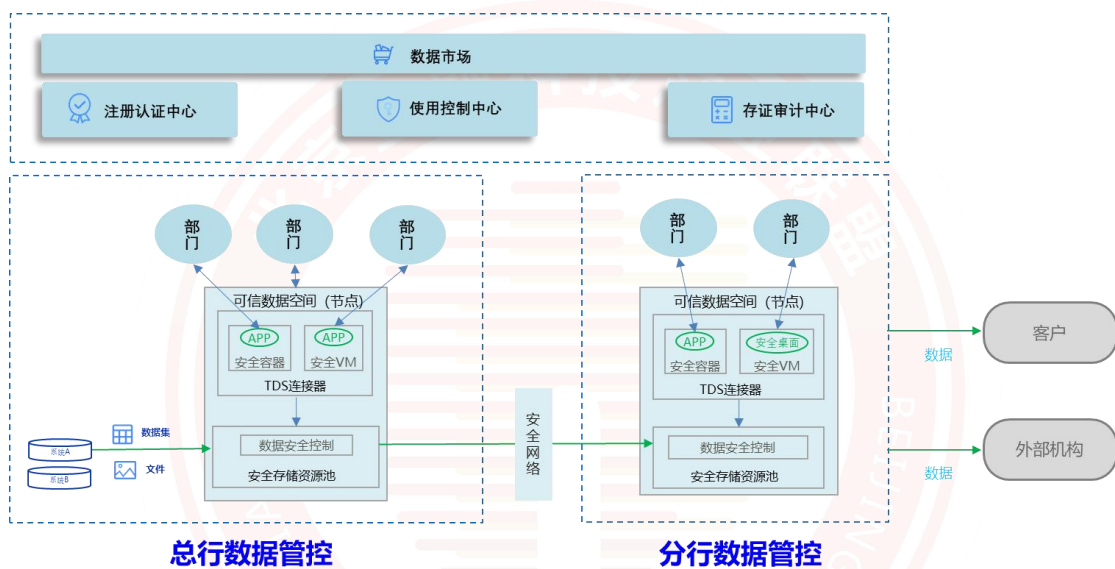


图 11 总分行数据管控

中信银行联合华为公司开展联合创新，在总分行部署可信数据空间方案，通过可信数据空间技术的应用，实现敏感数据安全优先、非敏感数据效率优先的总体目标，在数据下发源头即植入数据安全策略，在分行侧各类数据使用场景中，全过程校验安全策略校验。实现总分行两端、系统和用户之间端到端的数据使用安全控制。

基于数据存储资源池实现数据流动安全控制、数据使用安全控制能力。基于数据分级分类标签提供强制访问控制策略，满足

数据资源流动过程中的基础合规保障。面向业务应用提供数据流动、数据使用控制能力，满足数据按需流动、限时限期使用等安全策略要求。

基于可信执行环境构建安全底座，提供面向业务应用及用户的更加丰富的数据使用控制能力。例如依据业务需求及策略要求限定使用时间、使用地点、使用次数、使用方式、如何使用等精细化使用控制手段，确保用户符合最小必须要求合规使用；

3. 预期效果

技术价值：实现数据使用过程可感知、可管控、可审计，建立面向数据细颗粒度（如文件或字段）的使用安全控制，同时增加多重控制维度，实现“4W2H”（Where、Who、When、Do What、How to、How Many）最小化控制，基于最小必须原则满足总行统一数据管控策略要求。

业务价值：中信银行软件开发中心基于数据空间开展企业及行业数据流通探索，有效促进了内外部数据流通整合，支撑全域数据的统一管理、融合共享，助力金融产品和风控模型优化，提升金融服务和风险管控质效。同时，及时响应国家“数据要素×”行动计划，探索金融行业数据空间建设，为金融机构间数据共享共用和高效流通，为培育高质量金融数据市场贡献力量。

（二）工银金租数据流通场景

1. 场景及需求

2022年初人民银行印发《金融科技发展规划（2022-2025年）》，将充分释放数据要素潜能作为重点任务，高度重视客户信息数据治理工作，建设外部数据流通的生态体系，确保我行在安全、合规的前提下深度融入外部数据要素流通市场，提升内部外部数据融合场景赋能，助力我行抢占数据要素流通市场的先机和制高点。

在反欺诈数据交易合规防控中，尚缺乏有效的手段以保证客户信息的准确性，且在当客户信息发生变化时，无法及时获取相关情况更新客户信息。此外，隐私泄露、数据安全和数据孤岛等问题无法保证客户数据可信流通。

工商银行依托联邦学习平台，利用大数据分析、联邦学习等技术，积极推进数据要素的内引外拓，充分发挥数据精准直达优势提高企业在营销展业、风险防控、内控合规等方面的运行质效，同时为开展客户智能营销和金融科技创新提供精准的发力方向。

工商银行数据交易平台是同业首家建成的面向互联网开放的数据交易平台，目前已入驻企业34家，上架380余项数据产品，撮合交易1676万元。平台立足金融行业，涵盖精准营销、信贷风控、反欺诈、反洗钱等多个业务领域，已完成与上海数据交易所的深度对接，实现在数据交易平台展示上数所挂牌的388

项金融类数据产品的详细信息，是同业首家对接数据交易所的数据要素流通平台。

2. 技术验证方案

基于数据交易平台完成数据资产的交易流通，利用联邦学习平台完成数据资产的交付，利用隐私计算技术，将工银金租反洗钱系统和总行咨讯平台中的工商数据进行对接，通过工银金租客户的数据与工商数据的部分字段对比，从而校验工银金租客户信息准确性；利用区块链技术，实现数据权益鉴别、数据完整性核验、数据使用记录追溯等业务诉求，提供数据确权、数据鉴真及存证溯源服务，并对全流程交互信息进行可信存证监控，以支撑数据登记、数据交易、数据交付、使用审计等数据全生命周期流程的闭环。

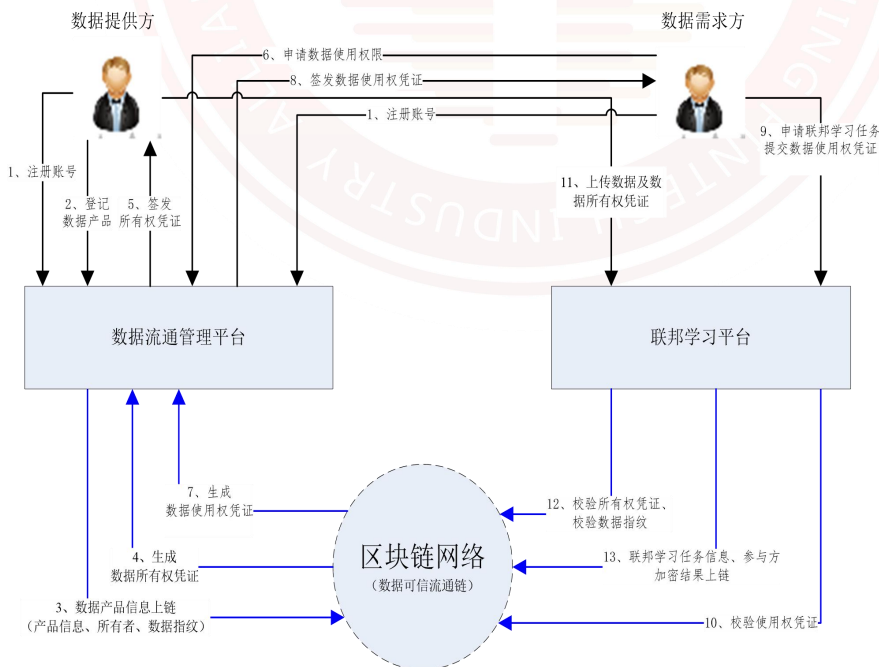


图 12 数据流通场景图

3. 预期效果

技术价值: 通过联邦学习技术, 在原始数据不出域的情况下, 实现多方合作联合建模, 在隐私保护跨机构数据共享的前提下, 数据撞库成功率达 90%以上, 提高客户信息准确性, 有效进行风险防控。联邦学习技术, 全面赋能数据要素的有效流通, 提高数据赋能水平, 增强企业竞争力。

社会价值: 工商银行软件开发中心基于数据交易平台搭建的工银金租数据流通项目, 能够助力银行全业务、全流程的安全保障, 形成全行用数的外部数据生态体系, 实现数据对业务的及时赋能和数据驱动智能化决策, 赋能普惠金融, 助力乡村振兴等实体经济。

(三) 银联安全生物特征支付场景

1. 场景及需求

数字经济时代, 用户生物特征信息的应用面临越来越高的合规风险。基于生物特征信息进行用户身份识别的生物识别技术, 在金融、安防、电子商务等诸多场景实现了广泛应用。一般通过客户端采集生物特征信息, 将用户的明文数据传输到云端服务端进行特征值的提取和验证。对于用户而言, 生物特征信息需明文传送至云端; 对于金融机构而言, 保留用户生物特征信息也需要承担数据泄露的风险。

在金融支付场景中, 更需要平衡业务需求与个人信息保护之间的关系。在人脸特征识别之支付场景中, 为保障数据安全, 金

融机构收集的人脸图片或特征信息不能完整存储于一方，需要在多方协同下完成身份验证与识别。为满足此应用需要，形成了基于安全多方计算和基于可信执行环境两种实现方案。

2. 技术验证方案

人脸识别支付是一种利用人工智能技术，特别是神经网络，来识别个体面部特征并进行身份验证的支付方式。系统通过卷积神经网络（CNN）从输入的图像中自动提取出人脸的深层特征，将图像数据转换为低维度的特征向量，通过与已存储的用户面部特征相匹配，从而完成支付过程中的身份验证。

基于安全多方计算人脸识别支付中，通过多方安全计算（简称“MPC”）秘密分享的方式将生物特征随机切分成碎片存储至两个独立的实体，任一参与方都无法恢复完整的生物特征，降低了泄露风险。同时，基于 MPC 安全多方计算技术进行人脸图像特征提取和特征比对计算，确保生物特征数据的安全和计算结果的正确性、完整性。在实用性方面，采用明密文混合运算优化深度神经网络的离线特征提取，采用秘密分享、同态加密混合计算优化 1:N 特征比对在线处理。在不改变用户生物特征识别处理流程的基础上，有效提升 MPC 安全生物特征处理效率，满足人脸识别支付场景的生产可用要求。

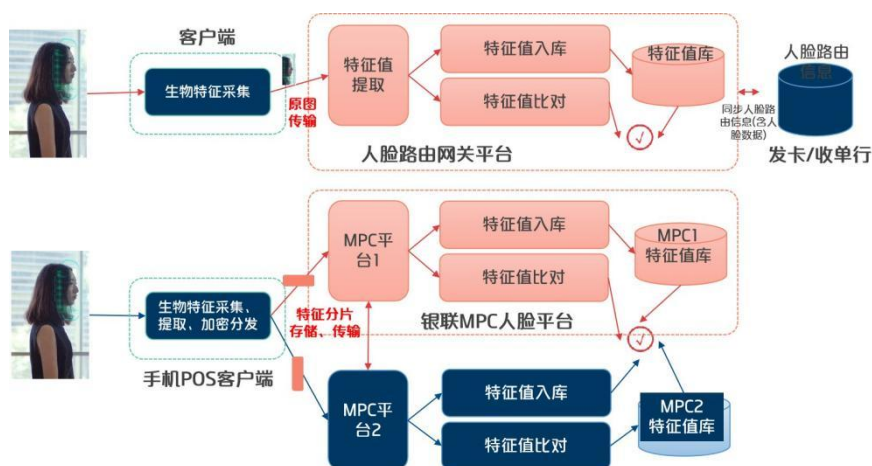


图13 基于安全多方计算的人脸识别框架

3. 预期效果

该项目于2021年4月入箱人民银行上海金融科技创新监管试点第二批应用试点，依托基于隐私计算技术的数据要素安全流通基础设施，完成卡组织和某银行双边网络的多方安全计算系统部署。2023年4月由北京金融科技创新监管工具实施工作组宣布完成出箱。

项目综合运用了隐私计算安全多方计算技术，深度结合人脸识别场景，为《中华人民共和国个人信息保护法》等法律法规中对于用户生物特征（人脸）信息的安全合规使用要求提供了解决方案。在用户敏感信息存储方面，提出了生物特征分散存储的模式。为确保用户生物特征（人脸）信息的合规使用，将用户人脸特征信息经处理后形成计算因子，分散存储在多个机构，即使单个机构的计算因子泄露，也无法恢复完整的用户人脸信息。同时，单个机构保存的计算因子无法独立完成交易验证过程。在隐私计

算应用方面，通过技术优化使得隐私计算安全多方计算在人脸特征提取、特征比对等处理的性能能够逐步满足生物特征识别场景的生产可用要求。安全多方计算在分片特征上的比对性能，当前响应时间已经达到秒级以内，使得整体产品能够达到真正生产可用的水平。

（四）金智塔小微企业智能授信风控创新实践场景

杭州金智塔科技有限公司联合某公司打造的《隐私计算助力小微企业智能授信风控创新实践》项目响应了国家关于数字经济、普惠金融的政策要求，通过平台实施落地，降低银行风险的同时，化解了小微企业的贷款难、贷款贵的问题，有力的推动了金融机构与小微企业高质量发展，助力浙江共同富裕示范区建设。

1. 场景及需求

2021年11月20日，中央政治局委员、国务院副总理刘鹤指出，金融机构要加大对企业创新的支持，探索利用数字技术为企业增信，解决小微企业及个体户融资难问题。但小微企业缺乏固定资产，有效抵押物不足，且信息透明度较差，难以提供真实有效数据用于风险评估。银行急需多维数据全面评估贷款风险，化解小微企业贷款难、银行风险高的问题。随着数据合规监管趋严，银行业又面临无法接入外部数据的难题。

2. 技术验证方案

本方案运用多方安全计算、联邦学习和区块链等技术，安全合规融合银行内外部数据，实现数据可用不可见，建立实时动态

360度小微企业用户画像与关系图谱，全方位了解企业状况。通过贷前准入规则、反欺诈、黑名单、信用评分卡以及额度利率等模型，实现智能授信、风控。具体技术方案如下：

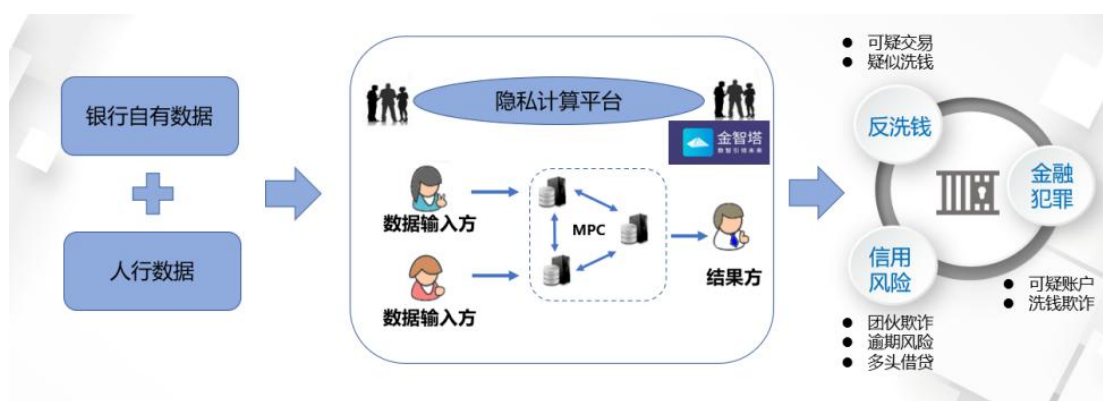


图 14 技术方案

1. 某银行和某机构部署金智塔隐私计算节点，某银行作为需求方，双方均作为数据提供方。
2. 某银行向某机构发起企业数据申请，某机构审批通过后将多维度企业数据导入隐私计算节点。
3. 双方数据根据企业营业执照号码进行隐私求交对齐，然后使用联合 SQL 进行特征分析、特征筛选。
4. 在特征工程的基础上，根据某银行提供的标签进行联合建模（线性模型、树模型），建立智能授信、风控模型。
5. 智能授信风控模型对增量企业进行评分，得到潜在优质客户名单。
6. 某银行根据行内业务规则，将模型评分作为决策因子，对企业进行进一步筛选，得到最终的授信名单。

3. 预期效果

本项目做了大量的技术创新，多篇论文发表在 WWW、KBS、IJCAI 等国际期刊上，并申请了 3 项发明专利，2 项已获授权。主要的创新点如下：

1、应用隐私保护机器学习新技术，在数据不出域的前提下，进行高效的机器学习建模。金智塔科技提出了一种将随机排列和秘密分享结合的隐私保护机器学习框架。这种方法比现有的加密方法更有效，可以显著减少计算开销。同时，金智塔科技的方法相比联邦学习算法更加安全。实验结果表明，金智塔科技的方法不仅计算速度快了 5 倍，而且减少了 80% 的网络开销。

2、创新设计基于两阶段的隐私保护 CDR 框架，在保护数据隐私前提下，有效缓解数据稀疏性。跨域推荐（CDR）被广泛研究以缓解推荐系统中普遍存在的冷启动和数据稀疏问题。大多数现有的 CDR 模型都假设信息可以直接跨域传输，而忽略了隐私问题。为了解决这个问题，在该案例中，金智塔科技提出了一种基于两阶段的隐私保护 CDR 框架。该方法既可以保护数据源的隐私，又可以缓解数据稀疏性。实验结果表明，在两个基准数据集上，金智塔科技的方法具有普遍的有效性。

3、设计新型全对称、去中心化的节点网络架构，增强平台在不同业务场景的灵活性和普适性。针对本项目中节点横向、纵向交叉分布的特点，金智塔科技提出了一种全对称、去中心化的节点网络架构。在该架构中，所有节点通过专线或者互联网组成

一个 mesh 网络，互联的一组节点可以组成一个 group。组中的节点可以通过某个指定的节点调度，协同进行隐私保护机器学习。实践表明，金智塔科技的架构相对于传统的集中式架构，对于不同的场景具有很强灵活性、普适性。

在应用成效方面，本项目上线后，较大的提升了用户的授信额度，户均授信额提升了 40%以上，显著的扩大了小微客户群体服务规模；有效的识别欺诈、多头借贷和洗钱，环比提高 50%以上；并降低了小微企业的贷款成本，与互金平台融资对比，降低了约 50%以上融资成本；且极大的提升了办贷效率，线上一键申请，线下一次签约，1 个工作日办结。

（五）华为公司与伙伴数据流通实践场景

1. 场景及需求

在非金融领域，可信数据流通同样有大量的实践应用。华为公司在集团内部以及华为与生态伙伴之间，有大量的数据交换场景，在华为以往的研发实践中，发现数据提供方只能将需求方所需数据不作区分的打包发送，数据权益完全依赖于需求方此前所作出的承诺，虽然这种承诺通常也会体现在双方的合作协议上，但是对数据使用的合规过程进行监管和审计的成本非常高，而且事后的追责已经失去了风险阻断的时效性。处于产业生态圈中的企业，迫切希望能够建立一种依赖于技术实现的对数据权益保护的数据交换平台。



图 15 跨不同主体的数据流通示意图

2. 技术验证方案



图 16 企业可信数据空间解决方案

基于可信数据空间参考架构，华为研发了企业可信数据空间解决方案，部署了数据空间连接器，即连接数据提供方与使用方，实现目录推送与资源检索、合约达成与执行等服务功能，以及日

志存证与溯源、数据使用控制等安全功能。采用该方案，华为实现了集团内部以及华为与伙伴之间的数据可信流通与共享。

3. 实施效果

目前，基于华为企业可信数据空间，已经实现了数据共享交换过程实例，为数十家产业链上下游参与方企业提供数据共享流通平台，企业可以通过该平台进行依赖程序自实现的跨企业数据可信流通。

(六) 富数科技基于多源数据的金融风控数据空间场景

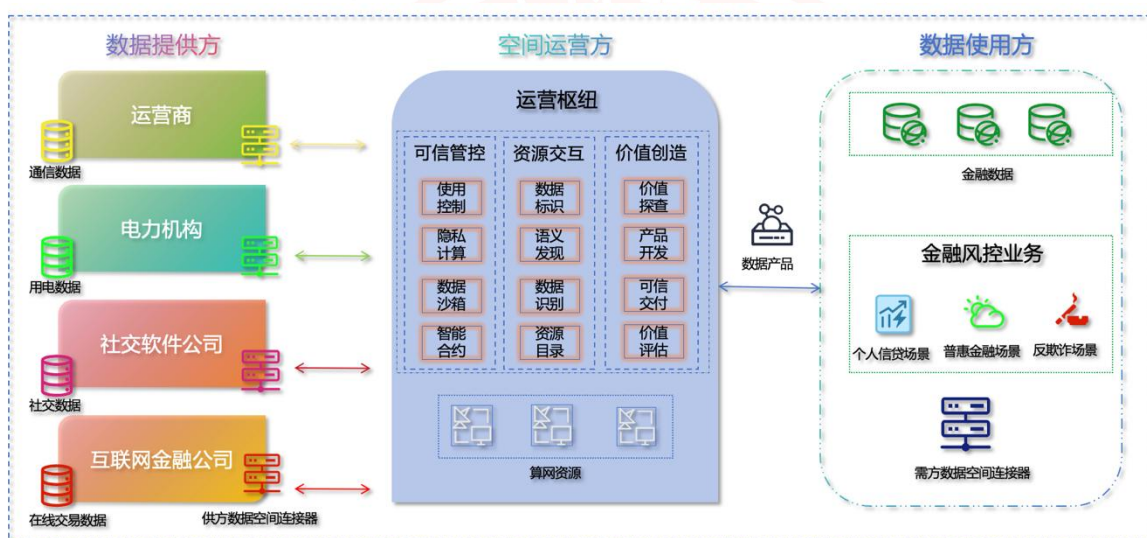
1. 场景及需求

随着数字化时代的到来，金融行业对数据的跨域融合与流通的需求变得尤为迫切。特别是在风险控制这一信贷业务的核心环节，风控模型的精准度直接关系到金融机构的收益与稳健性。然而，由于央行数据使用合规方面约束不断加强，风控模型可用数据源的供给渠道不断收缩；同时，在信贷场景中，信息欺诈和数据失真情况不断加重，传统银行风控模型因缺乏多维动态数据支撑，已经无法进行有效识别及预警。

富数科技联合某金融机构，依托隐私计算技术，打造金融数据空间，为金融行业引入运营商、电力、互联网企业等多方数据，围绕个人信贷、普惠金融、反欺诈三个典型场景，实现数据“供得出、流得动、用得好、保安全”。通过这一项目，旨在提升金融机构的风控能力，促进金融市场的健康发展和地方经济的增长。

2. 技术验证方案

项目基于隐私计算技术打造金融风控可信数据空间，整合金融机构、运营商、电力公司、互联网公司等的多源数据，确保数据处理的安全性和合规性。项目实施包括数据采集与加工、数据产品打造、数据产品发布与交易、迭代优化等阶段。技术措施涵盖多方安全计算、联邦学习、匿踪查询等，确保了数据处理的安全性和合规性。



全性和合规性。

图 17 技术方案

项目在数据采集阶段，确保数据来源合规、传输渠道安全。在数据资源加工阶段，采用隐私计算、数据加解密、模型水印、代理重加密、安全沙箱等技术，对采集到的数据进行清洗、转换和增强。在数据产品打造阶段，利用隐私计算能力打造高密数据

产品，与多方联合进行安全对齐，使用联邦学习联合建模。在数据产品发布阶段，经过严格的安全评估后，发布到数据空间的数据产品市场。在数据产品交易阶段，金融机构在购买数据产品后，可在本地部署并调用模型，实现风险控制和决策支持。

3. 预期效果

技术价值：通过隐私计算技术，实现数据的高效融合与智能分析，在确保数据隐私和安全的前提下，提升了风控模型的准确性和效率。项目在个人信贷、普惠金融、反欺诈等场景中，通过智能风控模型，信贷审批效率提高 30%，违约风险降低 30%以上，为金融机构带来直接经济效益。

社会价值：项目在多家金融机构落地，累计经济收益超过 1400 万元，实现业务成本节约与经济收益增长，形成新的业务增长点。通过金融普惠服务，增强了对中小企业的金融支持，促进了地方经济活力，预计提升社会就业率和经济增长速度。项目的成功实践为行业内外的数据安全与合规提供了示范，强化了其在该领域的标杆地位，为政策制定者提供了现实案例，促进了数据要素市场化配置的政策环境。

（七）蚂蚁科技三农普惠金融服务场景

1. 场景及需求

该项目在三农普惠金融发展中小农户贷款难的背景下，蚂蚁密算、网商银行、农业农村部大数据发展中心三方首次将时空大数据和密态计算相结合，在满足“数据可用不可见”的合规前提

下，基于卫星遥感时空数据和农业农村部动态库数据联合建模，形成农业信贷实时评估指标，有效解决了农户贷款评估难题，为大规模农业授信提供了行业解决方案，同时也为合规开发应用公共数据价值，提供了切实可行的参考思路和落地路径。

2. 技术验证方案

通过密态计算技术搭建密态可信数据空间，在满足大数据发展中心数据不出域的情况下，将网商遥感作物识别结果、授权用户信息与乡村动态数据（如人地确权、土地遥感数据）进行双方数据的联合建模，最终产出可对农户经营情况与金融扶持强相关的标准结果数据。

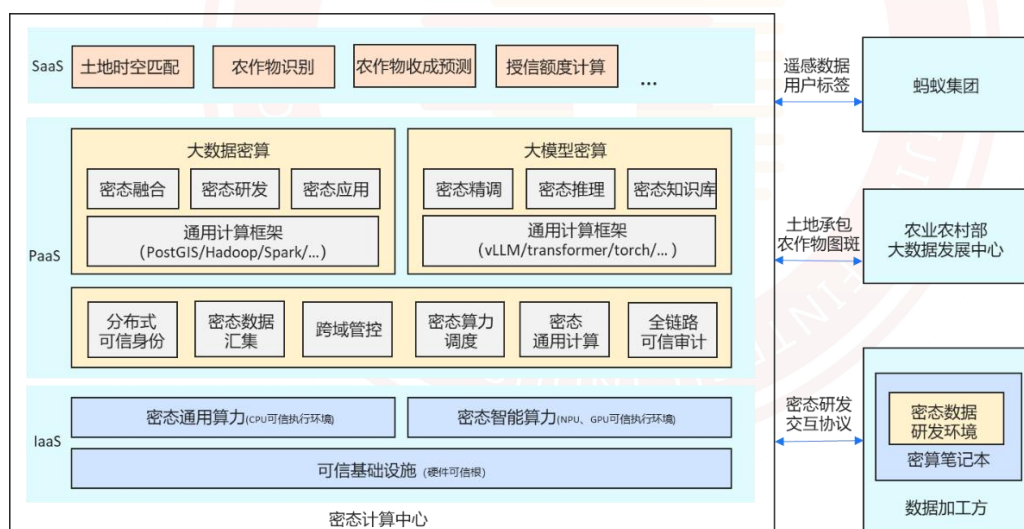


图 18 密态可信数据空间方案示意图

密态 IaaS 层提供密态计算所需的基础硬件。可信基础设施提供硬件可信根，用户可以依据它对密态计算中心的软硬件配置进行远程验证；密态通用算力、密态智能算力分别提供密态化的

CPU 的计算能力、GPU/NPU 计算能力。其安全保障程度可依据隐私保护计算通用安全分级标准和实际场景需求来确定。

密态 PasS 层主要提供密态服务能力。一部分是通用的密态服务能力，包括分布式可信身份、密态数据汇集、跨域管控、密态算力调度、密态通用计算、全链路可信审计等。这些提供了一系列能够防止系统运维方和数据研发人员主动攻击的基础安全能力。在此基础上，密态计算中心融合了主流的计算框架。按照计算框架类别的不同，又可以分为大数据密算(PastGIS、Hadoop、Spark) 和大模型密算(vLLM、transformer、torch) 等数据和模型加工处理能力。融合后的框架能够提供与明文框架相同的接口并处理多方密态数据。

密态 SaaS 层提供服务高价值高敏感数据的密态数据空间，用于实现与场景相关的具体数据业务功能。在本案例中，密态计算中心通过空间匹配，获得特定农户的农作物图像，并对农作物种类进行识别，以及对农作物的收成进行预测，基于农作物收成及农户的其他信息，计算农户的授信额度。

3. 预期效果

目前，超 606 万农户通过这一服务获得银行的贷款额度，累计授信 964 亿。他们来自全国超 2600 多个县级行政区，其中约 80% 的农户种植面积不到 10 亩。网商银行调研显示，66%的农户因此首次获得手机贷款，方案上线以后，农户借款不用跑网点，实现“手机贷款”“秒申秒贷”“秒借秒还”，农民能够像市民

一样获得便捷、灵活的金融服务，随时可以贷到款。这一实践通过密态计算技术创新公共数据的应用范式，为破解三农金融信贷难题提供了新的样本。



六、总结及建议

(一) 主要结论

可信数据空间建设正处于起步探索期，在各行各业都在基于业务场景进行规划和探索，通过实践不断地迭代更新发展。当前部分厂商参考欧盟数据空间参考架构、信通院可信工业数据空间系统架构等进行了产品实现，并在部分金融机构、政府及企业等机构开展了落地探索，在企业数据空间落地方面积累了一定经验。但面向行业可信数据空间、城市可信数据空间建设，仍存在法规、技术、标准、商业模式等方面的挑战。

在法规方面，缺乏明确金融数据流通的范围和适用场景等，金融机构对数据的敏感性没有统一标准，导致其“不愿流通”、“不敢流通”，使得金融数据被封闭在“孤岛”中，限制了金融数据在市场中的流通。

在技术方面，缺乏统一的可信数据空间参考架构、功能要求、运营规范等。例如可信数据空间连接器的功能定义、连接协议、身份认证协议、数据接入协议等，厂商间的实现未遵守统一技术标准，将提高客户技术集成难度以及使用门槛，在一定程度上会阻碍数据空间相关技术的落地。

在标准方面，缺乏厂商间的跨域互联标准、数据互操作标准等，难以支撑跨机构的行业级、城市级可信数据空间建设。按照国家数据局对可信数据空间的定义，可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的数据流通利用基础

设施。这就需要厂商间基于标准进行互联互通，共同构建可信数据空间，支撑数据跨域跨组织安全流动。

在商业模式方面，当前可信数据空间厂商盈利模式主要还是以产品销售为主，但数据空间建设运营方盈利模式尚不清晰，对于有意愿的运营方尚未有足够的吸引力。尤其在金融行业，行业可信数据空间谁来建设，谁来运营，如何盈利，相关利益方的商业模式的仍需进一步探索。

（二）相关建议

我国数据要素市场体系逐步确立，为最大化释放数据要素价值、推动数字经济大发展，数据资源的流通将成为必然趋势。基于数据空间的数据可信流通体系建设，将成为促进数据流通，释放数据价值的重要数据基础设施，建议国家及行业主管单位在相关技术标准、试点验证等方面做如下牵引。

1. 加强数据规范流通，促进金融数据要素价值释放

在金融数据分类分级要求的基础上，进一步明确金融机构数据流通的范围和适用场景等。针对不同类别和级别的数据，明确金融场景下可跨机构流动的数据类型和范围，以及配套的安全使用要求，建立差异化的授权使用规范，明确数据提供者、数据使用方、数据经营方、数据服务方等在数据流通过程中的权利与义务，规范数据流通行为，解决数据不敢流的问题，进一步释放金融数据要素价值。

2. 加快制定可信数据空间技术标准及互联互通标准

为更好的推进行业数据空间，甚至全国统一数据大市场的形成，数据空间互联互通至为重要。不同公司或者使用不同类型技术搭建的平台，存在技术上的差异性，需要在国家和行业层面构建互联互通标准。通过技术标准来规范厂商的技术实现，助力各行各业和各地区建立互联互通的可信数据空间，实现数据安全流通和高效利用，促进数据要素交易和协同创新。

3. 鼓励头部机构联合开展行业可信数据空间试点

可信数据空间还未实现大规模应用，对于金融行业应用还处在探索阶段，鼓励金融机构通过试点研究拓展可信数据空间应用场景，联合开展探索行业可信数据空间建设模式，构建跨机构甚至跨行业的数据流通基础设施，实现跨组织、跨行业的数据可信流通，促进行业数据要素价值释放，支撑金融机构业务创新。