TDM TRUSTED INDUSTRIAL DATA MATRIX CONSORTIUM 可信工业数据空间生态链

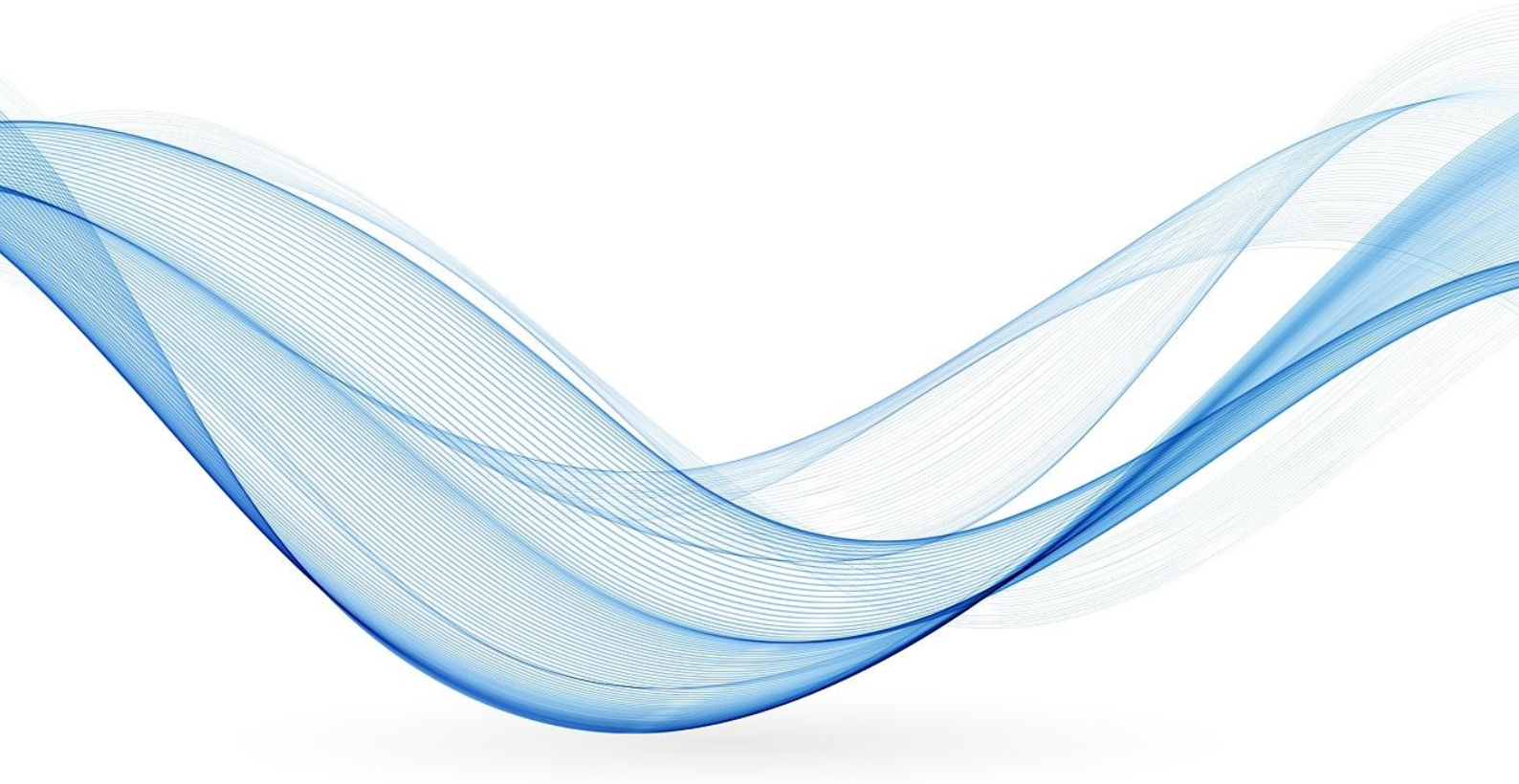
工业互联网产业联盟 Alliance of Industrial Internet

Trusted Industrial Data Matrix | 2023

可信工业数据流通应用案例集

声 明

Statement



组织单位

工业互联网产业联盟　　可信工业数据空间生态链

牵头编写单位

中国信息通信研究院

参与编写单位

华为技术有限公司、中国电信集团有限公司、南京理工大学、北京交通大学、中控集团、中国科学院信息工程研究所、之江实验室、华控清交信息科技（北京）有限公司、四川长虹电器股份有限公司、中企云链（北京）金融信息服务有限公司、 广东一知安全科技有限公司、深圳数鑫科技有限公司、广州赛宝联睿信息科技有限公司、北京双湃智安科技有限公司

编写组成员

吕东阳、韦莎、陈荣富、陈国润、李骏、陶耀东、王云河、牛犇、张玲翠、唐博、高志峰、刘铮、毛俊杰、马川、闫小龙、张广喜、蒋俊、李沂航、宋磊、周子文、高凡、范佳、黄振华、黄建新、蒋国辉、张扬、田仲秋、夏鹏程、王帅

前 言

随着新一代信息技术与制造业的深度融合发展，全球工业数据应用已经进入纵深发展的新阶段，数据作为新型生产要素和重要战略资源，正在制造业数字化转型过程中发挥出更大的作用。在这一进程中，工业数据的流通共享受到广泛关注。顺应新发展形势，我国积极营造多方主体参与的数据共享流通生态，国务院先后发布《关于构建更加完善的要素市场化配置体制机制的意见》、《要素市场化配置综合改革试点总体方案》，明确提出在确保数据安全的前提下，分级分类、分步有序推动部分领域数据流通应用。

本报告从数据共享流通的典型场景和模式出发，精选出8个工业数据可信流通应用场景案例汇编成册并发布。通过此应用案例汇编，希望多方位呈现工业数据共享流通在工厂内外的应用实践和成效，展望未来工业数据应用发展的趋势与方向，为更多的行业企业进行工业数据应用提供示范和标杆，形成一系列可复制的成熟经验和模式，推进规模化发展。

本报告共分为五个章节：第一章阐述了发展工业数据可信流通能力的意义。第二章论述了工业数据可信流通体系的内涵。第三章结合需求，总结提炼出工业数据可信流通的应用场景和模式。第四章梳理了八个工业数据可信流通典型应用案例。第五章从场景、模式和实践经验出发，总结提炼了工业数据流通应用的实践流程和路径，为企业实施推进产业数据共享流通提供借鉴。

目 录

第一章
Chapter 1

为什么要发展工业数据可信流通能力

（一）我国工业企业数据共享流通问题和需求报告

为了梳理企业在工业和产业数据共享、流通中的典型场景、采用的技术和管理手段以及存在的问题，工业互联网产业联盟联合可信数据空间生态链开展《我国工业企业数据共享流通现状问题和需求》问卷调查，问卷面向产业数据流通过程中的数据提供方、使用方、服务方等主要角色，对当前企业数据流通的主要环节、流通方式、技术手段、核心需求等关键现状进行梳理，共回收有效问卷27份，覆盖电子信息、制造、能源、物流、工业服务、工业信息技术等行业。问卷显示，96%的工业企业存在数据流通场景，覆盖研发、生产、物流、销售、服务等产品全生命周期。其中，研发、生产、服务的覆盖率超过了七成；62%的企业已经具备了数据流通相关案例或场景，85%的企业在具有安全可信的数据流通方案时，愿意通过数据流通创造价值。可以看出，相当部分企业已经开展数据流通实践，通过数据流通释放产业数据价值已经成为企业关注重点。

从数据类型来看，参与流通的数据类型多种多样，主要包含文档、各类软件和系统数据、设备数据、图片、影像、工业机理模型等六大类，其中设备数据（22%）、软件和系统数据（21%）、文档类数据（19%）占比最高，体现出工业场景下，对于企业信息管理系统（MES、ERP等）、控制系统、底层设备数据等企业、设备级工业数据的流通利用需求显著，对于工业数据的流通需求存在于研发设计、生产制造、供应管理、销售运输、产品服务等全流程。

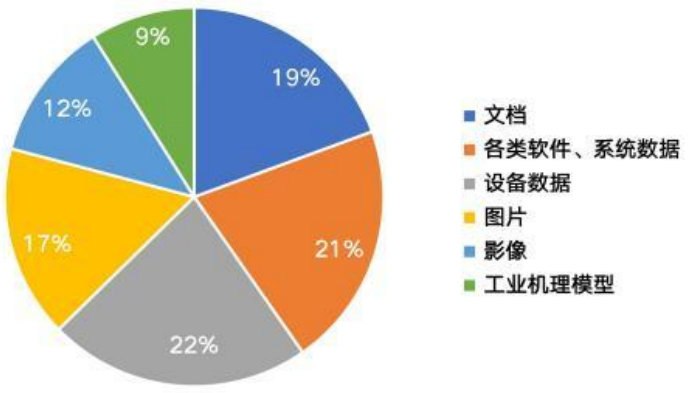


图1.1　参与流通的数据类型

从痛点问题看，当前企业在工业数据流通中主要存在环境安全问题、过程可信问题、数据可控问题、权属责任问题、数据内容问题、收益划分问题六大担忧。其中环境安全问题（20%）、权属责任问题（20%）、过程可信问题（19%）、数据可控问题（17%）位居前四，表明当前数据流通的难点、堵点集中在保障数据流通中不泄露、不丢失，用户身份可信、以及处理数据的应用程序可信，确保数据共享中的主体、时间、地点、行为以及客体可控等方面。

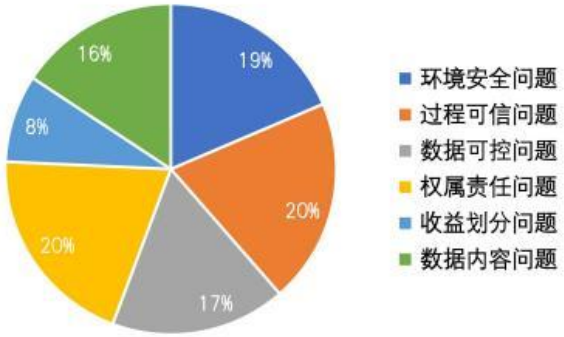


图1.2　数据流通中的痛点问题

从企业在数据流通过程中期望的管控手段来看，对使用时间和次数、使用地点、使用主体、使用行为、使用客体、衍生数据等六个方面的管控成为企业主要需求，其中使用主体（28%）、衍生数据（28%）、使用时间和次数（20%）成为前三大考量，这体现出对流通方案中的用户身份和应用程序认证、对新产生的数据归属界定、数据使用权限判定等方面提出了更高要求。

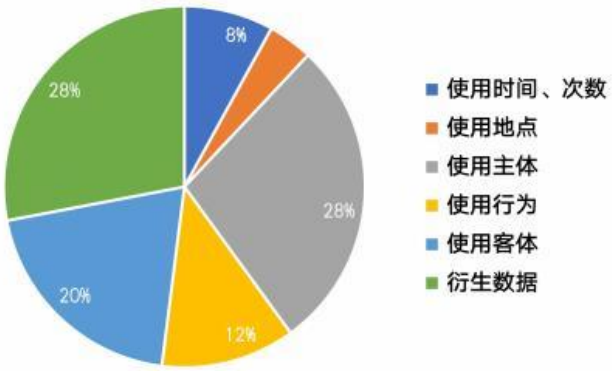


图1.3　企业在数据流通过程中期望的管控手段

从关键技术需求上看，企业目前对数据资产控制相关技术、可信环境相关技术、可信传输相关技术、身份认证相关技术、数据资产管理相关技术、日志存证及清算审计相关技术、供需对接相关技术、数据增值服务相关技术等八类技术最为重视，其中数据资产控制相关技术（27.19%）、可信环境相关技术（23.16%）、可信传输相关技术（22.15%）最受重视，表明实现数据流通过程中的过程可控，建立安全可信的存储传输环境是当前关注焦点。

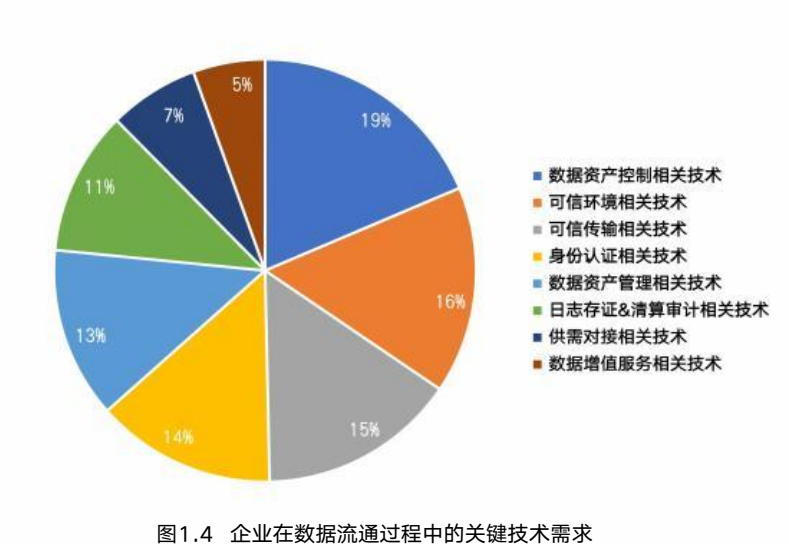


图1.4　企业在数据流通过程中的关键技术需求

从数据流通过程中是否引进第三方服务上看，企业对第三方服务仍存在较大需求，靠企业自身实现数据流通尚不现实，目前工业互联网平台（33%）、企业数据中台（29%）、数据交易服务机构（17%）是前三大数据流通服务提供商，这表明当前数据流通方案需要紧密和平台能力相结合，发挥各类平台在数据资源汇聚上的优势，形成体系化的数据流通能力。

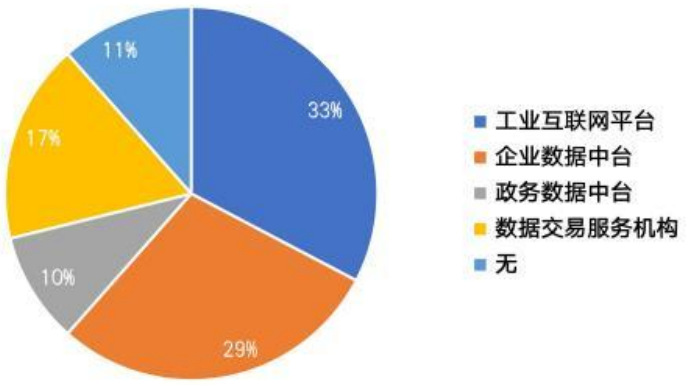


图1.5　企业数据流通过程中的第三方服务使用情况

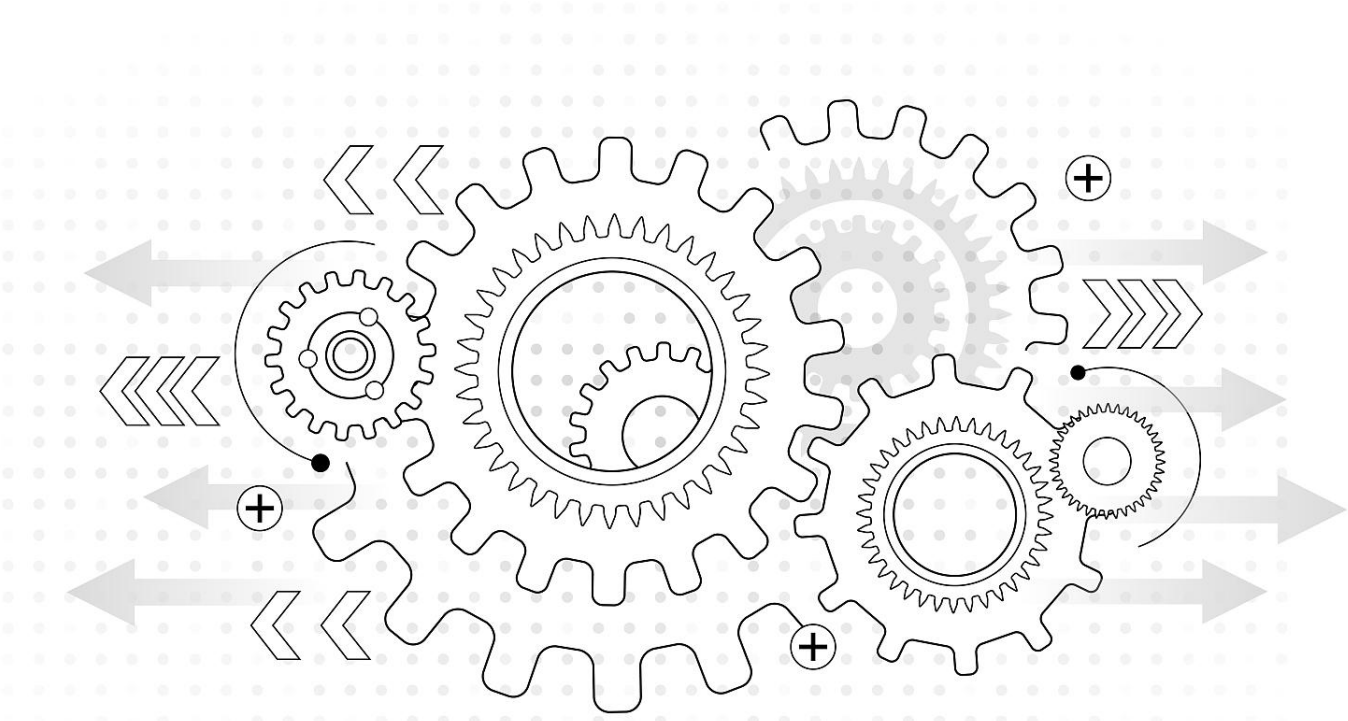
（二）发展工业数据可信流通能力是国家发展需要

当前，国家高度关注工业数据可信流通能力发展。习近平总书记强调，“系统推进工业互联网基础设施和数据资源管理体系建设，发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济。”《数据安全法》明确提出在保障数据安全有序流动的基础上，鼓励塑造数据自由流动的市场秩序。国务院先后印发《“十四五”数字经济发展规划》和《要素市场化配置综合改革试点总体方案》，明确将“以数字技术与实体经济深度融合为主线”纳入“十四五”时期推动数字经济健康发展的指导思想之中，探索建立数据要素流通规则。此外，工信部印发《工业互联网创新发展行动计划(2021-2023年)》，聚焦提升工业数据统筹汇聚能力，推动平台间数据互联互通。在此基础上，各地方紧跟推进，相继出台了相关地方性法规和管理办法，如《广东省数字经济促进条例》《上海市数据条例》等，促进产业数据共享流通。在多项政策和措施的引导下，工业数据共享流通的系统建设、技术研究、标准研制、应用推广、产业生态加速发展。

（三）发展工业数据可信流通能力是产业现实需求

通过面向工业数据提供方、使用方、服务方和监管方建立泛在连接，构建工业数据可信汇聚和应用网络，并基于统一规则实现对数据全生命周期的管理和控制，从而保障数据依法有序自由流动是激发实体经济潜能，培育实体经济新增长极的重要手段。我国是全球唯一具有工业领域全产业链的国家，**预计**到2025年，中国数据总量全球占比将接近30%，相比现在将提高超过20个百分点，其中工业、能源等价值互联网数据占比将达到80%。为推进工业数据共享流通的体系建设和产业应用建立了良好基础。

工业数据可信流通一方面催生新模式新业态，促进实体经济转型升级。通过形成产业链、供应链、价值链数据的互联互通，为实现数字孪生、人工智能等技术在细分行业中的新应用模式构建丰富的数据资源基础，提升数字经济对实体经济数字化转型的，融合赋能水平。欧盟预计通过数据空间等方式加强非个人数据流通，将在未来五年额外创造2700亿欧元、1.8%的GDP增长。另一方面助力新产业发展，实现实体经济扩容。工业数据可信流通体系通过各行业领域的数据、模型、算法的大范围交互，实现研发机构、企业等创新主体的协同创新，推动数字工厂、数字家庭、数字化医疗等新产品新产业发展。



（四）我国工业数据可信流通能力建设现状

产业上，多元化解决方案正在形成。一是传统互联网企业加强向产业领域适配。信息技术企业不断加强向制造、能源等重点行业领域的方案适配，并基于自身云和边缘能力，集成多种技术，形成产业数据共享流通方案。**二是安全类企业基于自身技术优势开发可信流通方案。**数据安全企业通过应用多方安全计算、区块链等技术，围绕数据可信交易、协同利用等方向，以建立多方数据联合训练平台的方式，实现数据安全传输以及模型的联合开发。**三是聚焦数据空间方案开发的专精企业开始涌现。**广东、江苏等地的一批新兴科技企业积极跟踪数据空间发展态势，相关产品化工作基本完成。

应用上，多场景空间应用逐步完善。一方面，聚焦研发协同，提高研发制造效率和产品竞争力。东方电气、中国电信联合建立研发数据空间，实现敏感研发模型的异地传输、使用过程控制与使用方式监督，解决了专人现场监督难的问题，有效打消数据提供方顾虑。**另一方面，聚焦产业链供应链协同，提升生产活动的快速响应能力和管控能力。**南京理工大学联合多家电子信息企业，构建仓储物流数据空间，打通上下游供应链的零部件数据共享壁垒，实现产线零部件的实时跟踪和关键数据交互，有效加速了产品交付。

生态上，产学研用各界初步形成合力。一方面，具有中国特色的数据空间架构体系达成共识。中国信通院联合产学研用各界积极开展中国数据空间的创新架构设计，兼顾了数据流通过程中的安全可信和监管需求，为建设符合中国行业、产业需求的，完全自主可控的数据空间发挥重要指导作用。**另一方面，国内数据空间生态联盟初步成型。**中国信通院、中国电信、华为、东方电气、北京大数据交易所、华控清交、北京交通大学等发起成立可信工业数据空间生态链，积极促进相关主体之间的交流和深度合作，持续推动方案开发和产业实践落地。

当前，仍有相当数量的工业企业对数据共享流通理念和定位认知不清，对技术特性和商业价值抱有疑虑，叠加我国工业企业数据质量差，底子薄的历史包袱，“不愿、不敢、不会”成为在企业间数据可信流动的主要障碍。亟需工业数据流通利用方案，为实现跨企业、跨行业的各类平台、产业主体之间的互联互通和数据价值充分挖掘提供示范和标杆。

第二章

Chapter 2

工业数据可信流通体系的内涵

（一）工业数据可信流通体系的意义和内涵

工业数据可信流通体系是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，解决数据要素提供方、使用方、服务方等主体间的安全与信任问题，进而实现数据驱动的数字化转型。

工业数据可信流通体系实现了产品全生命周期的应用场景涵盖，在系统层级上，建立工厂内，工厂外(B2B，B2C，B2G)数据的全链接；在数据管理上，实现对数据全生命周期的静态管理和动态控制，并保证了参与方行为可信、数据自身和使用过程可信；解决方案能力上，建立了数据-终端(软件、系统、硬件)-终端自组织网络-终端与中间服务平台间的解决方案体系，有助于打造数据流通的整体生态。

（二）从业务视角看工业数据可信流通体系

可信工业数据流通系统共有三种不同利益相关方，分别为数据提供方、数据使用方和中间服务方，每个利益相关方在可信工业数据流通系统开展不同的活动，如图2.1所示。

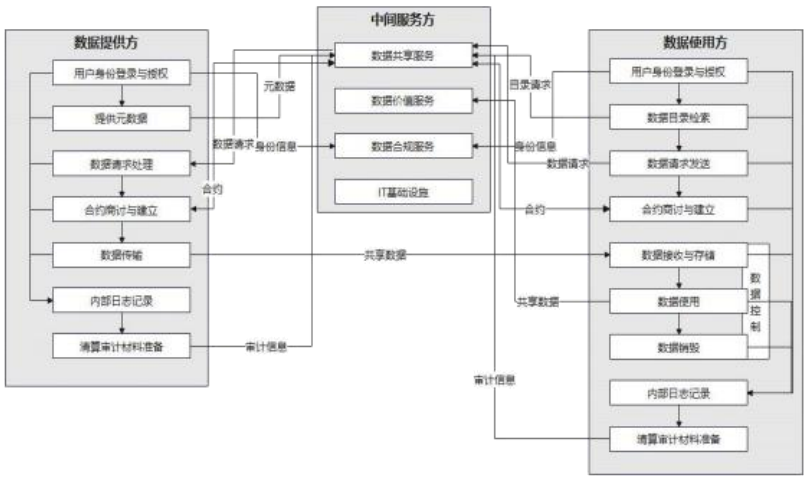
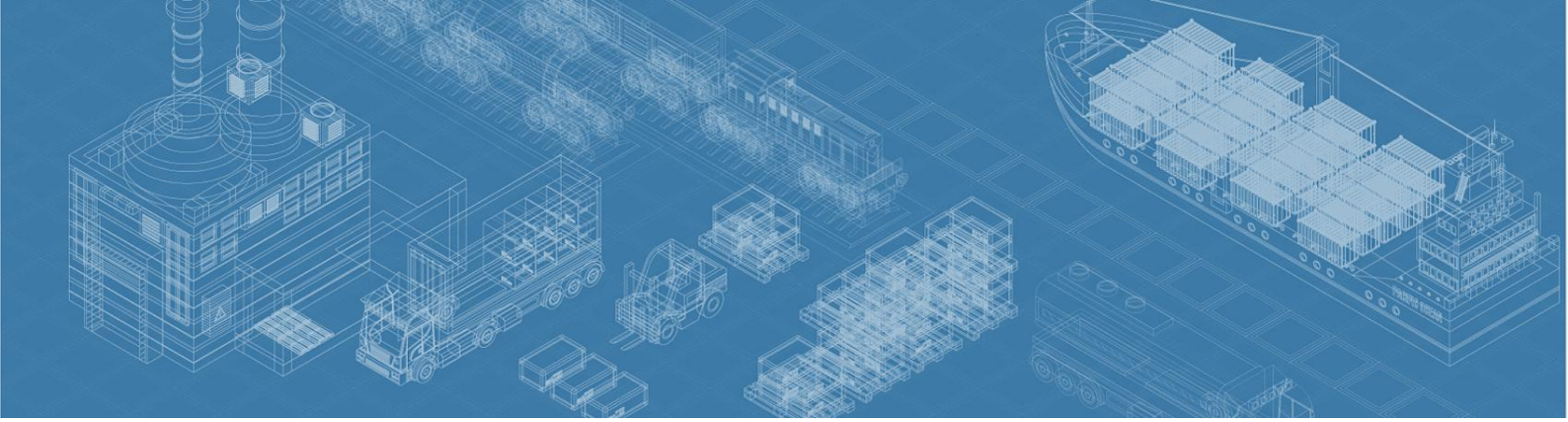


图2.1　工业数据可信流通体系的业务视角



数据提供方通过向中间服务方的数据合规服务方发送身份信息完成用户身份登录与授权，而后向中间服务方提供元数据并加入由中间服务方的数据共享服务方提供的数据目录服务。数据提供方从中间服务方获得数据共享请求，处理数据请求，通过中间服务方的数据共享服务提供数据共享合约或接受数据使用方发起的合约商讨请求并达成共识建立智能合约。数据提供方将共享数据传输至数据使用方。整个过程中每个活动发生时，数据提供方进行内部日志记录，并周期性进行清算审计材料准备，将审计信息提供给中间服务方的共享服务方进行审计。

数据使用方通过向中间服务方的数据合规服务方发送身份信息完成用户身份登录与授权，而后从中间服务方的数据共享服务方进行数据目录检索，向中间服务方中的数据共享服务发送共享数据使用请求。数据使用方可通过中间服务方的数据共享服务方接受数据提供方预设好的共享数据使用合约或通过中间服务方的数据共享服务方发起与数据提供方商讨共享数据使用合约的请求。数据使用方与数据提供方建立智能合约后，数据使用方接收数据提供方发送的共享数据并存储、使用、销毁，共享数据在数据使用方接收、存储、使用、销毁的过程中接受数据控制，数据使用方也可通过中间服务方的IT基础设施服务方对数据进行存储，通过中间服务方的数据价值服务方对数据进行使用。整个过程中每个活动发生时数据使用方进行内部日志记录，并周期性进行清算审计材料准备，将审计信息提供给中间服务方的共享服务方进行审计。

中间服务方提供数据共享服务、数据价值服务、数据合规类服务、IT基础设施服务。

（三）从功能视角看工业数据可信流通体系

数据可信流通具有鲜明的功能需求，具体来看。主要包括身份认证功能、供需对接功能、数据资产管理功能、数据资产控制功能、日志存证功能、清算审计功能、可信传输功能、可信环境功能。

1. 身份认证功能

身份认证功能是对利益相关方用户身份、用户设备进行认证的功能，以确保接入成员的身份可信。其主要包括用户登录管理、身份信息验证、用户身份管理三大子功能。

1.1用户登录管理：用户通过输入用户名、密码、口令等登入系统。

1.2身份信息验证：身份认证服务器对数据提供方用户身份、用户设备进行认证的功能。

1.3用户身份管理：系统对已注册用户、设备身份管理的后台功能。

2. 供需对接功能

供需对接功能是在数据提供方和使用方间进行精准对接并进行供需合约的协商和确定的功能，以明确数据流通要求并对据此对数据活动进行限制。主要包括数据目录管理、智能合约协商与生成两大子功能。

2.1数据目录生成管理：数据提供方用自己的元数据进行数据目录生成与管理。

2.2智能合约协商与生成：数据提供方和使用方就有意向共享的数据，进行数据流通合约谈判，确定共享数据使用要求，并生成对应智能合约的功能。合约商讨模式可为数据提供方预设共享条件，使用方接受条件达成共享合约或数据使用方或数据使用方发起合约商讨，双方协商后达成共享合约。

3. 数据资产管理功能

数据资产管理功能是对数据资产生成到销毁的全过程对数据进行管理的功能，以保障数据内外部使用和交换一致性、准确性、可靠性。主要包括数据预处理、数据资产标识和校验、数据资产描述三大子功能。

3.1数据预处理：对数据资源进行脱敏、加密、获取计算因子或特征因子等隐私化处理。

3.2数据资产标识和校验：对数据资产进行标识并在流通过程中对标识实时校验。

3.3数据资产描述：对数据资产的进行描述，并对资产变化情况、操作情况进行实时更新。

4. 数据资产控制功能

数据资产控制功能是基于供需双方签订的智能合约，通过机器可读的代码，控制数据对象的使用范围和方式的功能，以保证数据提供方的数据主权。主要包括使用策略配置、数据状态监控、控制策略执行、数据销毁三大子功能。

4.1使用策略配置：根据合约要求，为共享数据配置对应使用策略。

4.2数据状态监控：对于数据使用方在数据使用过程中的使用时间、方式、范围等进行实时监控。

4.3控制策略执行：按照智能合约要求，通过数据控制技术对数据访问和使用的方式、范围等进行限制和管控。

4.4数据销毁：数据流通合约结束后，对数据提供方以外留存的相关数据以及其副本进行不可恢复销毁或权限回收。

5. 日志存证功能

日志存证功能是对数据提供方、使用方、中间服务方等参与方的数据传输、共享、使用等活动进行存证的功能，以为审计清算等活动提供依据。主要包括日志本地记录、日志传输与解析两大子功能。

5.1日志本地记录：对数据的使用过程数据提供方、使用方、中间服务方等参与方的数据传输、共享、使用等活动进行本地存证。

5.2日志传输与解析：将本地日志上传至中间服务方，并以日志为依据为数据流通活动的清算计量提供参考。

6. 清算审计功能

审计功能指在数据共享流通过程结束后，对数据使用情况、参与方行为等方面进行校验和核查工作的功能，以保障数据流通活动按约履行、按约结束。主要包括活动记录清算、资金审计与支付、流通结束评价三大子功能。

6.1活动记录清算：根据日志等记录，根据智能合约规定，对数据使用情况、参与方行为等进行核查，确认是否出现违约情况，并进行判断。

6.2资金审计与支付：根据数据活动的清算情况，实现对资金进行冻结、解冻、支付等。

6.3流通结束评价：流通活动结束后，参与方对数据资源、流通情况等进行评价。

7. 可信传输功能

可信传输功能是指数据使用方、数据提供方和/或中间服务方之间进行数据、元数据、智能合约等安全通信的功能，以保障数据传输过程的安全可信。

8. 可信环境功能

可信环境功能指数据在数据使用方存储、使用的过程中与外部环境进行隔离的功能，以提供安全的数据使用环境。主要包括可信执行环境、可信存储环境两大子功能。

8.1可信执行环境：通过硬件层、系统层、软件层等隔离手段，使共享数据或使用共享数据的程序在运行过程中与其他数据或程序隔离。

8.2可信存储环境：加密或硬件隔离的存储环境。

第三章
Chapter 3

工业数据可信流通的应用场景和主要模式

（一）工业数据可信流通的主要场景梳理

推进数据空间的过程中，处于数字化转型中的行业企业不断挖掘研究数据空间中数据可信流通过程中内涵和价值，以解决实际需求和痛点为出发点，已经探索出了一批兼具示范效应和推广价值的数据流通应用场景。各场景通过数据空间纵向打通个人、企业内外、政府间数据可信流通、汇聚及协同，横向贯穿设计、生产、物流、销售、服务整个产品全生命周期中多业务、多领域环节，开展应用改造和创新，形成具有工业数据可信流通的三大层级，包含产品数字化交付、生产集中管控、供应链协同优化、设备资产全生命周期管理等主要场景，推动企业实现业务流程和商业模式的改造或重构，带动企业实施转型升级，实现降本提质增效减存，并不断催生新的增长点。具体工业数据流通场景情况见图3.1。

图3.1　典型工业数据流通应用场景

（二）工业数据的三大主要流通模式

工业数据流通的场景，有众多的场景因子。从目前众多工业企业的实践来看，通常包括如下场景因子：数据的类型、数据的采集方式、数据的交换模式、数据的使用主体、数据处理的软件能力类型以及数据流通基础设施环境等，最终汇聚形成如下三种数据流通模式。

图3.2　工业数据流通主要模式

一是复杂企业内部高密高价值数据流通模式。复杂组织内部通常分工侧重点明显，不同部门之间对应不同的业务流程和业务作业领域，如研发部门负责产品研究及设计、采购部门负责各个部门的部件采购、营销对口CRM等，不同业务部门所管理业务产生的核心数据构成了企业核心竞争力，业务域之间的有效协同通常也会涉及到高密高价值数据，依赖数据可信交换流通。通常是基于结构化数据集，通过系统集成/人工上传方式，使用通用的数据加工软件进行简单的分析计算提取有价值信息。

二是企业间支持业务协同下的数据流通模式。从企业内扩展到企业间，同样存在高密高价值的数据交换，通常是通过数据的价值再造(探索新的商业模式、业务创新、产品改进等)，由消费方主导，提供方协同，双方是协作关系，与传统企业B2B的业务合作有显著差异，如投资领域的尽调材料交换、审计领域的审计原始材料管控等。跨组织高密数据传输，与1)相比，通常包含了一些专业数据处理软件或者AI提取技术以获取有价值信息。

三是大型组织主导的生态数据交互流通模式。大型企业或者产业领头者越来越多的将平台模式及其周围的生态系统构建作为战略重心。在此场景下，作为生态圈的核心和众多生态成员之间，既有在生态圈内进行广泛的业务协作背景下需要高频的进行数据交换，又有对各生态成员数据泄漏的担忧。因此，也亟需一套可控数据交换系统来支持生态的安全和持续发展。生态内的场景差异更多地体现在数据的交换模式和基础设施环境。

第四章
Chapter 4

工业数据可信流通应用案例

（一）工业数据可信流通应用案例汇总

表4.1　工业数据可信流通应用案例情况汇总

案例名称	行业	参与方	模式	场景	服务范围	数据类型	数据敏感度	主要应用价值
港口物流运输数据可信共享流通案例	交通运输业	数鑫科技、某港口集团	企业内数据流通	港口多式联运数据共享	港口、铁路、运输公司（公路）、船公司（航运）	数据表等结构化数据	中	港口装卸作业效率提升、运输成本降低
家电业多系统数据对账验证协同优化案例	家电制造业	四川长虹	企业内数据流通	家电业多系统数据对账	工业生产、仓储物流	流数据	高	异常快速定位、责任精确定位、数据可信溯源
建筑陶瓷行业文件类数据可信流通案例	建筑陶瓷制品制造行业	宏宇陶瓷、一知安全	企业间数据协同	建筑陶瓷行业文件流通	设计厂商、制造商	文件类模型数据（文件类数据）	中	安全可靠的研发数据传输，实现合作生产
航空公司平台间油耗预测模型共享案例	交通运输业	中国电信、国内某三大航空公司	企业间数据协同）	航空公司油耗模型共享	航空公司飞机制造商和购买者	文件类模型数据（流数据/文件类数据，具体数据格式）	高	安全可靠的研发数据传输，实现平台间模型数据共享达到航司燃油使用预测性维护目的。
家纺行业设计生产一体化可信共享案例	纺织业	江苏金太阳纺织科技有限公司	企业间数据协同	家纺行业文件数据流通	设计公司、制造商	图纸文件类数据	高	解决图纸类数据传输后无法控制传播范围、使用方式、底稿留存等问题
华为鲲鹏/昇腾计算产业生态数据空间	电子信息业	华为、长虹、同方、宝德、新华三等15家参与方	生态数据交互	全环境数据可信交换	鲲鹏/昇腾计算产业生态中芯片/单板/部件商，OEM整机制造商	结构化数据集、非结构化文件	高	1、提供各参与方平等的可控可信可证的交换平台 2、实现敏感数据从不敢传递到可信传递，释放敏感数据的价值 3、实现更多数据类型的可信交换和全流程不同场景的快速协同
电子信息业产品自动化联合质检案例	电子信息业	熊猫电子产业集群	生态数据交互	多厂商联合质检	制造业厂商	工业模型	高	各厂商通过数据共享进行质检模型的联合训练，并进行自动化质量检测，实现降本增效
电子信息业供应链金融用户画像案例	电子信息业	中企云链	生态数据交互	供应链金融用户画像生成	供应链上下游企业	加密数据（流数据/文件类数据）	高	基于用户真实可信身份的用户画像

（二） 企业内数据流通模式下的典型案例

案例一：港口物流运输数据可信共享流通案例

1. 背景介绍

面向物流领域，港口多式联运场景。其中涉及港口、铁路、运输公司(公路)、船舶公司(航运)四方物流运输、港口作业相关业务数据共享流通。港口作为数据使用方，希望实时、安全、合规获取各方物流数据，并且方便与自身数据融合计算，以统一标准方式给到相关业务系统使用。而以铁路为主等数据提供方希望数据安全合规共享，自身能最大限度控制数据使用方式范围，及全过程可追溯。该场景主要采用去中心化、可信、可控、可追溯的新型数据空间模式，数据共享交换、可信多方计算等技术手段。

2. 案例建设主体

港口、铁路、运输公司(公路)、船舶公司(航运)四方

3. 案例建设目标

物流领域的港口多式联运场景，实现、安全、合规获取各方物流数据，并且方便与自身数据融合计算，以统一标准方式给到相关业务系统使用。

4. 案例整体情况

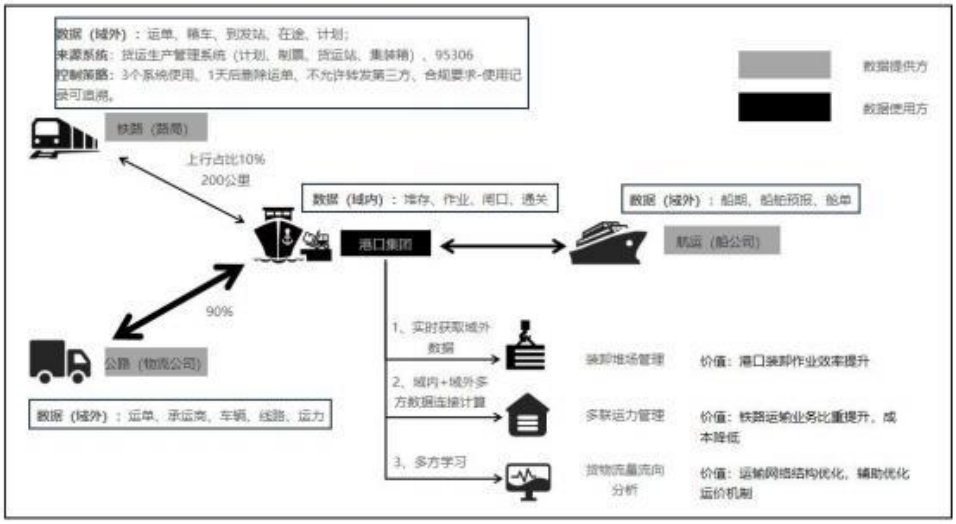


图4.1 案例部署方案

4.1应用场景：四方数据共享流通。铁路数据：运单(加密)、箱车、到发、在途、计划。公路数据：运单、承运商、车辆、线路、运力等。航运数据包括：船期、船舶预报、舱单等。多方数据通过安全通道传输到港口，与港口堆存、作业、闸口、通关等数据连接计算，内存中加工处理后输出货物装车、预确报、实时位置、物流轨迹、流量流向等明文或加密脱敏数据，供港口业务系统调用。

4.2当前痛点：铁路运输数据安全合规要求高，港口现有数据API接口共享流通方案不能满足铁路安全合规管控要求，港口上行货品通过铁路转运业务占比不足；大宗货物通过航运到达港口后只能选择公路运输，无法实现成本最优运输；港口不掌握品类及货物，各货运代理企业、货主等客户无法实时获得货物状态，且无法及时准确享受到政策优惠；精准判断预测货物流量流向已成为港口竞争关键因素。

4.3部署方案：建立铁路、运输公司、船公司、港口四方可信数据空间分发及控制平台，各节点分别部署，集成加密脱敏模块组件；

4.4案例应用的重点技术和应用情况：完整实现事前、事中、事后全链路数据控制及追溯。事前签订合同，合同中约束转为控制策略，如：铁路所要求的数据使用控制策略，包括：允许港口装卸堆场、多联运力管理、货物流量流向分析等3个系统使用、1天后删除运单、不允许转发第三方、合规要

求使用记录可追溯。事中机器自动解析策略执行，发现双方约定策略不满足情况下中断流通会话，事后通过审计日志追溯。

4.5方案自主研发性、创新性及先进性

5. 应用成效

- 港口实时获取域外数据，为装卸堆场管理堆存、作业、闸口、通关等业务提供支撑，提升港口装卸作业效率；
- 安全沙盒内实现域内+域外多方数据连接计算，为港口多联运力管理提供支撑，助力港口铁路运输业务比重提升，成本降低；
- 通过集成各类机器学习框架实现多方学习，各方数据联合进行货物流量流向分析，帮助港口实现运输网络结构整体优化，辅助优化运价机制。

案例二：家电业多系统数据对账验证协同优化案例

1. 背景介绍

随着工业物联网逐步走向成熟，数据成为整个工业生产流程中的关键因素。数据驱动的工业系统通过终端设备和其他业务系统采集数据，加以分析和优化，在提升效率的同时减少劳动力成本。为支撑可靠的生产和业务决策，实现跨系统的协同办公，一方面需要实现工业数据的完整性和一致性，一方面需要确定跨域数据的权责。

多系统数据可信对账验证案例是在传统多系统信息交互保障方案基础上进行的技术优化，通过引入区块链和分布式账本技术，增强数据从产生、交互、审计、溯源、修复全流程的可靠性。主要包括分布式存储、数据完整性保护以及数据一致性验证等核心功能。

2. 案例建设主体

四川长虹电器股份有限公司

3. 案例建设目标

多系统数据可信对账验证案例为供应链管理、信息交互、产品全生命周期管理、物流溯源等工艺协同优化场景提供分布式数据流通方案，明确跨系统的数据权属，实现数据的异步同步，解决流通数据的加密完整性、不可抵赖性和信息交互一致性问题。

在各主体部署区块链节点，依托多方共识算法，确保多系统数据副本的一致性；部署业务智能合约，实现秒级的自动化数据分析与比对，精确定位对账过程中不一致数据；基于分布式账本技术，链上存证对账过程数据和结果，支撑事后审计及多方系统定责、追责。

4. 案例整体情况

4.1应用场景：案例适用于多系统之间数据不一致的可信对账验证。目前，工厂每日产线运转前，需人工从多个系统导出日志数据进行人工比对，无异常情况下开始工作，若有异常需确定异常原因，并做对应修复，因此，需要能提升效率的跨系统的数据可信对账验证解决方案。案例能在保障数据可信使用的基础上，有效减少时间和人力的消耗，提升产线的整体工作效率。

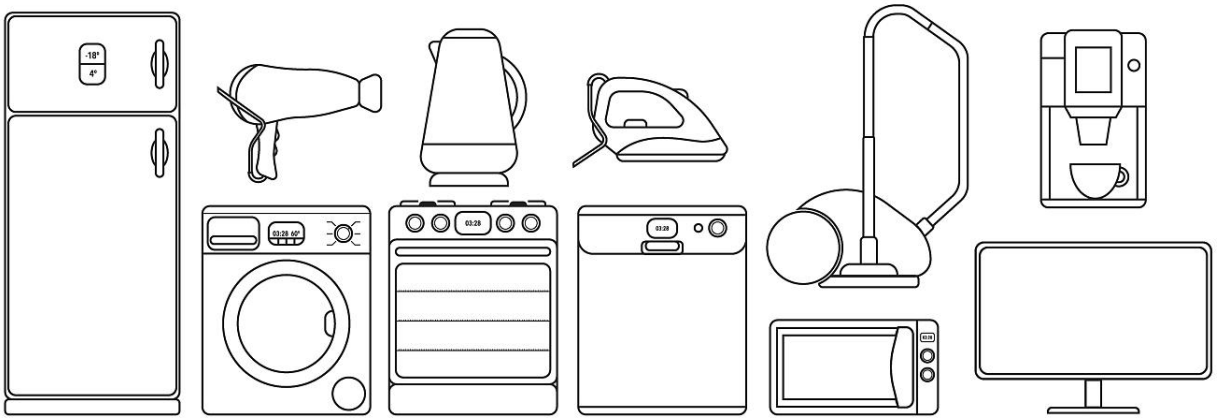
4.2当前痛点：业界目前常用的原生系统消息验证、集中式批量验证等信息交互一致性解决方案无法满足实际业务场景中不断增加的对度量实时性、结果公信力、业务可扩展性的诉求。具体应用痛点主要体现在下述四个方面:

(1)数据来源真实性无法保障。传统的数据一致性验证的数据来源是通过网络传输获取的，数据的初始来源是否真正的业务系统，在传输过程中是否被篡改，缺少强有力的保障。

(2)数据交互一致性验证结果缺少公信力。当前依靠单一系统的数据交互验证，给出的结果易受系统权限泄露、业务员恶意篡改、系统自身故障等多重潜在问题的影响，难以保证结果的公信力。

(3)结果溯源难。由于系统间交互存在潜在的网络故障、人为干扰、系统不稳定等因素，不易准确获取数据交互过程中的各个状态，定位引起错误结果的原点。

(4)数据修复缺乏可信基准。由于各方都是单一系统对比给出的比对结果，都存在单个系统出错的可能性，难以确定可信基准进行数据修复。



4.3部署方案：多系统数据可信对账验证应用共有三种不同利益相关方，分别为数据提供方、数据使用方和中间服务方。其中，数据提供方是进行业务活动的各工业系统，如WMS、ERP、MES等系统；数据使用方是产线上进行操作的业务员；中间服务方是提供多系统数据可信对账验证系统的软件提供商。部署架构图如下所示：

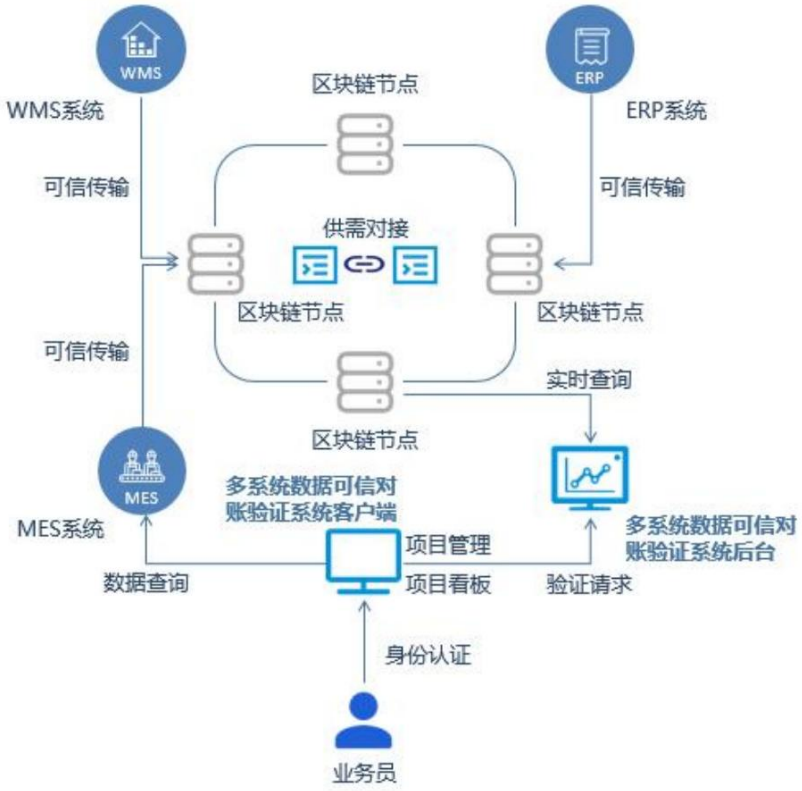


图4.2 多系统数据可信对账验证系统部署架构图

多系统数据可信对账验证系统通过搭建可信执行环境和可信传输网络，在后台实现数据资产管理和供需对接，面向业务员提供系统管理、用户管理、数据查询、对账验证项目管理、对账验证项目看板等业务操作功能。其中，系统管理实现了数据的清算审计和操作日志的存证。用户管理实现了数据使用方的身份认证。数据查询、对账验证项目管理、对账验证项目看板实现了数据使用方对数据资产的控制。

制造业中间服务模式下，业务员通过向可信对账验证系统客户端发送身份信息完成用户身份登录与授权，而后通过可信对账验证系统后台实现

数据目录检索，并通过可信对账验证系统客户端发送对账验证请求。业务员可通过可信对账验证系统内的对账验证项目调用MES系统、ERP系统、WMS系统预设好的对账验证合约或自己定制对账验证规则合约，并向MES系统、ERP系统、WMS系统发起数据使用合约的请求。业务员与MES系统、ERP系统、WMS系统建立供需对接后，业务员接收MES系统、ERP系统、WMS系统发送的工业业务数据并存储、使用、销毁，工业业务数据在业务员接收、存储、使用、销毁的过程中接受数据控制，业务员也可通过可信对账验证系统客户端对数据进行存储，通过对账验证项目对数据进行使用。整个过程中每个活动发生时可信对账验证系统进行内部日志记录，并周期性进行清算审计。

表4.2 系统数据可信对账验证案例数据控制细则

时间	存放时间	6个月
	存放时长	无限制
	使用次数	每天一次日志对账
地点	主网环境	长虹集团内网
	子网环境	长虹工厂生产内网
	接入点	有线网络
	接入设备	机房交换机，服务器
	设备软硬件环境	软件：linux centos7.x 硬件：1.系统应用服务器 (1)x86_64架构，CPU≥4核，内存≥8G，硬盘≥4T (2)千兆电口≥1 2.区块链服务器 (1)x86_64架构，CPU≥8核，内存≥16G，硬盘≥2T (2)千兆电口≥1
主体	进程	
	用户	工厂业务人员
行为	读取	用户读取对账验证结果、原始日志信息
	修改	修改对账状态，进行手工平账处理
	执行	系统自动执行对账任务
	删除	系统提供删除对账任务，提供数据定期删除
	转发	系统通过邮件向用户转发异常告警信息
	复制	用户复制下载对账验证结果、异常告警信息到本地
	其他	
客体	数据对象	日志数据，流量数据
	数据内容	物料代码、工厂代码、物料描述、物料的入库、出库、移库信息、对账信息

4.4案例应用的重点技术和应用情况：为保障多数据数据可信对账验证系统应用的运转，重点应用了下述2项关键技术：

(1)智能合约一致性校验技术。深入分析业务系统数据交互格式，提取关键参数，抽象为规则化的业务智能合约，实现数据流的自动解析与实时比对，并对结果进行链上存储。

(2)基于身份标识的溯源技术。建立基于区块链的全局唯一标识，支持链上可验证。进一步研究Merkel树机制，实现基于摘要的数据快速检索机制，支持链上数据的有效输出。

4.5方案自主研发性、创新性及先进性：本方案结合区块链的技术特征，提出基于区块链构建新型信任架构，在多方交互场景中实现可信数采、传输验证、审计溯源、自动修复等技术创新性应用。本方案通过自动执行智能合约，将之前T+1周期内对账提升为秒级对账，用机器信任代替了个人信任、制度信任，在多系统数据交互中实现快速定责。同时，提供数据的可信验证，快速定位异常数据，实现数据可信溯源。为减少对原有业务系统流程的影响，本方案使用了旁路上链的方式，保障了项目的顺利实施。

5.应用成效

多系统数据可信对账验证应用已在长虹河边智能产业园完成部署并正在生产环境运行调试，该组件在两台服务器上虚拟8个区块链节点，为智能电视生产线提供MES、ERP、WMS多系统的成品库存自动化验证服务，将数据验证周期从“T+1”日提升至“T+0”日秒级。应用上线运营时间超1年，减少因对账的误工时间超60工时，预估增加成品产值超2600万。

方案计划于2022年12月在两个园区形成项目示范，并于2023年在其它工业场景推广方案成果。

（三）企业间数据协同模式下的典型案例

案例一：建筑陶瓷行业文件类数据可信流通案例

1. 背景介绍

文件型数据可信流动场景，目前工业数据共享面临着巨大的挑战，难以保护数据所有者利益是其中最大的一个痛点：在工业数据共享时，数据提供方对数据是否被用于合同目的之外，商业情报随数据泄漏、技术随数据流出，以及接收方对数据保管不善等方面存在较大的顾虑。

2. 案例建设主体

数据提供方：宏宇陶瓷(陶瓷制造业)

数据接收方：合作方、生产代工方

3. 案例建设目标

基于工业数据空间的文件型数据可信流动场景。测试目标是陶瓷制造业的研发设计数据需要给到合作方和生产代工的企业，数据所有者可以控制数据使用策略(打开次数，时间)，远程清除传输的数据，以及避免数据被数据接受方未授权外发。

4. 案例整体情况

4.1应用场景：案例适用于工业数据共享场景，在工业数据共享时，数据提供方对数据是否被用于合同目的之外，商业情报随数据泄漏、技术随数据流出，以及接收方对数据保管不善等方面存在较大的顾虑。需要一种可靠的控制手段保障数据的安全流动。

4.2当前痛点：针对文件型数据流通的场景，例如某企业需要将配件图纸文件发送给另一个企业进行生产，目前经常采用U盘、邮件等方式进行数据共

享。但使用U盘进行物理传输，再由专人进行U盘的配送监督，以及数据的用后删除，不仅费时费力，且共享效率很低；而采用邮件等网络传输，又无法对发送后的数据进行严密的管控。另外也有采用文件加密的手段实现数据传输，但是文件加解密效率比较低，且解密后的文件内容也无法得到有效控制。

4.3部署方案：

针对文件型数据，搭建一个文件共享服务平台，满足身份认证、安全传输、文件共享策略的管控以及审计日志的记录。在数据流通传输的环节中，基于端到端的安全架构和隔离沙箱技术，在跨组织文件型数据分享中可以实现数据在发送、传输、使用、销毁过程中进行安全管控，保证数据不泄密。

在传输过程中，在空间内进行共享文件数据的策略配置。如文件的发送和接受、限制文件的使用策略、限制文件从空间内流出等。实现从数据的传输到数据的使用进行全生命周期的防护和控制，规范使用者操作。主要包含以下5点：

1.企业双方共享数据之前需要进行身份认证；

2.数据提供方可将数据安全传输到数据接收方，可控制数据不被发送给第三方；

3.数据提供方可对数据使用方式进行控制，限制使用时间、使用次数等；

4.可跟踪数据使用状态，记录发送日志、接收日志、策略执行日志等；

5.数据接收方收到的数据只能在安全空间内打开，文件不能随意外发，文件使用到期后自动删除。

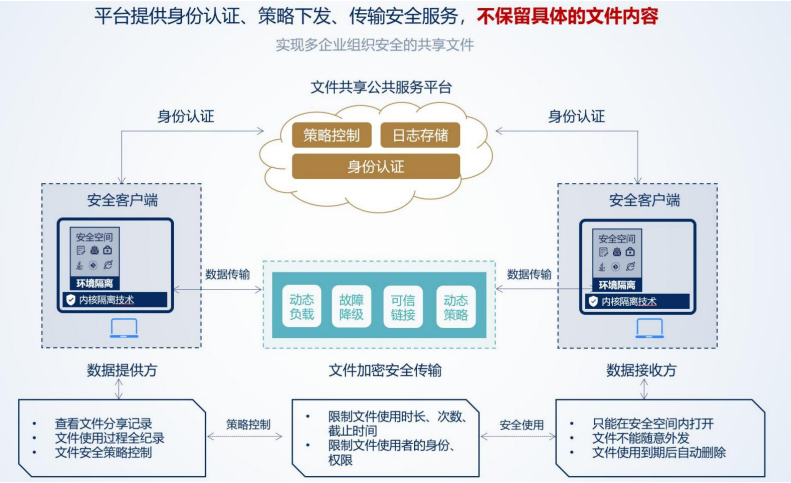


图4.3 案例部署方案

4.4案例应用的重点技术和应用情况：案例应用的重点技术：安全传输的客户端均采用数据沙箱技术，在数据提供方和接收方的终端空间上创建一个安全隔离的数据使用环境，通过安全加密传输，使得数据只在安全的使用环境中流动，数据提供方可以针对流通的数据进行安全策略控制，数据使用方需要在安全的环境中使用数据，实现数据“可用不可得”。

4.5方案自主研发性、创新性及先进性：可信环境相关技术(数据沙箱)通过在终端创建一个与个人环境(网络、文件、进程、模块、用户、会话、外设)完全逻辑隔离的安全域，域内所有数据进行加密存储；通过内核隔离技术以及对安全域本身的加固机制，防止数据被破坏及外泄。同时，对域内的行为执行安全策略控制和持续审计监控。实现在域内能安全的访问和使用企业敏感数据。

5.应用成效

应用提供了企业与合作方，代工方之间的数据可信传输，安全使用的解决方案，替代了之前企业采用U盘，邮件，文件加密等手段。解决了之前文件数据传输效率低，传输后不受控的问题，大大提高了跨组织数据流动的安全性和效率

文件型数据可信工业数据空间解决方案，提供了一个安全易用的数据流通方式。使用过程中终端构建出隔离的安全空间，空间内的数据和网络独立于终端环境，数据共享的双方均必须在可信空间内进行数据使用，数据提供方可以按需针对数据进行策略控制。实现数据安全流动的效果。

案例二：航空公司平台间油耗预测模型共享案例

1. 背景介绍

国内某航空公司A提供飞机采购服务，航司B和C在航司A处购买飞机后会回传QAR、巡航燃油流量表、巡航最佳高度表等数据到航司A的数据分析平台。航司A使用这些数据不断优化不同客观环境下飞行方式的燃油消耗模型。最终给出预测结果，同步给航司B和C数据平台实现航飞降本。

2. 案例建设主体

航司A为共享数据提供方，航司BC同时为原始数据提供方和模型预测数据使用方，无第三方平台介入。

3. 案例建设目标

基于工业数据空间的航空公司平台间油耗预测模型共享案例是为了实现不同数据平台环境中，航空公司核心燃油模型预测数据的安全可信传输，包括但不限于数据所有者可以控制数据不被发送给第三方、数据所有者可以根据需求在一定时间内撤回数据、数据所有者可以实现对数据使用状态的全程监控等，最终达到数据安全可信共享的结果。

4.案例整体情况

4.1应用场景：案例适用于不同平台之间数据流通共享场景下的工程模型数据的可信传输。目前在进行跨平台工业数据传输时，由于数据敏感度较高，数据提供方为保障数据隐私性，会使用较为复杂的传输审批以及数据加密机制，导致数据共享效率较低，因此需要能提升效率的可信传输解决方案。案例能在保障数据可信使用的前提下，有效简化传输流程，降低工业数据跨平台传输的成本。

4.2当前痛点：航司数据平台有数据保密需求，数据提供方对数据共享给同行业的数据平台有安全顾虑，希望设立保密环节，数据共享要通过层层审

批和加密才能通过数据接口方式共享出去，且无法精准控制数据使用细节以及数据使用方式。

4.3部署方案：数据使用方和数据提供方需要在各自的数据平台网络网络可达的环境中部署可信连接器。数据开放时数据提供方要指定数据的使用主体(航司BC)和使用控制策略(使用时长限制)，使用日志会保存在本地并且同步一份到记录流转中心。提供数据流通处理的日志存证，提供内外部合规记录，实现数据资源有效管理。

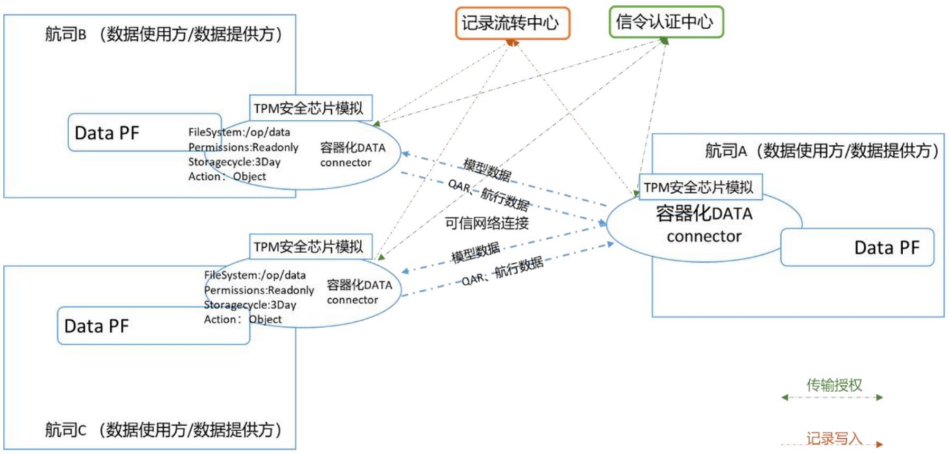


图4.4 案例部署方案

表4.3 数据控制情况

时间			地点					主体		行为							客体	
存放时长	使用时长	使用次数	主网环境	子网环境	接入点	接入设备	设备软硬件环境	进程	用户	读取	修改	执行	删除	转发	复制	其他	数据对象	数据内容
根据保密要求数据存放三天	--	--	--	--	--	--	--	通制服务器指定进程读取数据	--	只允许读取数据	不允许对数据进行修改	不允许对数据进行执行	不允许对数据进行删除	不允许对数据进行转发	不允许对数据进行复制	不允许对数据进行其他操作	控制对数据对象整体的操作	--

4.4案例应用的重点技术和应用情况：本方案中主要使用了

- 基于可信链接协议的数据通信技术
- 基于TPM/TCM的数据传输加密技术
- 基于容器化技术的可信连接器构建技术
- 基于目录文件级别的数据控制策略技术
- 可信链接器的授权认证技术

4.5方案自主研发性、创新性及先进性：

（1）自主研发性

- 连接器开发过程中，允许自主编译源码并打包，在工程中可自定义修改或添加功能
- 使用docker容器技术和docker-compose容器管理工具，可通过修改配置文件实现对连接器部署方式、部署架构和网络连接的调整
- 数据使用策略机制来自连接器接收的数据流控制策略，可实时设置和更新
- 数据路由规则文件使用外挂方式创建，数据链路可自主构建与修改

（2）创新性

- 自研的基于容器目录的数据访问策略机制

5.应用成效

案例建设前，数据共享环境不安全，需要航司内部层层审批，且无法控制数据共享的细节，数据无法做到完全可控可管。

案例建设后，基于可信环境的数据共享技术，航司数据共享审批流程缩短，能够精准控制模型结果数据的开放对象、开放时间、开放的行为，极大地满足了数据共享对安全性的需求。

方案可着力平台间数据共享场景进行推广，满足客户对数据共享的安全性和可控性的顾虑。

案例三：家纺行业研发数据流通管控案例

1. 背景介绍

家纺产业具有产业集群效应与垂直效应明显、企业规模普遍较小、信息化程度低、劳动密集等特征，就数据流通场景而言，企业向工厂传输图纸类数据后无数据的管控，令企业有较多数据泄露的担忧，在江苏金太阳搭建基于设计图纸远程管控的可信数据空间案例，对于探索构建家纺行业数据空间有重要意义。

2. 案例建设主体

江苏金太阳纺织科技有限公司作为应用场景提供主体，中国信息通信研究院作为建设支撑单位。

3. 案例建设目标

金太阳应用可验证可信数据空间对于图纸类数据的管控能力，解决企业在设计图纸传输使用中存在的实际问题。当前，在将分层图、设计图等传输到工厂后无法管控，企业担忧数据在使用之后工厂进行留存、复制、转发等操作，导致商业秘密泄露。建设可信数据空间金太阳应用，通过构建可信执行环境、构建智能合约以及配置数据控制组件等完成对设计图纸的全生命周期的管控，促进相关行业图纸类数据安全传输与可信使用。

4.案例整体情况

4.1应用场景：案例应用于企业之间图纸类文件的可信传输与使用控制。当前金太阳(数据提供方)将家纺设计图、分层图提供给代工厂(数据使用方)，使用的是线上传输，并由代工厂打印图纸，为企业提供进行数码印花服务，然而由于无跨域管控图纸传输后的手段，图纸之后的传播范围、使用方式无法确保安全可信，导致商家机密与知识产权具有泄露的风险，因此需要可以提高图纸文件数据传输与使用安全的解决方案。

4.2当前痛点：设计图纸类文件作为价值的数据，进行传输后无法管控图纸的使用范围、访问范围、使用时间、访问程序白名单、使用次数、读写权限配置、截录屏限制、访问IP权限配置、复制粘贴等行为，造成图纸类文件传输后泄露的风险大大增加，导致商业秘密泄露，市场同质化产品增加，企业竞争力下降等一系列问题。

传统的处理方式是通过业务员人工传输，并监督使用，或者将数据手动加密之后再进行传输，并将密钥收到分发给数据使用方，收到密钥的数据使用方对数据进行解密使用，但以上方式不但增加了成本，密钥泄露后任何得到密钥的人都可对数据进行使用，同时数据解密后仍可以随处复制，修改，图纸文件二次贴牌与知识类产权泄露无法得到有效解决，图纸安全传输与合规使用仍是数据使用方的痛点。

4.3部署方案：金太阳应用从系统架构上分为中间服务平台与可信数据空间使用端两部分内容，总体架构如图所示：

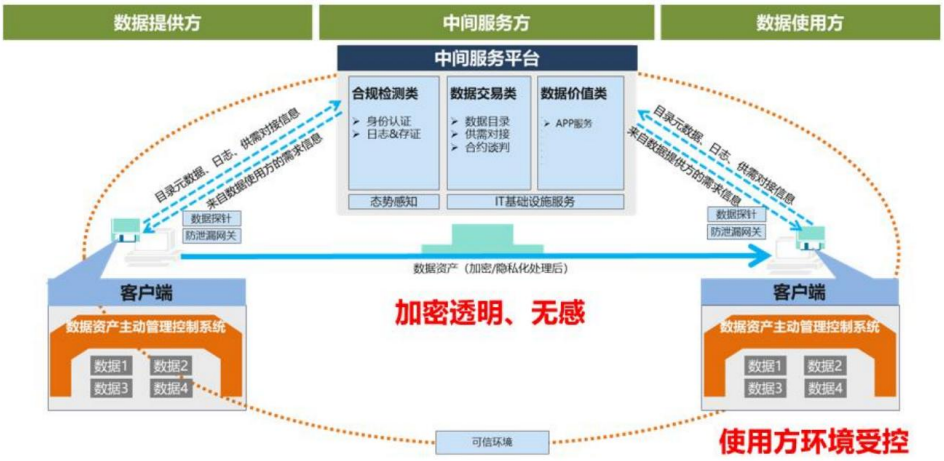


图4.5 案例部署方案

实施方案主要有两个核心模块，即中间服务平台以及客户端，支撑整个数据资源的流转、共享和使用管控。其中客户端是对数据实现贴身保护的主体，主要进行数据资产控制子模块的搭建以及可信环境的搭建。数据资产控制子模块搭建决策引擎PDP、拦截器PEP、执行器PXP等为数据提供方提

供跨域控制数据资产使用的能力，并可以预先设置流通资产的使用策略，控制因素如下图所示，生成预设版数字合约，可在设置成功后直接选择数据使用方确定数字合约，或将数据资产描述发送至中间服务平台。可信环境子模块的搭建确保图纸文件在使用过程中运行环境、存储环境安全。在数据资产控制模块中完成资产策略控制后可对数据资产进行无感加密，只有通过数据合约签订认证的主体客户端才可使用密钥解密并操作该数据资产，无客户端或非数字合约签订用户无法打开该资产。同时，构建零信任系统在数据合约签订后持续对数据使用方环境进行验证，并给予安全评分，只有符合数字合约的评分要求才可使用数据资产。

表4.4 使用控制策略控制因素示意图

控制因素	时间			地点					主体		行为							客体	
	存放时长	使用时长	使用次数	主网环境	子网环境	接入点	接入设备	设备软硬件环境	进程	用户	读取	修改	执行	删除	转发	复制	截图	数据对象	数据内容

中间服务平台作为服务提供的载体，负责数据流通对接、数据合约、日志存证等功能。其中流通供需对接提供了图纸类数据流通平台，数据提供方可以将需要共享的数据资产描述发送中间服务平台，通过身份验证的数据使用方可登录数据空间查找可以使用的图纸数据，经过数据资产使用商讨后，生成并分发数字合约，部署于数据提供方与使用方客户端侧，如数据使用方不愿公开发布数据资产目录，可以自行选定数据使用方发送合约。此外，本案例构建了日志存证子模块，对数据流通的各个关键节点进行日志存证，确保数据分发、接收、存储、使用、销毁等环节全程可追溯。

4.4案例应用的重点技术和应用情况：可信数据空间应用数据控制、身份认证、可信环境、数据合约、日志存证、数据目录等核心技术，构建面向数据提供方、数据使用方和中间服务方的可信数据流通体系，覆盖数据产生、处理、发布、共享、传输、存储、使用和销毁等数据跨域流通的8个环节，将数据管控划分到最小控制单元。本应用通过图纸类场景级测试为构建区域级行业级家纺业可信数据空间应用提供参考。

4.5方案自主研发性、创新性及先进性：可信数据空间在场景上实现了图纸文件全生命周期的应用场景涵盖，建立对数据全生命周期的静态管理和动态控制，保证了参与方行为可信、数据自身和使用过程可信。相关方案处于国际领先水平，对比国外方案，本方案实现了对文件图纸类数据的跨域管控、建立了终端、平台等不同载体上的数据服务模式。

5.应用成效

该案例是在家纺行业针对设计图纸类文件的实践探索，选择本场景作为应用是因为多领域多行业的这种文件图纸类传出的这种担忧具有普遍代表性。解决各行业设计图纸的所有者无法管控图纸流通范围，无法限制访问人员身份，在图纸传输后无法进行更细致的管控等问题，防止了设计图纸泄露，造成的商业利益与知识产权受到侵害等风险，也减少了传输后使用方二次修改贴牌套牌等情况的发生。为企业增加竞争力与设计图纸的知识产权的保护能力提供有力支持。同时，也为高价值数据的共享流通提供经验。

(四) 生态数据交互模式下的典型案例

案例一：鲲鹏/昇腾产业生态数据空间案例

1.背景介绍

鲲鹏计算产业是基于鲲鹏处理器的基础软硬件设施、行业应用及服务，涵盖从底层硬件、基础软件到上层行业应用的全产业链条。硬件方面，围绕鲲鹏处理器，华为提供包括昇腾AI芯片、智能网卡芯片、底板管理控制器(BMC)芯片、固态硬盘(SSD)、磁盘阵列卡(RAID卡)、主板等部件，整机厂商提供个人计算机、服务器、存储等整机产品。昇腾计算产业是基于昇腾系列处理器和基础软件构建的全栈AI计算基础设施、行业应用及服务，包括昇腾系列处理器、系列硬件、CANN、AI计算框架、应用使能、开发工具链、管理运维工具、行业应用及服务等全产业链。

鲲鹏/昇腾产业生态内，芯片/基础部件和整机构成相互依赖、高度协同的产业合作关系，涉及研发技术的共享、研发进度协同、制造流程衔接、质量问题溯源、培训赋能等诸多业务领域。业务本质上的共生关系要求华为与合作伙伴之间经常性数据交换，但是这些数据又属于企业高度敏感数据，传递使用过程中必须要保证安全不扩散，防止给数据提供方造成商业风险。传统方式下，数据传递缺乏安全可信机制保证，造成必须交换数据又不敢轻易交换数据的两难困境，人工邮件、电话方式的数据交换，效率非常低。

2.案例建设主体

鲲鹏计算产业是基于鲲鹏处理器的基础软硬件设施、行业应用及服务，涵盖从底层硬件、基础软件到上层行业应用的全产业链条。硬件方面，围绕鲲鹏处理器，华为提供包括昇腾AI芯片、智能网卡芯片、底板管理控制器(BMC)芯片、固态硬盘(SSD)、磁盘阵列卡(RAID卡)、主板等部件，整机厂商提供个人计算机、服务器、存储等整机产品。昇腾计算产业是基于昇腾系列处理器和基础软件构建的全栈AI计算基础设施、行业应用及服务，包括昇腾系列处理器、系列硬件、CANN、AI计算框架、应用使能、开发工具链、管理运维工具、行业应用及服务等全产业链。

鲲鹏/昇腾产业生态内，芯片/基础部件和整机构成相互依赖、高度协同的产业合作关系，涉及研发技术的共享、研发进度协同、制造流程衔接、质量问题溯源、培训赋能等诸多业务领域。业务本质上的共生关系要求华为与合作伙伴之间经常性数据交换，但是这些数据又属于企业高度敏感数据，传递使用过程中必须要保证安全不扩散，防止给数据提供方造成商业风险。传统方式下，数据传递缺乏安全可信机制保证，造成必须交换数据又不敢轻易交换数据的两难困境，人工邮件、电话方式的数据交换，效率非常低。

基于华为EDS解决方案，华为牵头建设鲲鹏/昇腾产业生态数据空间，支撑华为与硬件整机厂商之间可信、可控、可证交换流通数据。

3.案例建设目标

鲲鹏/昇腾产业生态数据空间，要实现下列关键目标：

(1)数据交换流通的安全

要实现数据存储、数据传输、数据使用全过程安全可追溯，支持身份认证和鉴权、授权操作，数据提供方对数据拥有完全控制权，数据消费者强制执行数据使用策略，数据交换和使用过程要可追溯。

(2)满足业务场景需求

要实现业务场景对于相应数据类型、数据文件格式的要求，满足不同数据交换模式(如点对点、订阅等)要求，实现关联计算、数据挖掘算法等数据处理。

(3)数据交换流通的高效

要实现便捷的数据查询，在线获取数据，数据交换流通效率显著提升。

4.案例整体情况

4.1应用场景

目前，鲲鹏/昇腾产业生态数据空间主要支持下列场景：

(1)华为技术研发资料共享，涉及芯片/部件相关的技术参数描述、研发路标规划、质量共性问题等，为非结构化数据文件，如Word、PPT、Excel、PDF等文件，从华为向合作伙伴单向传递。属于华为高密数据，需要严格控制使用范围，只允许查看。

(2)发货物流数据共享，涉及华为向整机厂商供货的当前物流状态数据，为结构化数据，从华为向合作伙伴单向传递。属于华为受控数据，需要控制数据使用范围，按需即席查询。

(3)产品现网问题共享，涉及鲲鹏/昇腾产品在客户使用时发现的问题数据，为非结构化数据，从合作伙伴向华为单向传递。属于机密数据，需要严格控制数据使用范围，允许查看分析。

(4)合作伙伴赋能互动，涉及合作伙伴研发评估表、评估举证数据，为半结构化、非结构化数据，双向交互，华为向合作伙伴提供评估项，合作伙伴反馈评估举证数据。属于高度机密数据，需要严格控制数据使用范围，允许查看和编辑。

4.2当前痛点

过去，产业生态内数据交换流通，存在诸多问题：

(1)高密敏感的数据传输困难，由于缺乏数据出域之后的控制手段，企业担心机密数据扩散风险。机密数据对外提供时，审批过程复杂困难。

(2)点对点分散协作，业务需要时，人和人点对点线下沟通，没有企业对企业的统一入口。数据保留在员工个人手里，存在较大风险。

(3)交换效率低，邮件、电话沟通方式，协作效率非常低，影响业务效率。

(4)数据深度应用困难，数据的使用比较简单，需要多种数据的运营分析时，难以汇聚数据联合加工分析。

图4.6 鲲鹏/昇腾产业生态数据交换需求与痛点

4.3部署方案

鲲鹏/昇腾产业生态数据空间，采用华为EDS解决方案。主要功能部件包括：

(1)Connector连接器

连接器Connector是数据空间最核心的部件，完成数据资源管理、数据Offer管理、数据合约管理、数据安全传输、数据使用控制等核心功能，实现数据流通的可信、可控、可证。各参与方对应自己的Connector连接器，独立部署在华为云上。

图4.7 案例部署方案

(2)数据空间公共服务部件

包括注册认证中心、使用控制中心、存证清算中心、数据市场，为数据空间提供统一公共服务，部署在华为云。注册认证中心负责参与者用户注册和身份认证，以及部件技术认证；使用控制中心负责数据使用策略定义、管理和控制；存证清算中心负责数据流通和使用过程的日记记录、上链存证、链路追溯；数据市场提供数据分类治理与面向不同范围的开放订阅的能力，支撑更高效的流通。

数据提供方和消费方之间数据流通交换时，采用数据使用控制机制保护提供方数据主权。数据提供方指定数据的使用控制策略，消费方使用数据时，强制执行使用控制策略。控制策略支持多种维度的控制策略，如：

(1)允许特定Connector：限定哪些参与方可使用数据

(2)限定特定群组：限定某个用户群组可使用数据

(3)限定特定用户：限定参与方的某个具体用户使用数据

(4)限定使用时间：限定某个时间段使用数据，使用时间的总时长

(5)限定使用方式：限定数据使用的操作类型，如查看、编辑、分析等

(6)阅后即焚：限定数据使用后立即删除

4.4案例应用的重点技术和应用情况

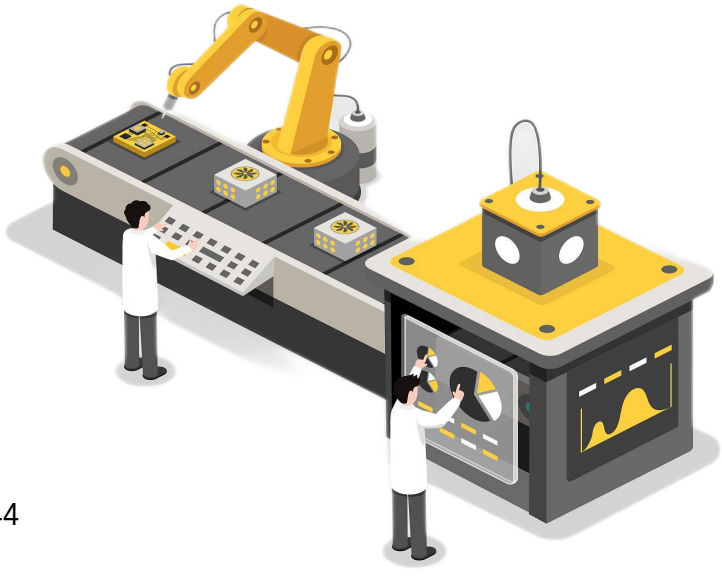
华为EDS数据空间解决方案采用系列化关键技术，实现“可信、可控、可证”的数据交换流通环境。

(1)可信

• 各参与方身份认证，由CA(CertificateAuthority)经过评估认证，向参与方颁发数字证书，作为身份唯一标识；

• 技术组件与App技术合规性认证，CA评估技术组件和App的技术可信合规性，通过认证后，取得数字证书，才能接入数据空间；

• 访问鉴权与可信通信，数据提供者与数据消费者之间，技术部件之间通信，基于PKI完成鉴权、数字签名，保证数据传输的安全性、完整性和实名性；



(2)可控

• 各参与方身份认证，由CA(CertificateAuthority)经过评估认证，向参与方颁发数字证书，作为身份唯一标识；

• 技术组件与App技术合规性认证，CA评估技术组件和App的技术可信合规性，通过认证后，取得数字证书，才能接入数据空间；

• 访问鉴权与可信通信，数据提供者与数据消费者之间，技术部件之间通信，基于PKI完成鉴权、数字签名，保证数据传输的安全性、完整性和实名性；

• 数据使用控制策略，基于“4W2H”设计原子策略，灵活设置数据使用控制策略；

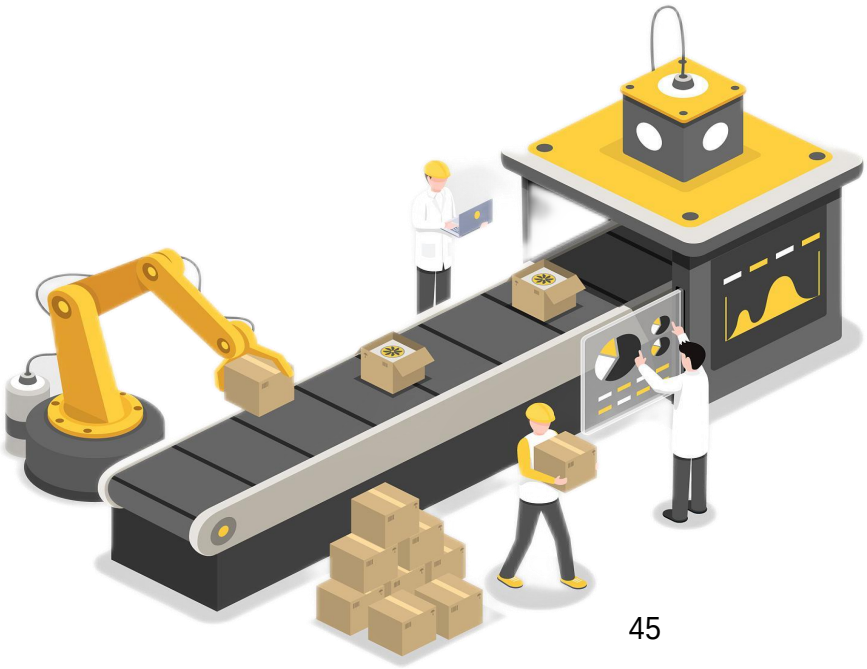
• 数据使用控制策略执行，数据消费方Connector内PEP(PolicyExecutePoint)与策略控制中心内的PDP(PolicyExecutePoint)交互，完成数据使用策略的强制执行；每秒万级高并发策略执行引擎；

• 数据基础安全能力，支持数据加密、脱敏、分级、隐私、安全消费、销毁、数字水印、防截屏/打印等基础安全能力；

• 安全执行环境，使用容器管理技术为个体数据服务提供分隔、安全的环境；

(3)可证

• 全流程数据操作日志上链,基于清算中心+区块链+全链路实现提供方查证追溯、消费方自证清白，监管方全过程监管审计；



4.5方案自主研发性、创新性及先进性

(1)业务场景设计因子收敛设计

实际各种业务场景对数据流通需求会有较大差异，对应的数据空间软硬件能力、配置参数要匹配业务场景需求。

华为EDS采用业务场景设计因子收敛的创新设计，以数据提供价值流和数据消费价值流为主线，抽象出若干场景设计因子。通过对各场景设计因子维度分析定义，形成适合业务场景的设计因子维度组合模型。

基于组合模型，自动生成数据空间配置模板包。配置模板下发部署到数据空间各部件，快速完成数据空间资源分配、运行参数设置，实现数据空间从需求分析到工程部署的敏捷建设。

(2)数据使用控制策略关键设计

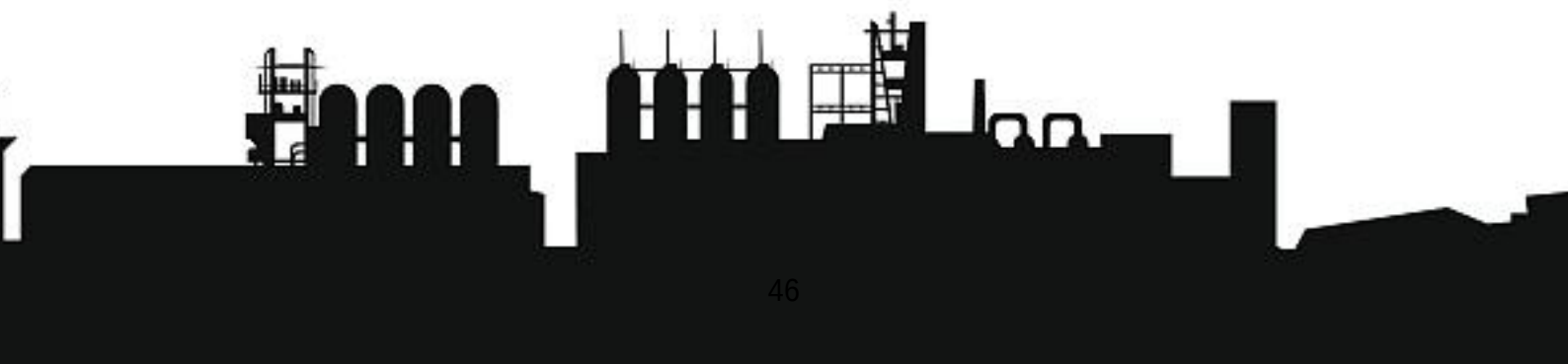
数据使用控制涉及两个关键能力：数据使用控制定义、数据使用控制生命周期管理。

• 数据使用控制策略定义，通过开放模型，支持不同标准语言描述的策略定义规范，支撑不同类型、不同厂商定义的策略定义规范；

• 数据使用控制策略生命周期管理，包含数据策略规范映射、数据策略冲突管理、数据策略实例化模式、数据策略协商、数据使用控制撤销、数据使用控制实施；

这些特性，需要数据连接器组件、认证中心组件、使用控制中心组件、清算中心组件、企业自有的外部应用系统共同协同。华为EDS方案构建了针对数据策略全生命周的部署方案：

• 数据使用控制规范统一接入并管理，可以对接不同厂商的策略定义接口



• 数据使用策略的映射：基于时间、地点、主体、行为、客体五个维度，构建4W2H的策略映射转换模型，兼容基于不同描述语言和模型的策略转换，如ODRL、MPEG-21等。

• 数据使用策略冲突管理：包含使用策略的冲突处理流程、冲突处理规则

• 数据使用策略实例化：提供标准化的策略实例化接口，提供给数据连接器定义策略、磋商策略，并在使用控制中心、连接器同步存储。

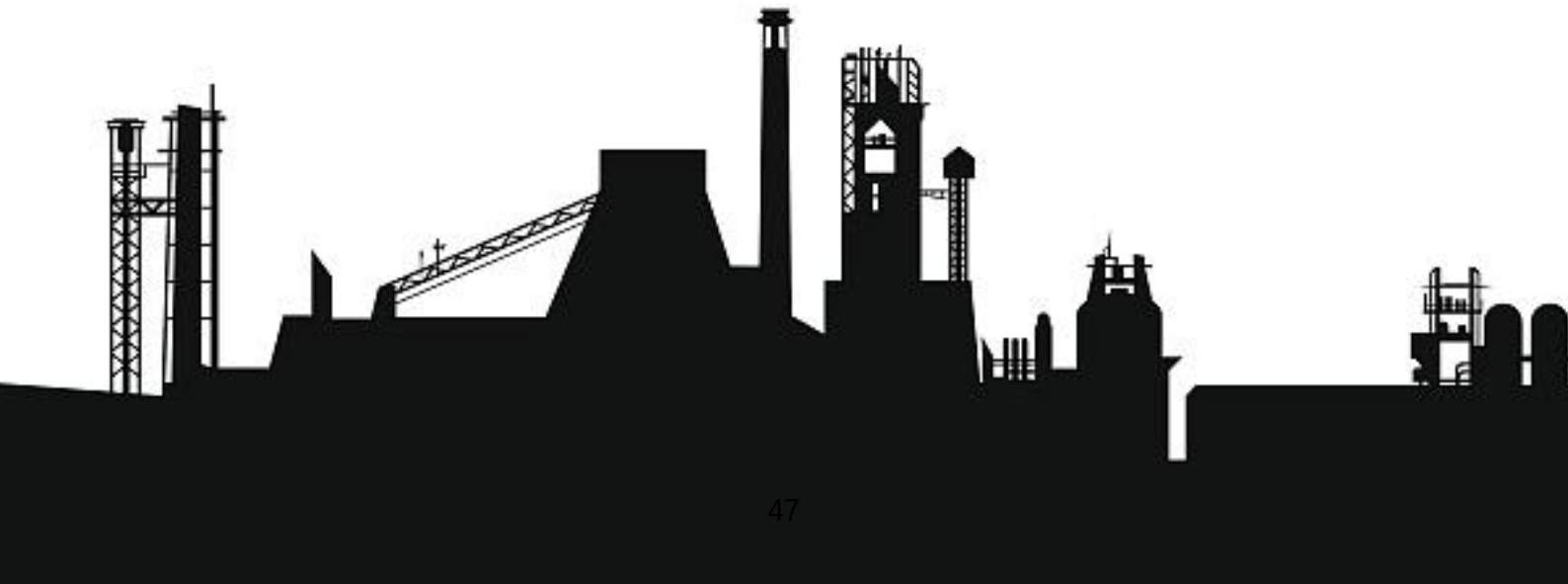
• 使用策略协商：提供在点对点场景、数据市场订阅场景满足数据提供方、消费方对策略规则进行对方磋商能力。

• 数据策略争议仲裁：数据提供方、消费方、运营方基于已有事实可发起合约执行争议，并在清算中心审核后，对特定合约策略进行争议仲裁，终止合约或更改策略。

• 数据使用策略评估提供多种方式部署：数据使用策略评估可以选择集中式统一在数据策略中心进行评估，也可以选择分布式的、分散在数据连接器进行评估。

(3)自主研发，拥有完全知识产权

华为在数据空间上，以压强原则重点投入，相关技术和标准跟踪持续6年，产品与服务开发已走过2年，数据空间已正式支持各种业务。数据空间产品所有代码全部自主开发，基于自主平台开发了完整的解决方案。



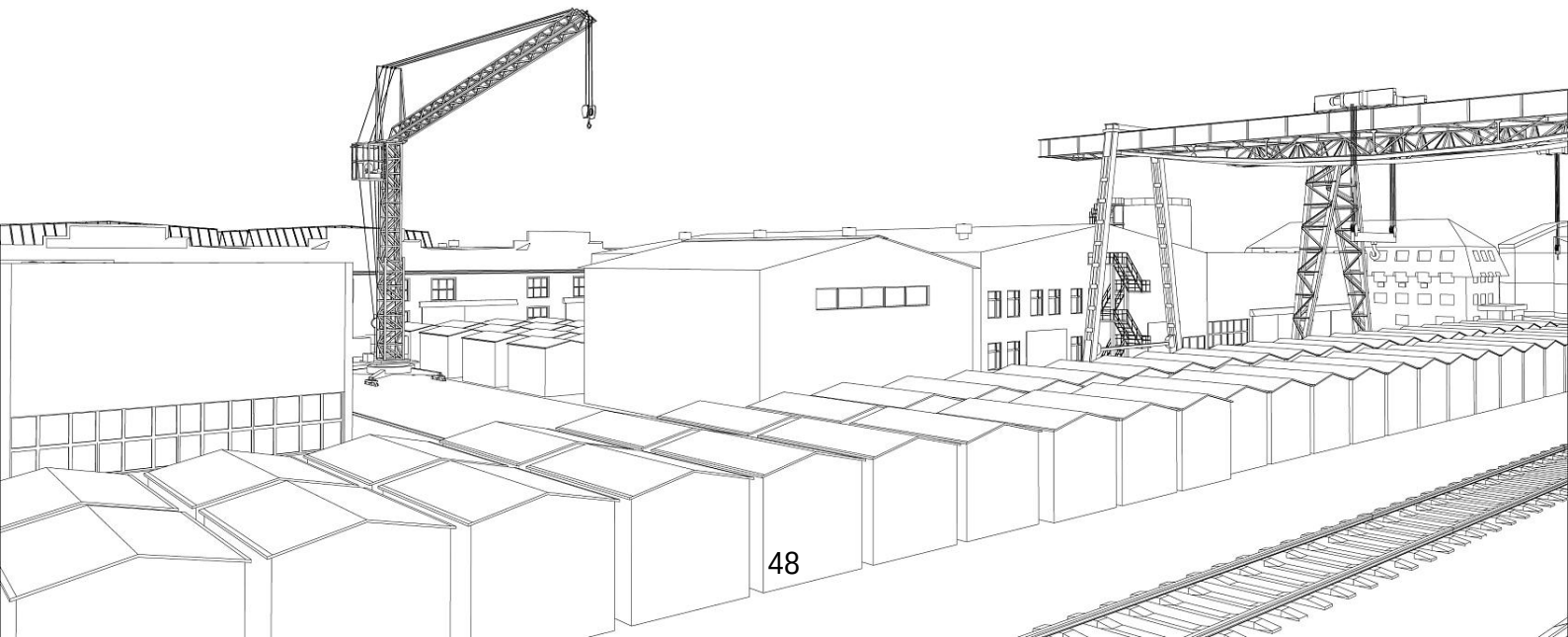
5.应用成效

鲲鹏/昇腾产业生态数据空间已于2021年上线使用，目前已加入生态伙伴13家，共15方参与，用户数达到300个，覆盖25种业务数据资产的交换，每月数据交换量超过2000次，累积数据交换量超过14000次。

鲲鹏/昇腾产业生态数据空间的使用，保证了企业敏感数据的可控使用，极大地提升了生态合作伙伴之间的协同效率，有效地支撑了研发部门、生产制造部门、产品服务部门等业务线工作效率和工作质量，取得显著的商业价值。

- 高密数据传输，交换数据资源的种类超过25类，敏感数据交换时间从几个月缩短到3天；
- 统一的数据交换接口，所有用户登录数据空间，在安全可信环境内实施数据申请、交换和使用，避免了人工电话、邮件存在的安全风险；支持21数据使用策略；
- 数据交换效率提升，数据查询时间从1周缩短到1分钟；
- 数据深度使用，从仅支持文档查看和离线报表，到支持在线数据组合分析；

面向未来，鲲鹏/昇腾产业生态数据空间会持续优化提升技术性能、扩大数据范围，使能更多业务场景，丰富商业运营能力。数据空间实践经验愿意开放分享给其他行业领域借鉴，共同促进数据要素流通市场的发展。



案例二：电子信息业产品自动化联合质检案例

1.背景介绍

在离散型工业制造供应链上，通常由多个零件生产商为下游企业供应零件，零件的批量较大，一般采用人工抽样检测的方式来进行工件质检。这样会造成两个问题：一是随机抽样方式不覆盖所有工件；二是检测完全依赖检验员的业务经验和工作态度，质检效果波动大、效率低。产品装配公司需要基于生产商全量样本数据进行模型训练，但是零件生产商不希望将零件数据本身的信息透露给其他生产商，所以需要建立一种原始数据不出本地、跨企业数据共享的分析挖掘方式。

本项目在熊猫电子产业集群搭建了能够实现以上需求的数据可信融合系统，其中可信融合平台采用隐私计算的数据融合架构，利用服务平台功能，将质检员在流水线每个环节采集到的问题工件图片，在本地进行模型训练后，利用差分隐私的方法进行模型的共享。

现存的问题：支撑模型训练的数据量不足或质量不高、收集的故障样本比例太少、设备类型较多导致各类模型训练开销大。

当前解决方案：使用基于联邦迁移学习的故障模型预训练与优化方法。

2.案例建设主体

数据提供方为离散型工业制造供应链上的各个上游零件供应商，数据使用方为下游装配公司，中间服务方为身份认证商、算法服务商、模型服务商。

3.案例建设目标

基于联邦学习的故障模型预训练与优化方案是为了在保障各家企业私有数据隐私安全的前提下实现模型的可信传输，通过5G网络的海量连接特性连接场内所有自动化装备，分析生产效率并优化，诊断设备故障，由计划性维护向预测性维护转变，最终实现生产效率的提升。

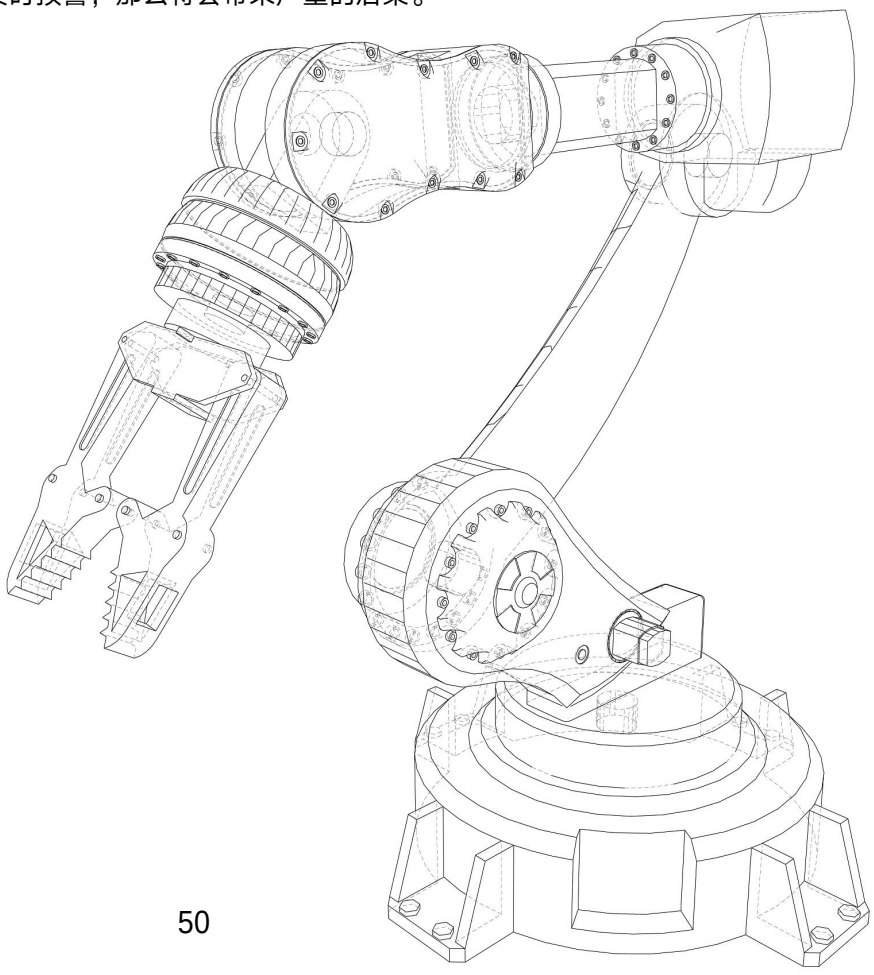
4.案例整体情况

4.1应用场景

案例适用于离散型工业制造链上多家企业联合质检场景下的数据可信共享，通常由多个零件生产商为下游企业供应零件。目前人工抽检的方式既不能保证工件检测全覆盖，也不能保证质检的效果与效率，因此需要在数据安全可信共享的前提下，建立一种原始数据不出本地、跨企业数据共享的分析挖掘方式。应用能够在数据安全流通的前提下有效降低质检成本，提高质检效果与效率。

4.2当前痛点

首先是缺少网络间的安全边界防护措施，这不仅使得工业生产设备的接入安全难以保障，还导致安全漏洞被放大，极易受到外界攻击；其次对于产业集群生产环境，海量多元异构生产数据无时无刻不在产生，设备种类、型号、工作环境与要求都不尽相同，难以统一管理，如果没有相应的安全管控措施，企业内或企业集群内生产流程安全以及关键过程数据的可靠存证与审计就更难确保；最后，如果不能实现有效的数据融合，在工业设备海量接入的情景下，就难以有效监测工业设备运行情况，对设备故障做出实时预警，那么将会带来严重的后果。



4.3部署方案

部署架构如图所示，数据提供方为供应链上游各零件厂商，数据使用方为下游装配公司，中间服务方为身份认证商、算法服务商以及模型服务商，存证方为内部存证机构与第三方存证机构。

数据提供方首先在本地训练根据工件图片训练质检模型，训练完成后将模型上传到中间服务方，同时发送日志给中间服务方以及存证方进行存证，中间服务方接收到模型后也向存证方提交日志。模型在中间服务处的最大可存放时长为1周，中间服务方对模型的使用时长等同于最大可存放时长，使用次数不限，中间服务商可对模型数据进行读取、修改、执行、删除以及复制等操作，但不可转发；数据使用方向中间服务方发出请求参数，并向中间服务方与存证方发送日志，中间服务方将聚合后的模型发送给数据使用方并向存证方发送日志，模型在数据使用方处不限制存放时长、使用时长与使用次数，数据使用方可对模型数据进行读取、修改、执行、删除以及复制等操作，但不可转发。案例的可信通信环境由数据传输储存等IT基础设施功能提供方保证。

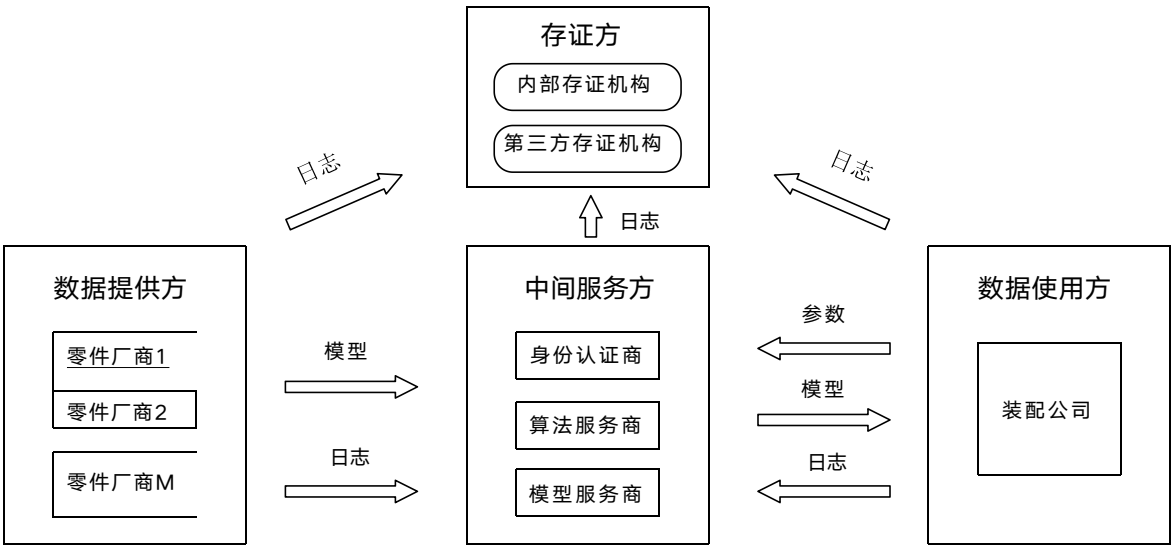


图4.8 案例部署方案

各企业参与方可以使用系统公共服务平台的联邦学习框架，在数据不出厂的前提下进行模型的安全聚合，同时利用公共服务平台的工业联盟链进行模型确权，最后使用联合优化好的模型进行本地实时推理。这样既可以在单个企业数据样本不足的情况下联合提升模型精度，又可以保护各家企业的数据隐私。

考虑到企业的多家客户方均有同类型设备，故可以利用中心云服务平台的联邦学习框架在保障客户数据隐私的情况下进行故障预测模型的再优化，提升模型精度。根据故障预测模型的推理结果，系统能够及时发现设备运行异常情况，并向企业给出相应的预测性维护建议。

4.4案例应用的重点技术和应用情况

方案应用技术涵盖安全技术中的差分隐私、隐私计算技术中的可信执行环境与联邦学习、数据控制技术中的访问控制技术与使用控制技术。重点技术为联邦学习技术，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。联邦学习做到产业链上下各单位的私有数据不出本地，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，建立一个全局质检模型，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，而联邦系统帮助产业链上各个企业建立了安全共享的策略，实现了安全可信环境下的联合质检。

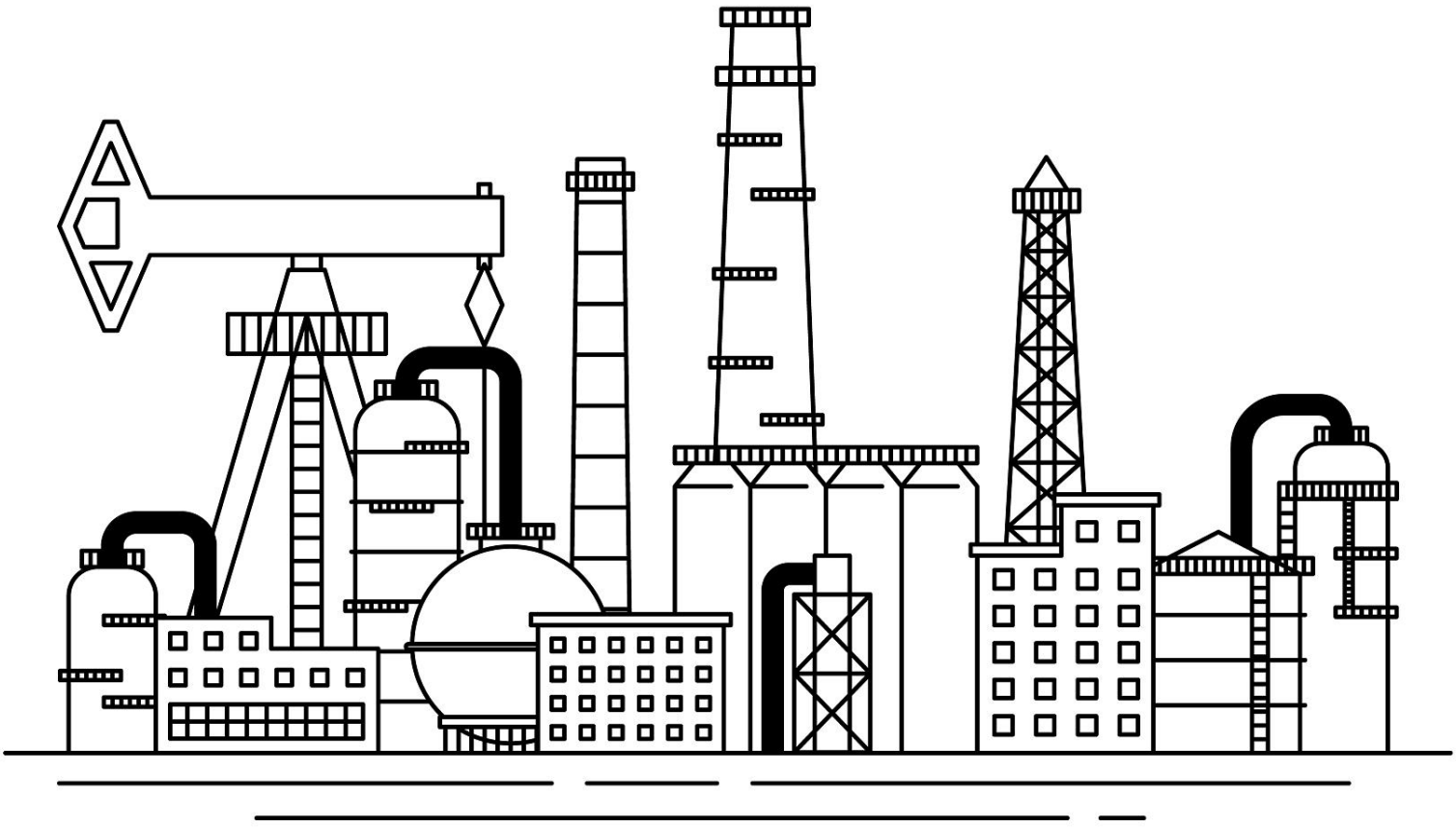
4.5方案自主研发性、创新性及先进性

自主研发云边协同的工业互联网平台，依托于可信基础设施，可提供包括安全技术、隐私计算技术、存证溯源技术、数据控制技术、管理技术、计算处理技术以及OT技术在内的部署与实施。工业互联网平台能够在该应用中担任中间服务商以及存证方的角色，在保证可信环境的前提下，高效执行数据控制、模型聚合与分发共享等职责，为供应链整体的联合质检降本增效。

5.应用成效

制造业产品自动化联合质检应用在数据可用不可见、可控可计量的安全前提下进行离散制造业供应链上下游企业模型的联合训练，提升了整体质检模型的准确率，最终实现了检测成本的降低、检测效果与效率的提升，同时促进了产业链在质量管理、数据确权与合作协同等方面的全方位提升。

该方案可轻易推广至各联合质检场景，对于研发、生产、供销、服务、财务等其他场景，找到不同企业单位之间合作协同的方式后，在工业互联网平台提供的可信数据流通环境以及包括安全技术、隐私计算技术、存证溯源技术、数据控制技术、管理技术、计算处理技术以及OT技术的帮助下可迅速进行协同生产业务的设计、部署与实施。



案例三：电子信息业供应链金融用户画像案例

1.背景介绍

当下，用户身份多次注册，多次实名，数据未被用户自己控制，信息更新需要去多平台进行更新等问题困扰着用户，为此，中企云链(以下简称为“我司”)利用区块链技术研发云链云身份联盟链，达到用户身份的自主控制权，多平台身份互通、企业身份聚合的目的。同时，基于云链云身份联盟链进行基于用户真实可信身份的用户画像。

云链云身份联盟链需要基于可信的、真实的用户身份开展身份共享业务，数据的安全可信以及安全存储传输可以说是平台的内核需求。而区块链技术的应用在此方面具有天然的优势。以云链与雄安平台对接为例，通过区块链的建设，将云链用户相关数据上链存储，可有效保证数据的真实性、不可篡改，从而提高数据的可信程度。在用户在使用雄安平台进行实名认证时，可以在授权后，直接调用在云链认证上传及填写的可信数据。

通过云链云身份联盟链节点的扩张，会有大量的权威机构或者企业的可信用户身份上链。云链云身份联盟链可以通过区块链联邦计算的方式进行可信数据的计算，结合公开的数据，进行供应链金融行业可信用户画像，为企业的供应链上下游提供服务。

2.案例建设主体

数据提供方：云链云身份联盟链各个节点。

数据使用方：云链云身份联盟链各个节点平台，及其供应链上下游企业。

中间服务方：通过中间数据服务方，获取企业公开的工商注册数据、上市公司财务数据等企业信息。

3.案例建设目标

基于云链云身份联盟链的供应链金融行业用户画像案例是为了实现在不同的供应链金融平台系统中，不同节点用户数据的安全可信传输，包括但不限于数据所有者可以控制数据不被发送给第三方、数据所有者可以根据需求进行授权或者取消授权、数据所有者可以实现对数据使用状态的全程监控等，最终达到各个节点多方可信协同、供应链金融行业可信用户画像的作用。

4.案例整体情况

4.1应用场景

基于云链云身份联盟链的供应链金融行业用户画像案例适用于某个行业内基于数据的可信传输，在不同企业平台之间用户互通、可信企业用户画像等场景。

由于各个平台大部分因为数据敏感度较高，数据拥有方为保障数据隐私性等原因，造成了数据孤岛，不同平台之间的企业用户数据是割裂的，从而造成了用户身份多次注册，多次实名，数据未被用户自己控制，信息更新需要去多平台进行更新等问题。因此，需要一个多中心的联盟，共同制定实名认证的标准，通过可信的传输逻辑，进行不同平台的用户互通，用户画像，从而为供应链金融行业的上下游企业提供相应的服务。

4.2当前痛点

(一)企业用户重复注册问题

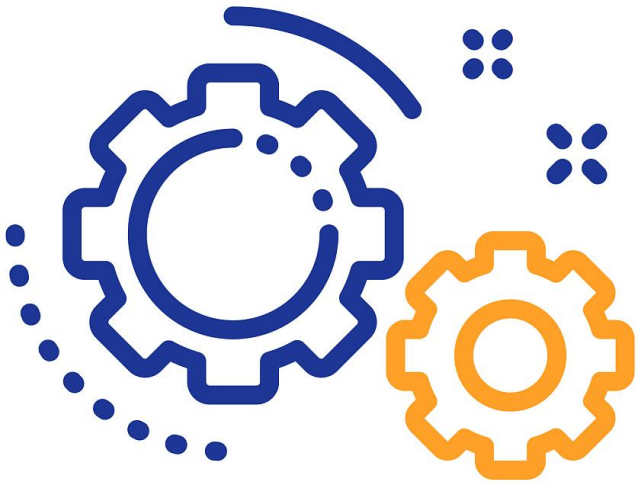
目前市面上存在着大量的互联网金融平台，以供应链金融平台为例，目前存在核心企业模式、资金方模式和平台模式，在三种模式下，都存在着大量正在运行的供应链金融平台，某个企业去不同的平台做业务，均需要做一次注册和实名认证操作，需要按照不同的平台需求，提供大量的材料以及说明，平均每个平台注册认证都需要一到两天，无形中消耗了中小微企业大量的时间成本与人力成本。同时，某个企业会去多个互联网金融平台进行企业用户的注册，如果企业信息出现变动，那么需要相应的人员，在不同的互联网金融平台进行资料的更新，也需要消耗大量的人力物力。

(二)身份数据授权与归属的问题

现在大部分互联网平台，都将用户的数据作为平台方自己的数据资产来看待，最终用户对自己的身份数据没有应享有的控制权，无法自主可控，从而导致了大量的数据泄露，非法身份窃取，非法身份授权等问题，造成了很多不良的社会影响。

(三)可信用户数据画像问题

由于各个平台大部分因为数据敏感度较高，数据拥有方为保障数据隐私性等原因，均在建设自己的生态，按照自有业务结合公开数据进行用户画像，造成了用户画像的不完善、不准确，从而使依靠用户画像的授信、风控、借贷等相关业务开展会出现困难甚至是风险。



4.3部署方案

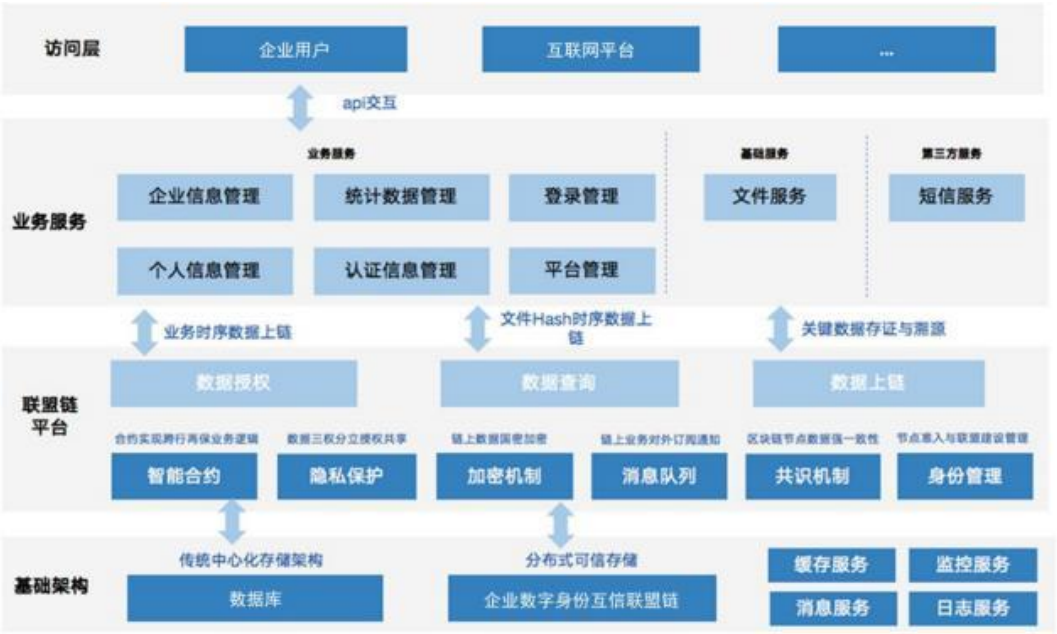


图4.9 案例部署方案

整体框架自下而上分为基础架构层、联盟链平台层、业务服务层与访问层。

基础架构在基于传统数据库存储的基础上，采用全新搭建的云链云身份联盟链作为分布式数据存储，实现中心化与分布式的混合数据架构，保障数据的安全性，同时底层区块链平台为国产自主可控，结合主流的Redis缓存服务、Prometheus监控服务、RocketMQ消息服务、ELK日志服务，为业务做好底层基础架构支撑。

联盟链平台层作为区块链核心服务，可进行数据上链、数据查询、链上数据管理等功能。同时实现基于“三权分立”下的数据可信隐私保护和共享。数据安全体系支持全国密方式，匹配国家信息安全要求。同时共识机制保证分布式节点数据强一致，联盟链平台层整体做好区块链各技术服务支撑。

云链云身份联盟链服务层实现应用业务等功能，包括企业信息管理、个人信息管理、统计数据管理、认证信息管理、登录管理、平台管理、授权管理、用户画像等功能。平台采用主流Java/SpringCloud微服务框架设计实现，采用负载均衡高可用架构保证稳定性，具备较好的兼容适配和高可用。中互金企业数字身份基础服务包括文件服务，为业务中产生的业务资料文件和各类协议等做好存储和查询。云链云身份联盟链可对接外部第三方服务短信服务，实现关键业务的通知，提升业务的可靠性真实性安全性。

访问层为需要与云链云身份联盟链平台进行业务交互的系统或平台，直接的使用方包括企业用户、供应链金融平台类用户，技术上采用联盟链构建对接的标准化，提升系统对接的效率。

在区块链技术应用方面，本项目基于区块链上的数据权限控制，实现基于三权分立的智能合约的数据授权管理，通过区块链的方式透明数据存证、数据请求、数据授权的全流程权限控制，保障数据的可信共享。对于大文件存储与区块链交互，可实现文件中心化存储或分布式分片存储，同时把文件Hash上链，以实现文件防篡改，保障文件真实性与可追溯性。

4.4.方案应用的重点技术和应用情况

1、身份认证技术及应用说明

用户的身份认证是做各种业务的前提标准，因此，必须保证认证标准的统一以及真实性，云链云身份联盟链根据业务属性以及身份全等级，将身份认证分为不同的等级标准，不同的标准可用标识作为区分，从而可以做不同的业务。为此，云链云身份联盟统一联盟认证标准，并且将整个实名认证的过程环节产生的电子数据进行存证，存证验证通过后，进行上链，确保用户的真实性以及证据链的完整性。

2、数据共享合约

数据提供方和使用方就业务需求，根据最终用户的私钥授权，确定共享数据使用要求，并生成对应的智能合约。各个联盟节点根据智能合约进行加密数据的互通流转。

3、联盟计算与身份互通

云链云身份联盟会根据各个节点的身份数据，利用用户画像模型，通过在用户节点进行本地隐私计算的模式，基于可信的身份数据进行用户画像，为供应链金融行业的上下游企业提供企业数字身份服务。

4、身份日志记录存证

在云链云身份业务过程中，会将整个实名认证的过程环节产生的电子数据进行存证，存证验证通过后，进行上链，确保用户的真实性以及证据链的完整性。

同时，整个用户授权的过程，各个节点对于用户数据调用的过程全部进行上链，确保可以利用区块链的可追溯性，完整地还原用户的业务操作流程。

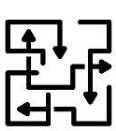
5、可信数据传输

由于所有的数据通过分布式存储分别碎片化加密存储在联盟链各个节点上，只有在用户私钥授权后，才能通过智能合约进行数据组合，并通过加密传输的方式传输给数据适用方。

4.5.方案自主研发性、创新性及先进性

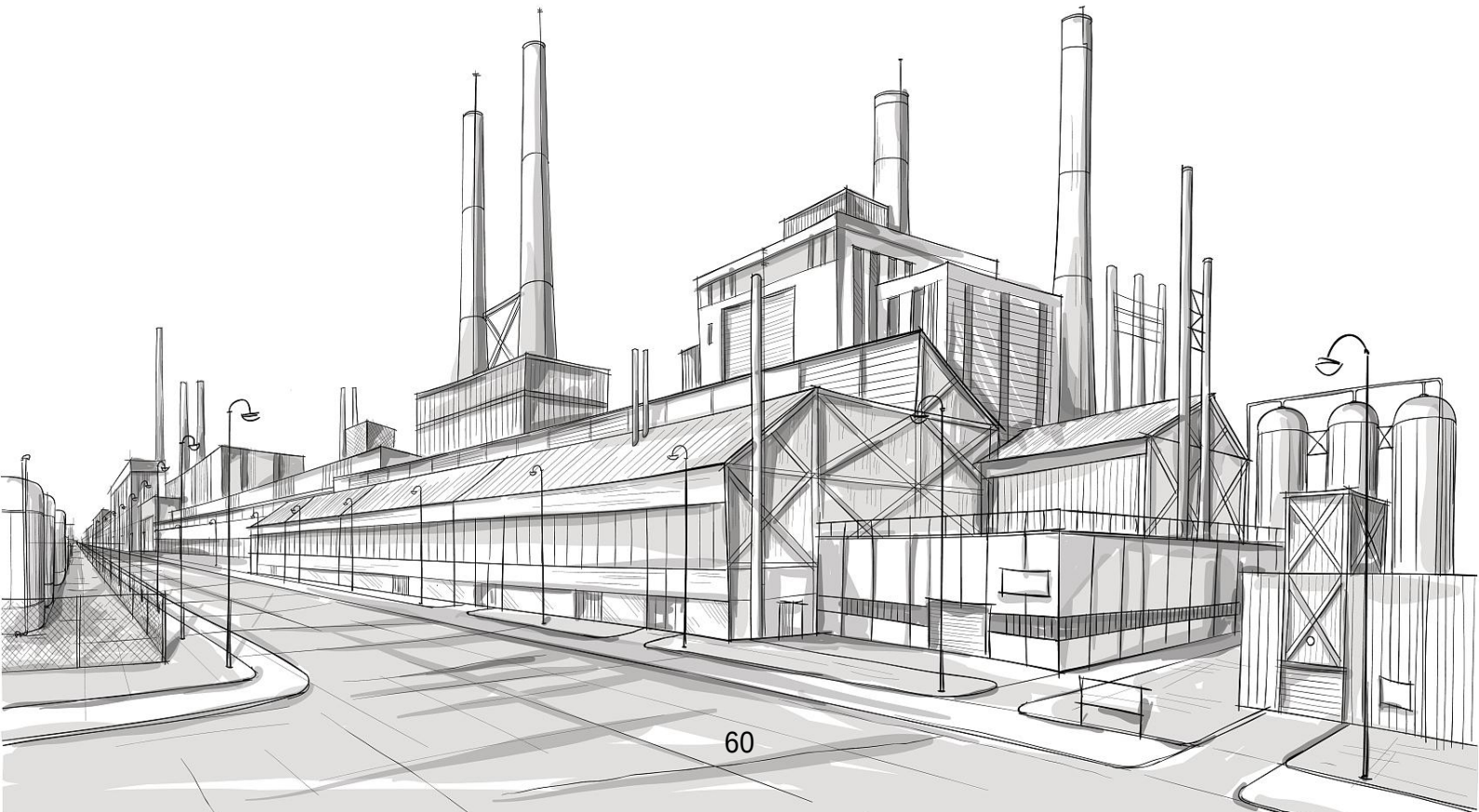
案例利用区块链技术，在保障数据可信使用的前提下，进行用户身份的互通，将身份数据所有权交还给用户，通过联邦计算利用可信用户进行用户画像，降低整个行业的用户进入门槛，提高联盟各个平台的效率。



5.应用成效

一是建立了自主可控，自主授权，安全高效的用户端，可实现企业用户在平台端进行一次认证，即可实现多平台授权注册，且身份可控，平台不拥有用户身份信息所有权，而且企业用户可自主授权，根据需要进行平台授权或取消授权。另外，链上所有数据都通过非对称加密技术进行了数据加密，信息隐私可得到全面保障。当前已使用云链云身份进行平台身份信息注册的用户，平均注册周期缩短到了10分钟以内，极大提升了工作效率。二是建立了快速获客，交叉验证，真实可信的平台端，企业用户的身份注册环节时间的缩短，可以减少用户在此环节的跳出率，能够实现快速获客，免重复审核认证加速用户获取，获客成本减少90%。另外，区块链上各权威机构之间可实现企业身份的交叉验证，充分保障企业用户身份真实可信，减少了用户利用虚假身份从事交易的风险。三是建立了信息整合，多维把控、风控前置的资金端，其提供的KYC服务可通过多节点信息的整合而能够更加完善和有效。在提供服务的阶段，用户可通过身份的统一标识，整合散落在各平台的数据，提供给资方作为评级放款的依据，为资方节省了审核和识别信息风险的时间80%。



第五章

Chapter 5

工业数据可信流通应用建设路径

(一) 需求调研

通过需求调研，深入了解相关参与方的业务需求和痛点，明确系统要解决问题的范围。数据流通是从数据提供方到数据需求方的闭环，要满足双方的供需关系匹配。

针对数据需求方需要调研的内容，主要包括如下维度：

• 关联业务及优先级：涉及到业务流程，与周边业务的关系，业务价值和优先级。

• 数据要求：如数据内容、类型(结构化、半结构化、非结构化)、数量级、使用频次等。

• 数据处理方式：如阅读、查询、统计、机器学习等，是否与本地数据关联处理等，使用的数据处理工具，处理实效要求。

• 周边系统接口：与周边系统的接口形式、协议要求。针对数据提供方需要调研内容，主要包括如下维度：

• 供方的数据特征：如数据来源、数据内容、数据类型、量级、产生频次。

• 数据使用约束规则：如数据等级、使用范围、使用人员要求、使用期限、处理方式要求、存储要求。

综合数据提供方和数据需求方的数据需求及约束，双方能达成一致的场景优先纳入需求范围，并根据业务价值优先级排序，决定实施的先后顺序。

需求调研阶段，形成正式需求列表并纳入管理，持续审视刷新。对于暂时没有达成一致的需求，可纳入长期需求跟踪。

(二) 方案设计

1、信任机制设计

• 生态业务各参与方的身份认证。CA(CertificateAuthority，认证中心)经过评估认证，向参与方颁发数字证书，该数字证书是唯一的身份标识。

• 访问鉴权与可信通信。数据提供方与数据使用方技术部件之间的通信，基于PKI(publickeyinfrastructure，公共密钥基础设施)完成鉴权、数字签名，从而保证数据传输的安全性、完整性和实名性数据使用控制。

2、数据使用控制设计

• 数据使用控制策略：基于“4W2H”(Who、When、Where、DoWhat、HowTo、HowMany)设计原子策略，灵活组合，实现精准的数据使用控制。

• 全流程精细管控：全流程操作通过日志记录+区块链存证+全链路血缘，实现数据提供方可查证追溯、数据使用方可自证清白、数据监管方可监管审计。

3、智能合约设计

• 跨主体的数据交换生成智能合约，基于契约化的合约，实现双方要求承诺的IT化，并通过区块链进行存证，防止篡改。

• 合约中包含的数据使用控制策略，通过技术手段被IT强制遵守，避免人工执行带来的不可控风险。

4、应用改造与工具适配

• 数据处理应用改造：数据应用使用数据时，要执行数据控制策略约束，业务处理逻辑要做相应调整，适配数据使用约束规则。

• 数据处理工具适配：Office类文档工具、BI分析工具等数据分析工具，要执行数据控制策略约束，如禁止另存、只读、禁止导出等，数据处理工具要做相应调整，适配数据使用约束规则要求。

(三) 系统部署

1、IT资源申请

基于数据量及作业量估算，申请所需要的计算、存储和网络等IT资源。数据流通涉及多个参与方，是多节点的分布式架构。依据数据保护级别、业务上线时间要求、IT成本等因素综合考虑，可选择云计算、本地、混合方式提供IT资源。

2、部署业务公共服务

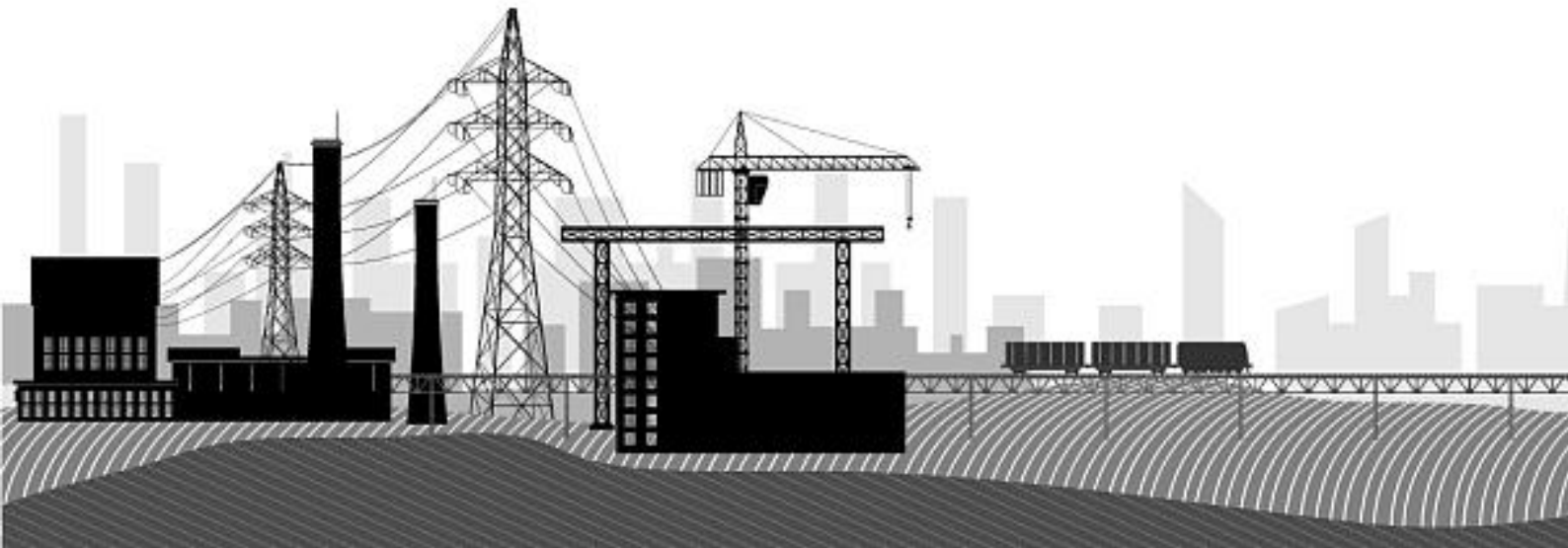
认证中心、使用控制中心、存证清算中心、数据市场等模块组成的业务公共服务，对所有参与者开放，优先部署在云上。

3、部署数据节点环境

数据提供或消费方，是数据流通主体，分别部署本方数据节点环境，支撑安全可信的数据处理和流通环境。数据节点环境包含基础安全环境资源(如容器等)、数据应用、数据分析工具、资源库等。运营方通过部署工具一键式安装。数据节点环境可根据数据安全要求、业务上线时间要求等选择部署在云上或本地。

4、业务系统集成

数据流通系统与业务系统相互协同，在数据提供方，从业务系统获取数据；在数据消费方，处理结果传递给业务系统使用，数据流通系统与业务系统要实现集成对接。



(四) 测试上线

1、账号申请与权限分配

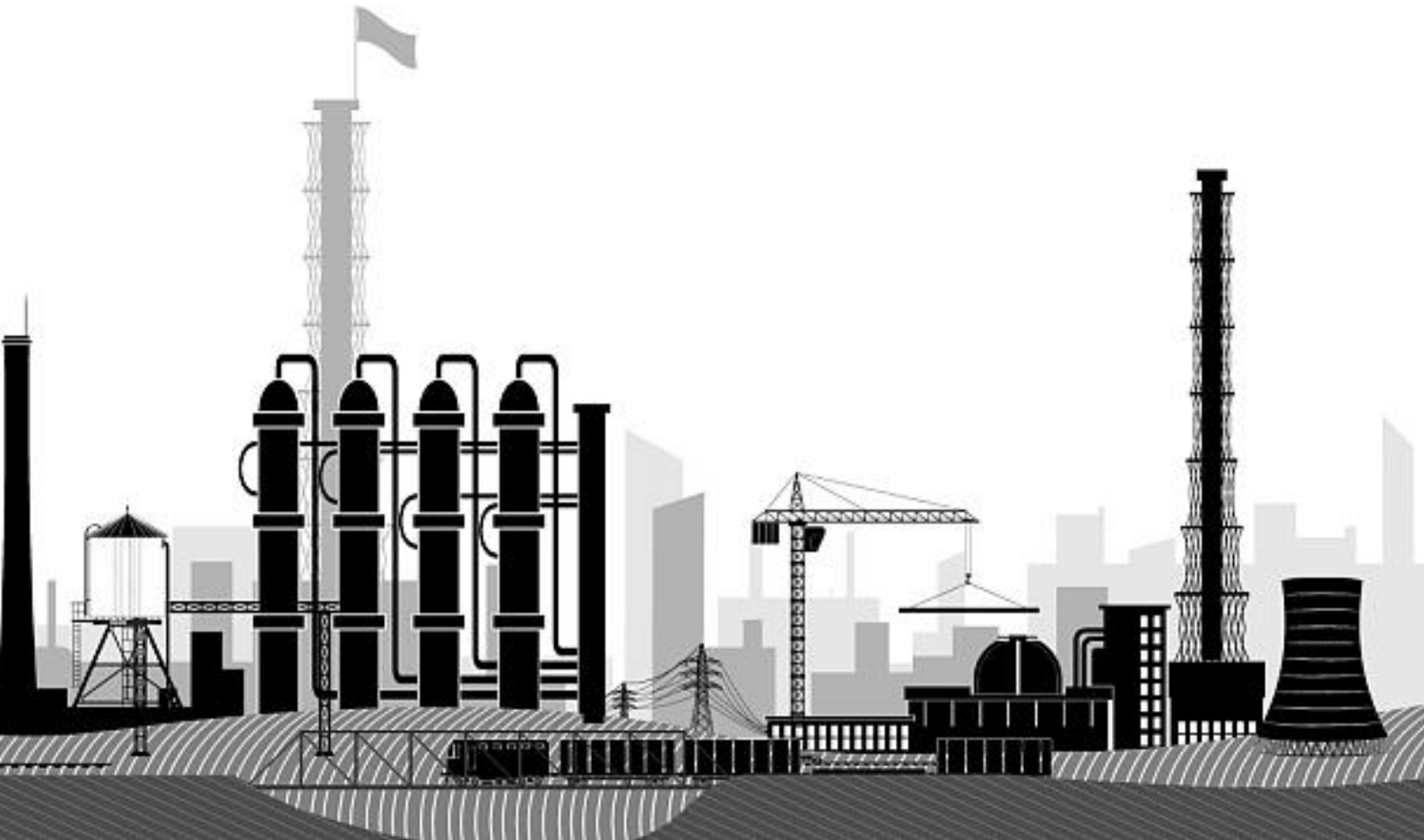
企业用户申请账号，经运营管理员批准后，可以参与数据流通作业流程。每个账号绑定一定角色，具有不同的操作权限。

2、业务UseCase测试

根据需求列表，形成场景化UseCase测试用例清单，验证数据流通全过程能力，主要涉及业务开通、数据资源上架、数据使用规则设定、数据规则执行、数据处理、两方流通交换、多方流通交换等核心能力；并进一步从业务视角，验证数据流通能否满足业务实际需求。

3、跟踪监管测试

通过审计数据供需方围绕数据流通的行为记录，保证数据流通过程合规合法。完成功能测试和业务验证后，经评估满足需求后，数据流通应用可上线运行。



(五) 运行优化

数据流通应用上线运行后，业务方、运营方、方案提供方在日常使用实践中，可进一步探索需求场景、丰富系统能力、完善系统功能。

1、问题发现与解决

在日常业务实践中，不断发现系统的功能、性能问题，通过迭代优化，不断完善系统功能。

2、需求探索与场景扩展

基于数据流通应用，尝试支撑更多业务场景，扩大数据流通的作用范围。探索过程，会进一步发现更多需求场景，驱动数据流通系统不断完善增强。

结 语

当前产业数据共享流通能力已经成为影响数据价值释放的关键。现阶段工业数据流通体系建设虽取得一定进展，但面对我国庞大的工业门类及多元的应用场景，应用覆盖还远远不足。本次报告的发布，一方面是对现阶段工业数据流通应用成效的展示，为产业提供参考和借鉴；另一方面希望能够带来业界对工业数据流通更深刻的思考与讨论，推动建立数据跨行业、跨企业连接的价值网络，更好的服务于企业及行业数字化转型，促进数据的安全、有序共享，提升数据资源价值，进一步发挥数据的基础资源和创新引擎作用。

本报告是全国范围内第一批工业数据流通方向的应用报告。特别感谢参与编写本报告的众多企业，以应用为导向推动工业数据流通是我们的不竭动力，参与访谈和编写的各位专家提供宝贵智慧与经验，感谢相关领导对本案例集提出了宝贵的意见。相信未来在业界同仁的共同努力下，随着工业数据流通的推广应用，技术不断下沉、不断融合创新应用，我们的应用案例也会愈加丰富，推动数据共享流通迈向更高水平。

欢迎扫码关注
加入可信工业数据空间生态链
共同助力数据要素流通

工业互联网产业联盟
Alliance of Industrial Internet
北京市海淀区花园北路52号
010-62305887
http://www.aii-alliance.org