

# 可信数据空间技术路线的研究与家纺行业应用

刘海阳，李哲行

(中电数创(北京)科技有限公司, 北京 100083)

**摘要：**在数据要素市场化配置改革的背景下，构建完善的国家数据基础设施体系对推动数据要素高效流动与价值释放、赋能数字经济提质增效具有重要意义。聚焦可信数据空间技术路线，系统剖析其架构、关键技术与实施路径，旨在解决数据流通中的安全性、可控性与互信问题。结合家纺行业实际应用场景，提出了基于 JSON 格式的数字合约实现方案，并与传统数据保护技术进行对比，凸显其在细粒度控制与性能方面的优势。该研究为可信数据空间的行业落地提供了技术参考与实践范例。

**关键词：**数字合约；可信数据空间；使用控制技术；家纺行业

**中图分类号：**TP399      **文献标志码：**A      **DOI：**10.19358/j.issn.2097-1788.2026.01.006

**中文引用格式：**刘海阳, 李哲行. 可信数据空间技术路线的研究与家纺行业应用 [J]. 网络安全与数据治理, 2026, 45(1): 35–41.

**英文引用格式：**Liu Haiyang, Li Zhexing. Research on the technical roadmaps of trusted data space and its application in the home textile industry [J]. Cyber Security and Data Governance, 2026, 45(1): 35–41.

## Research on the technical roadmaps of trusted data space and its application in the home textile industry

Liu Haiyang, Li Zhexing

(China Electronics Digital Innovation, Beijing 100083, China)

**Abstract:** Under the background of data factor marketization reform, constructing a robust national data infrastructure system is crucial for facilitating the efficient data flow and unleashing data value, thereby enhancing the quality and efficiency of the digital economy. This research focuses on the technical roadmap of trusted data spaces, systematically analyzing its architecture, key technologies, and implementation approaches, with the aim of addressing issues related to security, controllability, and trust in data circulation. By incorporating practical application scenarios from the home textile industry, a JSON-based digital contract solution is proposed. Comparative analysis with traditional data protection techniques highlights its advantages in fine-grained control and performance. This study provides both technical references and practical demonstrations for the industrial deployment of trusted data spaces.

**Key words:** digital contract; trusted data space; usage control technology; home textile industry

## 0 引言

2019年10月，党的十九届四中全会明确指出将数据列为新型生产要素，与土地、资本、劳动力、技术等传统生产要素并列，标志着数据要素市场化配置正式上升为国家战略。此后，国家出台多项政策文件，系统推进数据要素市场培育与发展，并将其作为数字经济时代的重要制度安排。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）》（以下简称“行动计划”），明确指出到2028年，可信数据空间运营、技术、生态、标准、安全等体系取得突破，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<sup>[1]</sup>。可信数据空间通过使用控制、数字合约等核心技术，结合隐私计算、区块链等技术有效保障数据安全流通，打破“数据孤岛”，促进跨组织、跨领域、跨区域协作。其核心价值在于建立权属清晰、流通可信的机制，激发数据要素潜能。同时，标准化接口与合规框架能提升数据供给质量，推动形成高效、公平的市场化配置体系，为数字经济高质量发展提供数据设施支撑。

本文基于国际数据空间协会（International Data

Space Association, IDSA) 与国内可信数据空间生态企业的相关研究, 对可信数据空间的发展现状与存在问题进行梳理。针对相关问题, 依据国际数据空间架构元模型设计了一套可信数据空间系统架构, 创新性地基于 JSON 格式并结合《可信数据空间 数字合约技术要求》标准, 实现一个类开放数字权利语言 (Open Digital Rights Language, ODRL) 的数字合约样例, 并结合家纺行业的实际应用案例展开介绍, 旨在为可信数据空间技术路线的研究与应用提供参考和借鉴。

## 1 现状背景

### 1.1 发展现状

可信数据空间的概念最初源自德国弗朗霍夫应用研究促进会的创新研究成果, 其核心架构通过分布式存储与中心化认证相结合的混合模式, 构建安全可靠的数据协作生态。该技术体系依托数字合约、访问控制以及使用控制实现自动化规则执行, 确保数据在流通过程中的安全性与合规性要求得到满足, 适用于需要跨组织数据共享与协同的应用场景。近年来欧盟在可信数据空间体系上持续投入, 在战略规划、资金支持和行业推动下已经成为欧盟数字基建的重要部分。目前受《欧洲数据战略》规划支持, 以及数字欧洲计划、地平线计划等计划的资金支持, 欧盟已建立 14 个通用可信数据空间<sup>[2]</sup>, 覆盖能源可信数据空间、农业可信数据空间等。截至 2024 年 8 月, Data Spaces Radar 共计公开了 145 个可信数据空间案例, 涵盖智慧城市、农业、健康等行业。图 1 统计了近年欧盟可信数据空间数量及发展趋势<sup>[3]</sup>。

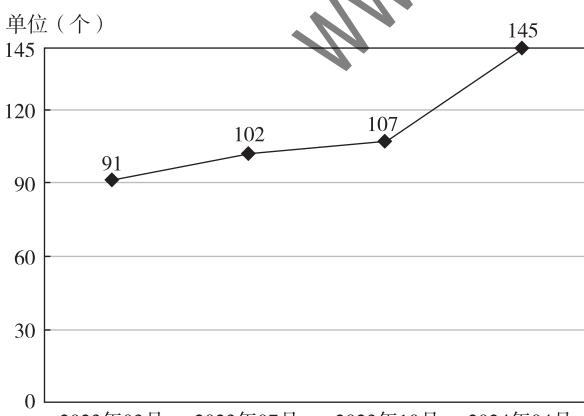


图 1 可信数据空间案例数量  
(数据来源: 国际数据空间组织)

相较于欧盟, 我国基于前期国外研究基础, 近些年在可信数据空间技术路线上亦持续投入, 除出台上述行动计划以外, 在政策上国家数据局还发布了

《2025 年可信数据空间创新发展试点工作方案》, 组织开展企业、行业、城市三类可信数据空间试点工作<sup>[4]</sup>。截至 2025 年 7 月, 试点名单企业共有 63 家<sup>[5]</sup>, 覆盖上海、温州、贵阳等共计 13 个城市。

在标准层面, 目前主要由国家数据局下属全国数据标准化技术委员会 (以下简称“数标委”) 和企业自发组织的可信数据空间发展联盟 (Trusted Data Spaces Alliance, TDSA) 牵头制定, 目前已发布的标准如表 1 所示。

表 1 标准发布梳理表

序号	数标委	TDSA
1	可信数据空间 技术架构	可信数据空间标准体系建设指南
2	可信数据空间 数字合约技术要求	可信数据空间 能力要求
3	可信数据空间 使用控制技术要求	
4	可信数据空间 技术能力评价规范	

综上可见, 我国可信数据空间技术路线发展正按照行动计划逐步推进, 发展已初具规模, 但在配套资金投入总额上较国外稍显滞后。

### 1.2 面临问题

当前, 我国可信数据空间建设已取得初步进展, 但仍面临诸多挑战。一方面, 基于 W3C 标准的开放数字权利语言 (如 ODRL、MyData 等) 开源资源较为匮乏, 难以支持数字合约的签署与实施, 制约了可信数据空间的进一步发展。另一方面, 可信数据空间形态与模式尚未明确定义。尽管数标委和 TDSA 等机构已发布相关技术文件与标准, 企业在实际构建产品过程中仍处于探索阶段, 其原因在于可信数据空间概念被过度泛化, 导致生态企业难以明确其具体形态应表现为硬件、软件系统、平台还是客户端。

针对上述问题与发展现状, 本文提出应明确可信数据空间的核心技术范畴, 系统阐述各类技术元模型并给出参考示例, 同时基于国际可信数据空间架构元模型, 设计了一套可信数据空间系统架构。结合《可信数据空间 数据合约技术要求》标准, 创新采用 JSON 格式实现了一套数据内容使用权限的数字合约示例, 并通过家纺行业的实际应用案例进行说明, 以助力解决数字权利语言资源不足、数字合约实施困难等关键瓶颈, 为可信数据空间的技术研究与实践应用提供参考。

## 2 核心技术

### 2.1 访问控制技术

访问控制技术是一种安全机制, 其核心功能是通过预先定义的策略和规则, 对系统资源的访问进行精确授权与限制。访问控制参考模型如图 2 所示。

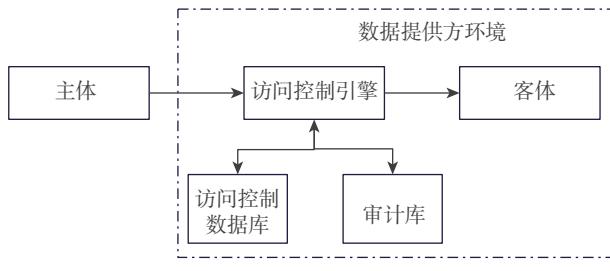


图 2 访问控制参考模型

注：主体是请求访问的实体（如用户或进程），客体是被访问实体（如文件、数据库或服务）。访问控制引擎调取访问控制数据库中访问策略对访问请求进行管控（如仅财务部可阅），并将访问请求的行为记录在审计库中

访问控制类型分为自主访问控制（Discretionary Access Control, DAC）、强制访问控制（Mandatory Access Control, MAC）、基于角色的访问控制（Role-Based Access Control, RBAC）、基于属性的访问控制（Attribute-Based Access Control, ABAC），各类型具体内容如表 2 所示。

表 2 访问控制类型示例表

访问控制类型	定义	访问控制策略
DAC	在 DAC 框架中，访问控制策略的制定权归属资源创建者。所有者基于自主决策机制，动态定义主体对客体操作权限集，并通过显示授权实现跨用户的受限资源共享。	策略：访问客体由创建者预定义访问控制列表，如小米进程可读写相册数据，支付宝进程仅可查阅相册数据。
MAC	强制访问控制模型的核心特征在于为主体（如用户进程）和客体（如文件资源）分配不可篡改的安全等级。该等级由系统安全策略管理器或授权管理员依据相关法律、标准与安全规则设定。	策略：绝密人员可读取机密文件。
RBAC	在基于角色访问控制模型中，系统管理员负责定义一组角色，并将这些角色指派给系统中的主体。同时访问权限被关联到客体或客体类型上。主体能否执行特定相应操作（如访问、修改某个客体），取决于主体是否被赋予了相应权限的角色。	策略：员工仅能查看自己薪酬，人事总监可以查询公司全部人员薪酬。
ABAC	通过动态计算一个或一组属性是否满足某种条件来判定是否可以访问客体。	策略：年龄大于 18，互联网协议地址（Internet Protocol Address, IP）在加拿大，可读取网站数据。

## 2.2 使用控制技术

使用控制是通过在数据使用方设备开辟一块数据提供方可控区域，通过加载执行相关使用控制策略将数据控制权始终保持在数据提供方。常见的数据使用

控制策略包含基于控制数据使用时长与控制数据使用次数的策略。使用控制参考模型如图 3 所示。

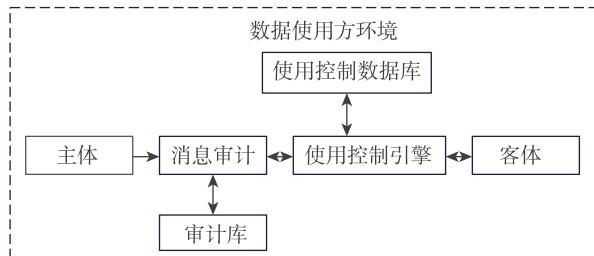


图 3 使用控制参考模型

注：主体是请求访问的实体（如用户或进程），客体是被访问实体。消息审计负责记录主体访问行为，并将行为存储在审计库中。使用控制引擎负责调取使用控制数据库中参数与策略，判断是否到达数据使用边界条件

参考 IDSA 技术架构<sup>[6]</sup>（如图 4 所示），在连接器数据处理流程中，数据提供方侧强制执行数据使用控制。核心容器负责数据处理，并利用 Apache Camel 中间件进行消息路由拦截与汇总。为实现控制集成，系统强制所有消息流经数据使用控制应用程序，确保连接器处理的任何数据均受到管控。在数据使用方侧，当连接器消费数据时，将数据转发至使用方的数据接收端。与提供方侧基于路由配置强制执行控制的方式不同，使用方侧采用拦截模式来实现数据使用控制。该模式允许控制逻辑嵌入到每个消息路由中，从而能够在数据流转的各个环节灵活应用控制规则。因此，提供方侧的控制核心在于路由配置，确保出口数据必检，而使用方侧的核心控制在于消息拦截，实现对内部处理流程的细粒度监管。

## 2.3 数字合约

参考数标委发布的 TC609—6—2025—01《可信数据空间技术架构》，数字合约可以定义为一种基于机器可读的数字化协议，通过预编程逻辑自动执行、验证并强制履行合约条款。预编程逻辑包含但不限于对数据使用方、使用方式、使用次数、使用范围等作限制<sup>[7]</sup>。这里数字合约可不依赖区块链技术实现。基于 JSON、XML 合约描述语言示例如下：

```

(1) JSON: {
  "contractId": "connector-3509",
  "contractName": "测试合约"
}

(2) XML:
<digitalcontract>
<contractId>connector-3509</contractId>
<contractName>测试合约</contractName>
</digitalcontract>

```

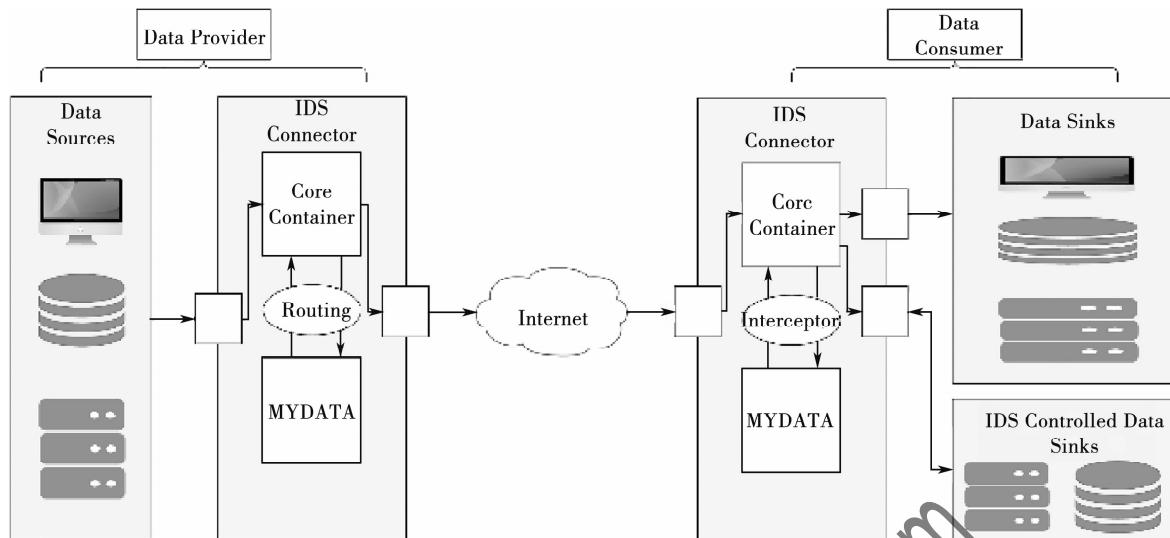


图 4 路由和拦截方式  
(数据来源: 国际数据空间组织)

## 2.4 连接器技术

连接器是用于可信数据空间实现主体互联、数据互通的装置, 可以是软件客户端形式, 亦可以是硬件路由器形式, 用于实现可信数据空间入网检测、点对点传输、使用控制等核心功能。其关键核心为在数据

使用方侧开辟一块数据提供方侧可控的资源。

入网检测: 通过连接器对进入可信数据空间的用户进行身份校验。通常每个合法连接器均会颁发一个合法标识, 相关标识体系可参见表 3<sup>[8]</sup>。当前我国出台标准中, 尚未明确具体参考标识体系。

表 3 标识体系示例

编码体系	编码格式	描述	示例
VAA	发行机构代码 服务机构代码/企业内部代码	VAA 基本代码结构由三部分组成: 发码机构代码、服务机构代码和企业内部代码。服务机构代码分为三部分: 国家代码、行业代码和企业代码。企业内部代码由企业自行分配。	88. 100. 12345678/abc
Handle	前缀/后缀	Handle 标识由前缀和后缀编码构成, 两者之间由“/”分隔。从一级前缀开始, 从左向右依次拓展, 尾码可直接使用本地化标识。	86. 1000. 14/00121336401058520100
OID	国家标识码. 领域标识码. 行业标识码. 企业标识码. 内部编码. 对象标识码	OID 编码结构为树状结构, 由一系列数字、字符或符号组成, 不同层次之间用“.”分隔, 标识编码是由根到叶子节点全部路径上的节点顺序组合而成的字符串。	1. 2. 156. 3001. 05. 01. 1001. 01
Ecode	版本 编码体系标识 主码	Ecode 编码结构一般为三段式, 由版本 (V)、编码体系标识 (NSI) 和主码 (MD) 构成。V 用于区分不同数据结构的 Ecode; NSI 用于指示某一标识体系代码; MD 用于表示某一行业或应用系统中标准化的编码。	0 0001 6901234567892
GS1	厂商识别码 商品项目识别码 校验码	GSI 由三部分组成, 分别为厂商识别码、商品代码和校验码。右侧示例中, 6901234 为厂商识别码, 其中 690 为前缀码, 由国际编码协会分配给中国; 56789 为商品项目代码; 末尾数字为 2 为校验码。	6901234567892
MA	用户标识/对象类目/自定义对象个体编码	MA 编码为分级编码结构, 分为用户标识、对象类目、自定义对象个体编码三个部分。用户标识由前缀“MA”、国家地区领域代码、地域或行业代码、用户代码四部分组成。对象类目分为通用编码结构和自有编码结构两种情形, 通用编码结构由三个节点组成, 自有编码结构层次数量由用户定义。自定义对象个体编码由用户根据应用需求自定义节点数量和每个节点的位数。每两部分之间以“.”或“/”符号隔开。	MA. 156. 3701. 1369/10. 321672. 型号码/自定义编码个体

点对点传输：连接器形式暴露数据提供方或使用方侧 IP 地址，通过 post 或 pull 形式将数据发送至数据使用方侧，中间不通过任何中间服务平台，实现数据点对点直传。

使用控制：使用控制技术逻辑上文已做介绍，这里不多做阐述，连接器除将使用控制技术应用集成外，还将数字合约和数据的使用环境与外界隔离，防止数据和数字合约被恶意篡改，保障使用控制的有效实施。

### 3 应用场景

#### 3.1 场景背景

可信数据空间在非结构化数据处理中具有广泛的应用前景。在图纸类传输与协同设计等场景中，由于对图纸数据精度与色彩保真度具有极高要求，必须确保图纸在传输过程中不会因压缩、加密等处理而导致失真，从而能够以高度还原的形式送达使用方。针对此类需求，结合数字合约的使用控制技术展现出显著优势，能够实现对数据使用权限的精准控制，同时在保障安全性的前提下维持数据的完整性与可用性。

以家纺行业落地场景为例。家纺行业入门门槛较低，当前产品生产大多以白布为基础，通过数码印花技术印制图案后进行销售。因此，数码印花图纸成为家纺企业核心竞争力的关键所在。然而，数码印花图纸的盗用现象频发，严重损害了相关企业的品牌信誉与经济利益。实现在图纸盗用之初就进行及时有效的管控非常必要。

#### 3.2 架构设计

针对以上背景，本研究参考 IDSA 架构元模型构建了家纺行业可信数据空间架构，创新性地基于 JSON 格式并结合《可信数据空间 数字合约技术要求》标准，实现一个 ODRL 的数字合约样例，并在合约中生成一个基于家纺行业的打印布匹米数的行业策略。通过该策略，对数码印花打印机布匹打印米数做使用控制，并在数码印花图纸打印完毕后自我销毁，实现了数码印花图纸数据流通使用范围可控。家纺行业可信数据空间参考架构如图 5 所示。

此架构涵盖数码印花图纸提供方、连接器、中心服务平台、数码印花图纸布匹打印代工厂（简称“代工厂”）四个主体。数码印花图纸提供方负责提供数码印花图纸。连接器负责审核数码印花图纸提供方与代工厂身份可信，并部署使用控制引擎结合数字合约对布匹打印米数做控制。中心服务平台负责数字合约商讨与签订。代工厂负责按照数字合约要求打印数码印花图纸布匹。具体实施步骤如下：

- (1) 数码印花图纸提供方与代工厂通过连接器进入可信数据空间；
- (2) 数码印花图纸提供方与代工厂就数码印花图纸使用范围、打印米数做商讨，并签订合约；
- (3) 签订数字合约在中心服务平台备份，并同步发送给数码印花图纸提供方与代工厂连接器，数码印花图纸提供方发送数码印花图纸到代工厂；

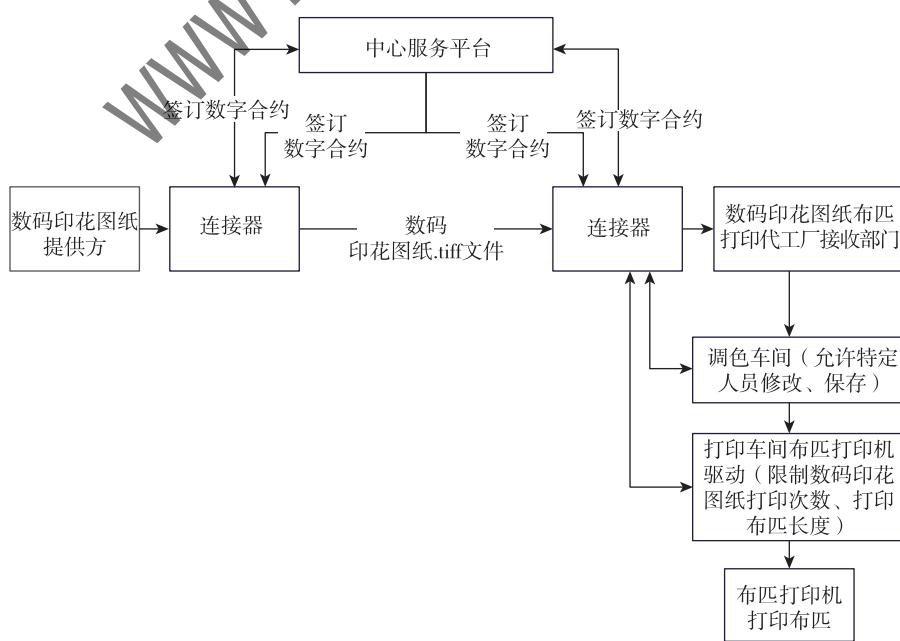


图 5 家纺行业可信数据空间架构图

注：双方在中心服务平台磋商数字合约，数字合约约束数码印花图纸使用边界条件，如布匹打印米数、印花图纸打印次数、印花图纸传输次数

(4) 代工厂按照数字合约生产印花图纸布匹, 代工厂的连接器实时监测印花图纸使用状态;

(5) 数字合约伴随印花图纸使用状态动态更新, 一旦到达边界条件, 代工厂连接器启动自我删除功能, 将数码印花图纸删除。

场景中的连接器以客户端形式实现, 数据调用信息可以应用 IDSA 中 Apache Camel 进行拦截与汇总, 亦可以应用其他中间件进行消息汇总与拦截。合约主体内容参考《可信数据空间 数字合约技术要求》<sup>[9]</sup> 标准做了相应修订与裁剪, 如表 4 所示。通过对数码印花图纸制定数据使用策略, 并将策略以数字合约形式部署在数据方客户端中, 结合使用控制技术, 有效保障家纺行业数码印花图纸提供方的数据主权。场景中, 自我删除执行时间接近 0 s, 有效限制数码印花图纸滥用<sup>[10]</sup>。

表 4 数码印花图纸合约主体内容

序号	合约信息	说明
1	合约标识码	数字合约的唯一标识。
2	合约名称	描述数字合约具体内容的标题名称。
3	合约简介	数字合约的简要描述信息, 包括但不限于合约标的、签署主体名称和合约策略说明。
4	合约状态	数字合约全生命周期的状态, 如发起、协商、签署(失败、成功)、执行、终止。
5	创建时间	数字合约创建完成的时间, 如 2025 年 6 月 1 日 12: 00: 00。
6	签署模式	数字合约签署方式, 如数据提供方与数据使用方点对点签署、可信数据空间服务平台作为中介方协调数据提供方和数据使用方完成签署以及多方主体之间达成共识签署。
7	签署主体标识码	签署主体的唯一标识。
8	签署主体名称	描述签署主体的名称。
9	签署时间	数字合约多方最终签署完成的时间, 如 2025 年 6 月 10 日 12: 00: 00。
10	签署签名	数据提供方、数据使用方和数据服务方等数据参与方主体签署数字合约的数字签名信息, 应包括合约标识码、签署时间。
11	扩展信息	其他相关说明, 如合约版本、附件信息、补充条款等。
12	执行后属性	这里涵盖合约结束日期。
13	合约属性	数字合约具体约束条件。

### 3.3 数字合约与策略展示

合约场景: 数码印花图纸提供方 A 允许代工厂 B 生产加工数码印花图纸布匹 100 m, 代工厂在分发合

约前有对合约署名义务, 违约则被追责, 图 6 是基于场景, 用 JSON 生成的数字合约示例。contractId 是中心服务平台生成的合约唯一标识字段, 可用于防篡改。contractPolicies 是用于规定合约属性内容的字段, 此字段基于家纺行业, 细化一个 printmeter 的行业属性, 用于约束打印布匹米数。



图 6 数字合约示例

## 4 技术对比

### 4.1 对比数字版权管理

传统数字版权管理 (Digital Rights Management, DRM) 系统通常侧重于内容加密与终端设备绑定, 通过严格的版权许可管理防止未授权访问与复制。然而, 其控制逻辑相对僵化, 难以适应跨组织、高频率的数据协作场景。在性能方面, 传统 DRM 通常需要对整个文件进行加密或解密, 在处理高清晰度与高精度的数码印花图纸等大型非结构化数据时, 性能开销与延迟显著。本文方案通过连接器在数据使用环境内实施控制, 无需全程加密传输, 保障了数据原始保真度与传输效率。在适用性方面, 传统 DRM 多为封闭生态系统, 跨平台、跨厂商协作困难。本研究基于标准化的 JSON 合约和可信数据空间架构, 打破了不同主体与系统间的数据孤岛。

## 4.2 对比区块链

区块链技术通过分布式账本和数字合约确保了交易不可篡改与可追溯性，但在相关应用场景也存在局限性。在性能与吞吐量方面，区块链尤其是公有链的交易处理性能有限，且存在延迟，难以满足家纺行业高频、大规模数码印花图纸传输与合约验证需求。本文方案将数字合约与区块链解耦，合约的执行在连接器内部完成，仅需将关键审计日志上链存证，从而实现性能与可信的平衡。在适用性方面，区块链方案适用于对交易清算、权属证明有强公证需求的场景。而家纺行业中更加关注数码印花图纸的使用过程控制，其核心是实时、高效地执行策略，基于轻量级 JSON 合约的连接器方案更加轻便、灵活，成本效益更高。

表 5 列出了本文方案与传统 DRM 方案、区块链数字合约方案的性能对比。

表 5 可信数据空间与传统技术对比

对比维度	传统 DRM 方案	区块链数字合约方案	可信数据空间方案
适用性	访问控制、防复制	交易确权、存证	使用控制（次数、范围、行为）
性能开销	高（加密计算，尤其非结构化数据场景）	高（共识延迟、链上计算，尤其非结构化数据场景）	低（本地执行策略，无共识开销，加密可按需配置）

## 5 结论

本文系统梳理了国内外可信数据空间的发展现状与关键技术，聚焦于数据流通中的安全性、可控性与互信问题，提出了一套面向家纺行业的可信数据空间架构与数字合约实现方案。核心贡献包括：

(1) 明确了可信数据空间的核心技术体系，涵盖访问控制、使用控制、数字合约与连接器技术，并基于国际数据空间架构元模型设计了适用于家纺行业的实施框架；

(2) 创新性地采用 JSON 格式实现了符合《可信数据空间 数字合约技术要求》的数字合约示例，提出了针对印花图纸使用控制的行业策略，实现了细粒度、高性能的数据权限管理；

(3) 通过家纺行业实际应用案例，验证了该架构在防止数据滥用、保障数据主权方面的有效性，为行业落地提供了可借鉴的实践路径。

展望未来，建议从以下方面持续推进可信数据空

间的发展：一是加强标准落地与开源生态建设，推动数字合约技术的标准化与共享；二是深化行业应用研究，拓展更多高价值场景；三是加大政策与资金支持力度，提升我国在该领域的自主创新与国际竞争力。

## 参考文献

- [1] 国家数据局. 可信数据空间发展行动计划（2024—2028 年）[EB/OL]. (2024-11-21). [https://www.gov.cn/zhengce/zhengceku/202411/content\\_6996363.htm](https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm).
- [2] 云基华海前沿技术研究院. 2025 年国际可信数据空间发展现状与趋势研究报告 [R]. 2025.
- [3] International Data Spaces Association. The Data Spaces Radar report [R/OL] [2025-08-01]. <https://internationaldataspaces.org/use/data-spaces-radar/>
- [4] 国家数据局综合司. 国家数据局综合司关于组织开展 2025 年可信数据空间创新发展试点工作的通知 [EB/OL] (2025-04-03). [https://www.gov.cn/zhengce/zhengceku/202504/content\\_7017511.htm](https://www.gov.cn/zhengce/zhengceku/202504/content_7017511.htm).
- [5] 国家数据局. 2025 年可信数据空间创新发展试点名单公示 [EB/OL] (2025-07-08). [https://www.nda.gov.cn/sjj/hdjl/wsdejgs/0708/20250708101622072845053\\_pc.html](https://www.nda.gov.cn/sjj/hdjl/wsdejgs/0708/20250708101622072845053_pc.html).
- [6] International Data Spaces Association. Usage control in the international data spaces [EB/OL] (2021-xx-xx). <https://internationaldataspaces.org/>.
- [7] 全国数据标准化技术委员会. 可信数据空间 技术架构 [S/OL]. (2025-04-30). [https://mp.weixin.qq.com/s?\\_\\_biz=MjM5NjE1OTc4Mw==&mid=2651643625&idx=2&sn=a8eb80b4dd6b411e033336eba3462239&chksm=bc8fc92176aff2db5e35d0122294f8de85bf78a75c5e00d8cb9a08bd7f156588afec1d2720c0&scene=27](https://mp.weixin.qq.com/s?__biz=MjM5NjE1OTc4Mw==&mid=2651643625&idx=2&sn=a8eb80b4dd6b411e033336eba3462239&chksm=bc8fc92176aff2db5e35d0122294f8de85bf78a75c5e00d8cb9a08bd7f156588afec1d2720c0&scene=27).
- [8] 工业互联网标识智库. 全球工业互联网标识解析体系总揽 [EB/OL] (2022-11-13). [https://mp.weixin.qq.com/s?\\_\\_biz=MzU1OTUxNTI1NA==&mid=2247524231&idx=1&sn=49bad1f696ddbd59ee57c6017d976c85&chksm=fc14cc9ecb634588a38f89d80ebd23f13bc8d33835dc356bd32767df5e12bbfd2e8285594b56&scene=27](https://mp.weixin.qq.com/s?__biz=MzU1OTUxNTI1NA==&mid=2247524231&idx=1&sn=49bad1f696ddbd59ee57c6017d976c85&chksm=fc14cc9ecb634588a38f89d80ebd23f13bc8d33835dc356bd32767df5e12bbfd2e8285594b56&scene=27).
- [9] 全国数据标准化技术委员会. 可信工业数据空间 数字合约技术要求 [Z]. 2022.
- [10] 江苏省人民政府. 南通市家纺行业数据基础设施入选国家优秀案例 [EB/OL] (2025-09-01). [https://www.jianshu.gov.cn/art/2025/9/1/art\\_87819\\_11642978.html](https://www.jianshu.gov.cn/art/2025/9/1/art_87819_11642978.html).

(收稿日期：2025-09-01)

## 作者简介：

刘海阳（1991-），男，硕士，工程师，主要研究方向：数据元件、可信数据空间技术路线、数据要素领域标准化。

李哲行（1989-），男，硕士，工程师，主要研究方向：数据要素、产业规划、城市规划。

## 版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部