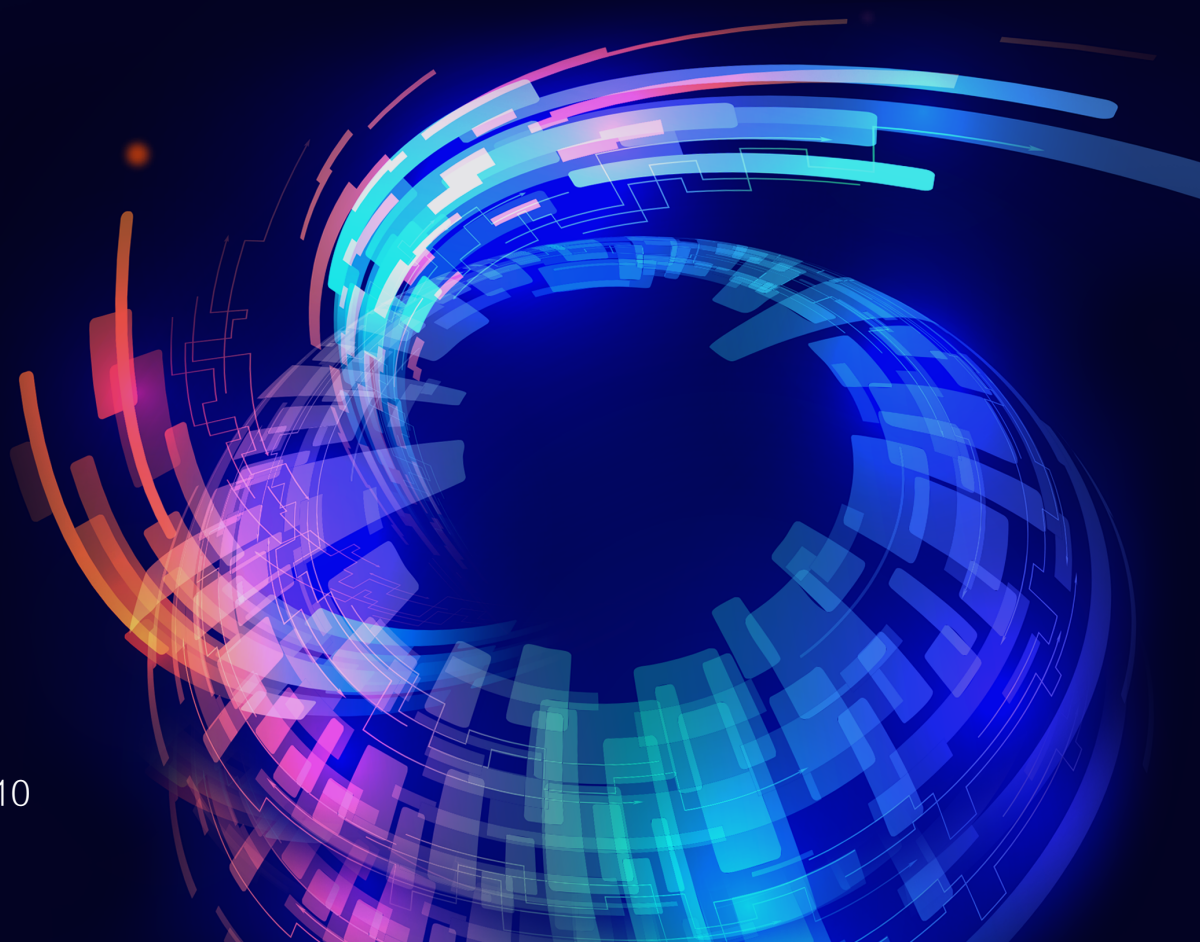
FISCO金链盟

观韬中茂律师事务所 Guantao Law Firm

金融科技微洞察

DDTP：分布式数据传输协议

个人信息可携带权的中国路径倡议



2021.10

PREFACE

前言

数据要素已成为数字经济时代最核心的生产要素，如何解放数据生产力、发挥数据要素提升生产效率的作用、推动数字经济高质量发展已经成为社会各界广泛关注的议题。

在所有类型的数据中，个人信息（或称“个人数据”）占比最高，面临的挑战也最大：个人数据虽然由个人创建，但很多情况下却需要在企业之间流转，责任主体和利益主体不一致，导致个人数据流转困难。

个人信息可携带权的出现为应对这一挑战提供了思路。个人信息可携带权赋予了个人主动在企业间流转个人信息的权利，因而有望解决个人数据流转困难的问题。

欧洲、美国、新加坡、韩国、印度等国家和组织已经针对个人信息可携带权出台了相应的法律制度。在国内，2021 年 8 月 20 日正式通过的《个人信息保护法》也首次规定了“个人信息可携带权”的相关内容。个人信息可携带权的立法，体现了将个人信息权利还归个人的立法思路，为个人信息流转提供了新的方向，也将为行业带来新的机遇。

实践方面，个人信息可携带权在境外已经形成了平台主导和政府主导两种不同的发展路径。不过从效果上来看，这两种模式均缺乏可信的验证机制和激励机制，暂不能实现广泛的、可跨行业通用的个人信息携带，在安全存储、可信传输、协同生产三方面存在局限性，难以解决当前问题。

在国内，随着区块链等新技术的发展，个人信息可携带权的实践模式出现了一些亮点，如粤澳健康码互认项目。该项目由用户个人主导，通过用户主动发起个人信息数据传输并自行上传，结合基于哈希值的可验证数字凭证——“数据指纹”上链，做到了信息携带与可信验证的平衡，进而实现了数据的

前言

可信传输。该方案对未来通过个人信息可携带权解决个人数据流转问题带来了启发。

基于此，深圳市金融区块链发展促进会（以下简称：金链盟）联合观韬中茂律师事务所、金融科技·微洞察等，联合发布 DDTP（Distributed Data Transfer Protocol）白皮书。本白皮书对全球现有主要个人信息可携带权的实践模式进行梳理，分析其优势和局限性，在结合已有案例的基础上，提出适合我国的个人信息可携带权实践模式倡议，希望能为社会各界提供借鉴和参考。

Contents

目录

01

核心目标：解放数据生产力，助力数字经济发展

数据要素的特殊属性、治理挑战和应对思路

随着数字经济的蓬勃发展，中共中央、国务院在 2020 年发布《关于构建更加完善的要素市场化配置体制机制的意见》中，首次将数据要素与劳动、资本、技术和土地等要素并列，构成新时期经济发展的五大核心生产要素。

与其他传统生产要素相比，数据要素具有易复制性、非竞争和非排他性、分散性、价值聚合性和价值认知多样性等特殊属性。这给数据要素的使用和治理带来了巨大的挑战。

作为生产要素的通用要求和数据要素的特殊挑战，数据要素需要满足三大核心诉求：安全存储、可信传输及协同生产。其中，安全存储是指满足数据的安全计算和可靠存储要求；可信传输是指数据在不同所有者和控制方传递过程中，能追踪数据全流程，保护数据权利，并保证数据的可信任、可检验；协同生产是指打通多方之间的可信数据，互联互通，让更广范围内的更多数据联合发挥更大价值，并在此过程中满足隐私保护和合规要求。

为此，在进行数据相关的应用探索时，需要考虑通过区块链、人工智能、云计算、大数据等前沿技术构建新型的数据新基建解决方案，实现更深层次、更广领域的信任传递，最终实现数字经济生产力的全面解放，推进产业数字化的发展。

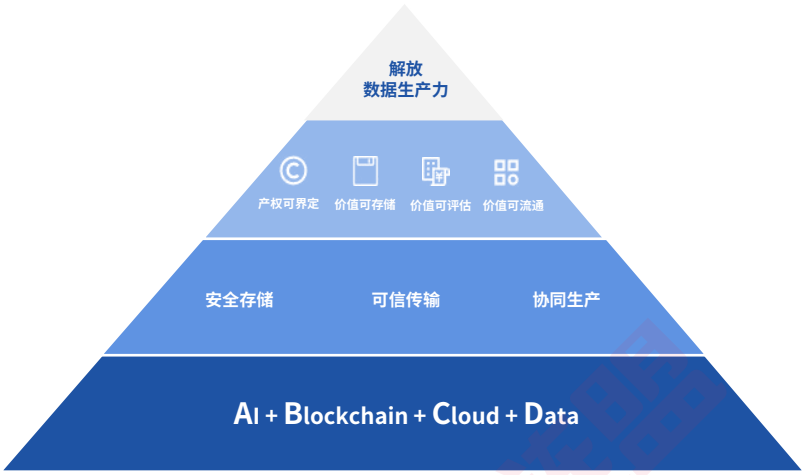


图 1 解放数据生产力

个人数据占比最大且挑战复杂

一般认为，数据按照创建来源可以分为政务 / 公共数据、企业数据和个人数据。

规模方面，在参考了业界的多份研究成果后进行的估算结果显示：在全球产生的所有数据当中，政务数据占比不到 1%，企业数据占比约 32%，个人数据占比则可高达 68%[1]。

近年来，各级政府和各类市场主体都在努力通过公共政策和产业布局来充分发挥各类数据的作用，释放数据生产力。政务 / 公共数据方面，面临的挑战主要来自于体制机制障碍和壁垒。各级政府通过制定数据开放政策、建设大数据平台等方式，大力推进政务数据共享和开放，持续破除体制机制障碍和壁垒。企业数据方面，主要问题是数据流通和交易不畅。随着征信机构、数据交易所等机构的发展，这个问题也正在逐步得到解决。

个人数据方面，主要面临着个人数据流转难的问题。与其它两类数据相比，个人数据具有来源更加分散、价值聚合性更强的特点，还面临着产权不清晰，处理难度大等现实问题，针对个人数据的基础设施建设进展缓慢。随着个人信息隐私保护逐渐趋严，个人数据获取成本日渐提高，个人数据流转难的问题日益凸显。

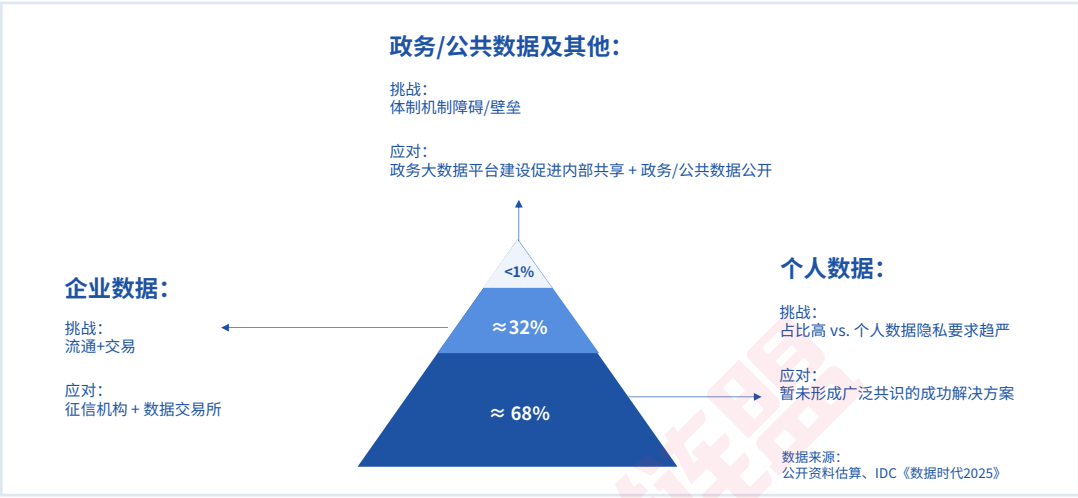


图 2 个人、企业和政务 / 公共数据的比例及面临的挑战

个人数据占比最高，面临的挑战最复杂，迫切需要一个合适的方案，实现个人数据高效且合规地流转和使用。

个人信息传输现状：三重授权的被动模式（B2B）

目前，国内外个人信息流转的主流实现模式为基于商业合作的企业间直接传输模式。流转方式较为简单，个人信息的流转由提供者或接收者发起，经个人授权同意后，个人信息数据就直接从提供者通过 API 传输到接收者。

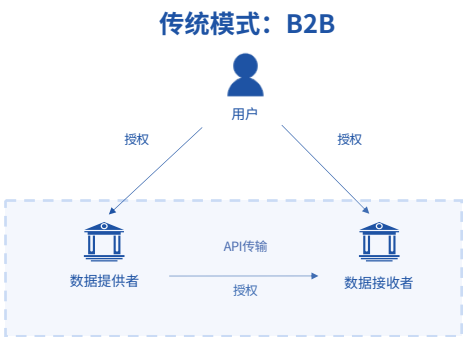


图 3 国内外主要个人信息流转模式

以国内为例，参考北京知识产权法院（2016）京 73 民终 588 号这一指导案例的判决书：“个人信息流转需要遵循三重授权原则，即用户授权提供者使用个人信息，提供者授权接收者使用其获取的个人信息，用户授权接收者可以使用其从提供者处获取的个人信息。”

实际操作时，信息接收者通常会先和信息提供者签署使用用户信息的相关协议，再在为用户提供服务时申请用户授权。

不过，这种模式下的数据传输是基于商业利益进行的，用户处于被动地位，无法主动进行个人信息的精准授权，也无法避免强制授权、过度授权等情况的发生，用户权利难以保障。在存储方面，用户个人信息存储在数据提供者服务器，存储安全性依赖于数据提供者，用户也不可自行选择存储位置。在协作方面，由于没有标准化的统一数据传输方式，每次协作都需要企业间两两协商确定协作方式，同行业的企业之间由于存在竞争关系，也很难进行协作。

因此，在《个人信息保护法》正式实施后，这种模式将面临巨大的法律挑战。《个人信息保护法》第二十三条规定：“个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。”这就极大地增加了个人信息流转的法律合规成本，个人信息处理者必须积极探索新的个人信息流转合规模式。

表 1 个人信息流转主流模式的优缺点比较

	优点	局限性
安全存储	-	• 安全性依赖数据提供者 • 用户不可选择存储位置
可信传输	经双方定制可传输多种类型数据	• 用户地位被动，隐私权利难以保障 • 无法精准授权
协同生产	基于商业利益的跨行业协作	• 无标准协同方式，需企业间两两协商，协作效率低 • 同业竞争性机构间难以实现协同

【注】

[1] 个人及企业数据量根据 IDC《数据时代 2025》估计，政务数据量根据中国信通院《政务数据共享开放安全研究报告》中的数据估算。由于数据每时每刻都在加速产生，总量较难统计，目前具体类型数据的占比尚无权威数据，因此本估算数据仅供参考。

02

立法倾向：个人信息可携带权将个人权利还于个人

个人数据流转难的关键在于个人数据虽然由个人创建，但大多数情况下却需要通过企业流转，责任主体和利益主体不一致。近年来，随着“个人信息可携带权”的出现，明确了个人拥有主动在企业间流转个人信息的权利，为个人数据的流转和使用提供了新的机遇。

全球个人信息可携带权的立法进程

“个人信息可携带权”这一法律概念最早由欧盟立法提出。2016 年 7 月，欧盟理事会和欧洲议会表决通过了《通用数据保护条例》（GDPR），并于 2018 年 5 月正式实施。这是全球范围内首个提及可携带权的法案，其中第 20 条规定：“数据主体有权获取其提供给数据控制者的相关个人数据，其所获取的个人数据形态应当是结构化的（structured）、通用的（commonly used）和机器可读的（machine-readable），且数据主体有权将此类数据无障碍地从该控制者处传输至其他控制者处。”

2017 年 4 月，欧洲数据保护委员会（EDPB）在《数据可携带权指南》（Guidelines on the right to data portability）中进一步规定了数据可携带权的具体权利范围和保障措施。例如，可携带数据的范围应遵循“provided by”原则，即数据主体“提供”的数据，如主动上传的姓名、地址、邮箱，以及观测数据主体而产生的原始数据，如日志、浏览记录等。传输方式上，可以是 API、Portal 等方式，也可以是 XML、CSV 等易用的一般通用格式。

GDPR 颁布后，其它国家和地区也纷纷跟进。如美国加州于 2018 年 6 月签署了《消费者隐私法案》（CCPA）。与 GDPR 类似，“消费者有权要求经营者将其个人信息以易于使用或传输（即可携带）的方式向消费者提供，以便消费者可以无障碍地将信息传输给第三方”。印度

2019 年 12 月通过的《个人数据保护法》规定："数据主体有权以结构化、通用化且机器可读的格式接收向数据受托者提供的个人数据，以及以该格式将该数据转让给任何其他数据受托者"。韩国先是在 2020 年 1 月修订的《信用信息法》中规定了在 MyData 等政府服务中可以应个人要求传输个人信息到服务运营商，后又在 2021 年 1 月公开征求意见的《个人信息保护法（修正案草案）》中添加了个人信息可携带权的相关条款。新加坡 2020 年 11 月通过的《个人数据保护法》（PDPA）修正案也规定："个人可以要求负责数据转移的机构组织将个人资料传送至指定的数据接受方"。

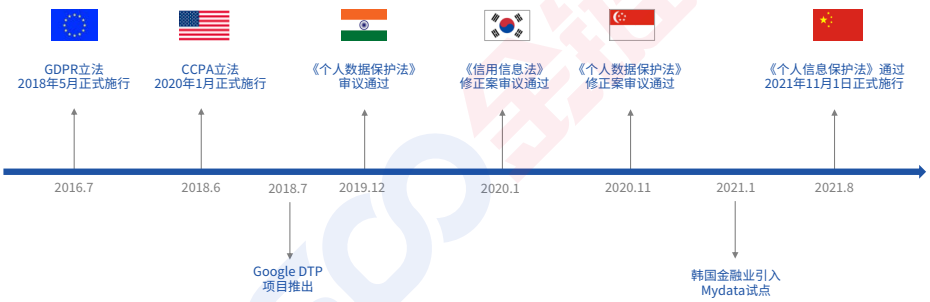


图 4 全球个人信息可携带权立法进程

在我国，个人信息可携带权的设立可谓一波三折。早在 2017 年 3 月，45 位全国人大代表就在当年的两会上提交了《关于制定 < 中华人民共和国个人信息保护法 > 的议案》，并同时提交了《中华人民共和国个人信息保护法（草案）》作为附件。该草案首次在国内立法层面提出了信息可携权："信息主体有权就其被收集处理的个人信息获得对应的副本，并可以在技术可行时直接要求信息控制者将这些个人信息传输给另一控制者。"不过 2020 年 10 月提请人大常委会审议的《中华人民共和国个人信息保护法（草案）》（一审稿）删去了可携权条款，2021 年 4 月提交的二审稿也未见个人信息可携带权的相关表述。而在二审稿公开征求社会意见后，2021 年 8 月提请人大常委会审议的《中华人民共和国个人信息保护法（草案三次审议稿）》又重新添加了可携带权条款，并最终获得通过。《个人信息保护法》第四十五

条规定，“个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。”由此，个人信息可携带权制度在我国正式确立。

个人信息可携带权的内涵解构

个人信息权利可以分解为国家主权、人格权和财产权三方面的权利。国家主权方面，《网络安全法》和《数据安全法》在多个条款中规定了其它个人信息权利的行使不得对抗国家主权；人格权方面，《民法典》第四编“人格权”下第六章“隐私权和个人信息保护”做了原则性的规定，《个人信息保护法》进行了细化，如个人拥有个人信息的查阅复制权、更正权等多项权利；财产权方面，我国暂时还没有具体的法律法规，但《民法典》第二编“物权”中关于一般私人财产权的相关规定或可参鉴，即个人对私人财产拥有占有、使用、收益和处分的权利。

个人信息可携带权是一种新型复合权利。一方面，个人信息可携带权是个人信息查阅复制权利的延伸，具备人格权的特性；另一方面，更重要的是，通过个人信息可携带权，个人可以要求接收者给予财产上的回报，因而个人信息可携带权也符合财产权的主要特征。

除此之外，个人信息可携带权还是一项主动性权利。《个人信息保护法》中规定的部分个人信息权利属于被动性权利（如更正权等），只有当相关权利被侵犯时，个人才有权要求相应的救济。而个人信息可携带权的行使并不以该权利被侵犯为先决条件，是一项主动性权利。

个人信息可携带权同时具备主动性及财产权的特性意味着，个人可以主动发起个人信息流转，并从中获益，这就解决了个人信息流转中责任主体和利益主体不一致的问题，为解决个人信息流转难的问题提供了难得的新机遇。

《个人信息保护法》将此项权利赋予个人，也充分体现了将个人权利还于个人的立法初衷。

03

应用雏形：全球个人信息可携带权的实践初探

个人信息可携带权的立法为个人信息的主动流转提供了法律支持。而从全球实践来看，这项权利得到了较为初步的应用。其在境外具体可归纳成由平台主导和政府主导的两类实践模式。

平台主导的个人信息携带模式：美国企业 DTP 项目

这类模式的典型应用代表是 Google 等美国企业发起的 DTP（Data Transfer Project）项目。在 CCPA 立法后不到一个月，总部位处加州的 Google、Facebook、Microsoft、Twitter 四大互联网企业联合发起了该项目，目的是为用户创造一个在不同服务商之间传输数据的平台。

DTP 的参与公司通过 API 技术共同建立一类数据传输标准，当用户需要执行可携带权时，只需要进行授权操作，信息提供者就可以直接通过 API 接口把个人信息传输给接收者，这就解决了个人执行可携带权时授权复杂、操作不便等问题。

在技术上，DTP 的参与者需要部署 DTP 系统，该系统由三个组件构成：数据模型（Data Model）、适配器（Adapter）和任务管理库（Task Management Library）。

数据模型构建了传输文件类型和元数据的标准，适用于少量类型已经被充分定义的且被广泛采用的标准数据，如图片、音乐、邮件、联系人数据。所有参与 DTP 的公司都必须采用 DTP 系统的数据模型，以方便个人信息传输。

适配器分为数据适配器和身份认证适配器，前者用于 API 和数据模型之间的格式转换，后者则用于用户身份认证。

任务管理库用于处理后台任务，包括数据存储、任务调用、故障处理等。任务管理库通过一个通用的云接口进行部署，因而可以部署在本地、云端或生产环境中。DTP 系统所传输的数据也是先通过任务管理库加密后再进行传输，即 DTP 系统使用了加密 API 传输技术。

数据提供者和数据接收者均可以选择将 DTP 系统部署在自有或第三方的服务器（本地或云端服务器均可）上，按照不同的部署模式组合个人数据传输会经由不同的服务器路径。DTP 的主要参与者均选择将 DTP 系统部署在自有服务器，因而大部分情况下个人数据传输并不会经由第三方，而是从数据提供者直接传输到数据接收者。

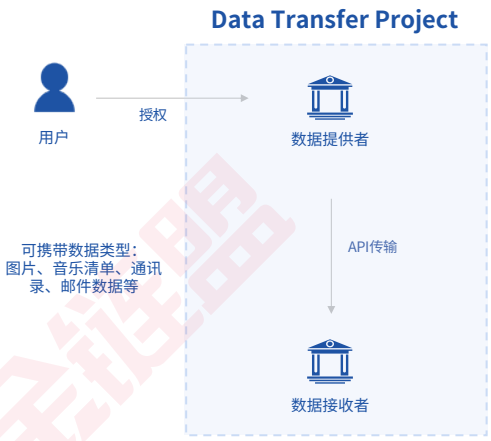


图 5 DTP 模式示意图

目前，DTP 的参与者除了互联网巨头 Google、Microsoft、Apple、Twitter 和 Facebook 外，还有数十家图片音乐网站及云存储服务商，如 Flickr、SmugMug、500px 等，包括了美国用户存储图片、视频和音乐的主要渠道。

DTP 模式主要的优点是简化了相关操作，个人信息流转快速，便于进行数据协作，此外，个人信息数据存储在参与公司的服务器上，技术安全性较高。

DTP 模式也存在不少局限性。在 DTP 模式中，用户无法选择个人信息的存储位置，一旦个人信息携带过程出现问题也难以追责。个人信息携带过程中，可携带的信息还必须满足提供和接收者都能处理这一前提条件，因此只能在有限的公司之间传输重合程度高、较为标准化的数据，例如图片、音乐清单、邮件数据。DTP 模式的个人信息携带需要基于平台已整合完成的互联网基础服务进行，因此参与方主要为几大互联网巨头，难以覆盖更多中小参与者，也无法实现跨场景、跨行业应用。如何拓展更多的数据可携带领域，吸纳更多的公司参与可能是 DTP 模式当前面临的最大的问题。为了可携带权而建立的 DTP，如果最终仅有少量公司参与，那么实际上阻止了 DTP 内外之间的数据流通，有违设立可携带权的初衷，还会造成新的垄断。DTP 模式的具体优点和局限性见表 2。

表 2 DTP 模式的优缺点比较

	优点	局限性
安全存储	在企业服务器存储，技术安全性高	用户不可自行选择存储位置和方式
可信传输	传输操作简便	• 信任机制完全依赖企业信用 • 透明度低、用户权利保障责任不明确
协同生产	使用统一API标准、便于协作	仅支持联盟内有限机构及场景，难以实现跨行业应用

政府主导的个人信息携带模式：MyData 服务

与 DTP 模式不同，以韩国为典型代表的 MyData 模式由政府主导，思路是政府通过牌照准入的方式，审核、批准 MyData 运营商建立服务平台。当用户请求访问个人信息数据时，信息提供者需要将个人信息传输给 MyData 平台，再统一由 MyData 平台传输给

个人，相当于 MyData 平台整合了各公司的个人信息数据，方便个人访问和携带个人信息。而当个人需要执行可携带权时，只要授权信息接收者从 MyData 平台处获取即可。

目前 MyData 模式已经在韩国落地应用。2021 年 1 月韩国在金融领域开展 MyData 服务试点，医疗、能源等 8 个领域将陆续跟进，并计划在 2021 年 8 月在全国范围内全面推行 MyData 服务。

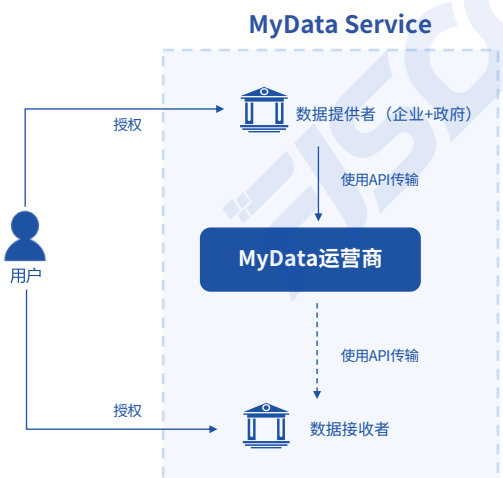


图 6 韩国 MyData 模式示意图

在已经开始的试点中，运营商 PAYCO 与韩亚银行、韩华生命保险、韩华损害保险、韩华投资证券、新韩金融投资、Welcome 储蓄银行等六家机构合作，推出了“PAYCO MyData”服务，用户通过该服务可以享受查询所有合作机构信息的“金融信息一站式查询”服务，自行下载信息的“数据下载”服务，查看个人数据使用者使用明细的“数据查询记录”服务，以及使用合作金融机构推荐产品的“综合金融超市”等服务。

按照规划，MyData 服务全面推进后，金融领域用户可以通过 MyData 服务查询账户信息、存贷款信息、支付信息、保险和投资信息等上百项个人信息。而在此之后，MyData 服务还将提供个人自助数据分析、个人信息携带等进一步功能。

技术上，韩国 MyData 服务大量使用了 API 技术，其所用 API 可以分为三类：认证类 API、信息传输类 API 和支持类 API，分别用于使用者身份认证、个人信息传输和后台数据查询，相关的标准由 MyData 运营商、合作金融机构、MyData 支持机构等多方共同制定，并根据用户和金融机构的需求，不断添加和完善。

截至 2021 年 9 月，韩国共发放 MyData 运营商牌照 45 张，多为金融科技公司、银行、保险公司获得，而根据韩国《金融领域 MyData 服务指南》，信息提供者包括银行、证券、保险公司，几乎覆盖了所有金融机构，不少运营商同时也是数据提供者或数据接收者。

不过截至目前，韩国对于 MyData 服务的试点难称成功。原定于 2021 年 8 月全面推行的时间点被延迟到 12 月，而就当前进度来看，12 月能否如期推行也还不得而知。MyData 服务覆盖的个人信息类型也远不如规划中丰富，韩国用户在 MyData 平台上暂时只能查看个人信息，还不能执行个人信息携带的操作，可查看的个人信息类型也远没有达到规划中的上百项。另一方面，尽管政府已经发放了 45 张牌照，但目前韩国仍仅有 Payco 一家运营商提供 MyData 服务，服务用户数量也不多，相关工作进展并不尽如人意。

和韩国 Mydata 服务思路类似，新加坡政府在 2020 年 12 月推出了名为“新加坡财务数据交换平台”（简称 SGFinDex）的公共数字基础设施项目。SGFinDex 允许新加坡用户使用电子政府密码（SingPass）来授权认证任何参与其中的银行，授权后用户可以在该银行的页面上查看到各家银行不同户头的存款各种贷款、信用卡欠款、公积金存款、组屋贷款和所得税资料等，实现了个人金融数据和政务 / 公共数据的整合查看。SGFinDex 平台上个人可以查看的数据量要少于韩国，但可以进行少量个人基本信息的携带。不过 SGFinDex 的开放银行属性决定了其主要功能是查看个人信息，无法进行大规模的个人信息携带。

同样与 Mydata 思路类似的还有印度。2021 年 9 月印度政府上线了名为萨哈马提（Sahamati）的账户聚合（AA）系统，该系统由 8 家头部银行参与，联通了金融、税务、电信等数据源，用户可以将这些数据分享至持有 AA 许可的金融科技企业以获取信贷、资产管理、财务规划等服务。和 SGFinDex 类似，账户聚合系统本质上提供的也是一类开放银行服务，无法实现更大范围的个人信息携带。

与 DTP 模式相比，MyData 模式加入了政府的

作用，通过牌照准入的方式，以政府信用代替企业信用，提高了用户的信任度，增加了企业的参与度，整合了更多类型的数据。由于数据存储在参与公司和运营商服务器上，MyData 模式还具有数据存储技术安全性高等优点。

但是 MyData 作为一种中心化的模式，受限于垂直行业，无法有效激励数据提供者的积极参与，依然存在跨场景、跨行业协作困难等问题。同时一些 MyData 运营商并不中立，既是服务平台又是个人信息处理者，存在潜在利益冲突，还带来了新的垄断问题。MyData 模式也没有解决用户不可自主选择存储位置的问题，相反，由于增加了 MyData 运营商作为额外的个人信息存储节点，增加了个人信息泄露的风险。

表 3 MyData 模式的优缺点比较

	优点	局限性
安全存储	牌照准入、技术安全性高	• 多方存储增加了风险 • 用户不可选择存储位置
可信传输	• 基于统一API可查看行业内结构化数据 • 机构持牌参与，可信性强	-
协同生产	可覆盖本行业内主要机构	• 按场景切分，难以形成跨行业协作 • 数据运营商不中立，潜在利益冲突，容易形成新的垄断

现存实践模式的局限性

如上所述，传统主流的 B2B 直接传输模式，在没有公共机构的约束及用户自主发起的情况下，数据主体的个人意志将很容易被裹挟。而基于个人数据可携带权的现有模式在部分解决个人信息携带的同时，各有局限性。DTP 和 MyData 模式更多是平台或政府主导推动，均没有充分发挥用户在其中的作用。

从安全存储、可信传输和协同生产三方面来看，现有模式存在以下问题：

安全存储方面，用户缺少个人信息存储的选择权，个人信息存储也没有遵循最小必要原则。DTP 模式下用户只能选择将个人信息存在某个处理者的服务器上，My Data 模式下用户也只能选择存储在数据运营商，而不能自行指定存储位置，限制了用户可携带权的范围，而运营商作为第三方，只需要提供传输方案就已经足够，完全不需要存储用户数据，不必要的多副本存储提高了数据泄露风险；

可信传输方面，个人信息真实性难以有效验证，用户权利保障的方式不明确，也缺乏信任机制。当前三种模式中，个人信息接收者只能被动接收从提供者或平台传输来的个人信息，无法验证真伪，从而导致携带而来的个人信息可靠性大大降低。如果用户个人信息携带的过程中出现问题，很难判断是提供方还是接收方的责任，又或者是 API 传输协议出现了问题，用户也很难就此进行追责。此外，DTP 模式由企业自发组织，是企业为了履行法律规定而设，会更多考虑企业本身利益而非用户利益，MyData 模式中一些数据运营商本身就是数据处理者，用户很难相信其不会为自己谋利，传统主流的 B2B 直接传输模式也是由企业发起而非用户主动提出，这就导致了数据携带过程中的信任机制缺失，用户参与程度不高；

协同生产方面，用户可携带数据的类型有限，现有模式也容易造成新的垄断。DTP 模式中，只有用户在使用各种服务过程中上传的图片、音乐清单、邮件数据才可以携带，而在韩国

MyData 模式中，尽管用户可以查看上百条信息，但暂时并不能携带个人信息，也难以实现跨行业跨场景协作。更重要的是，现有个人信息携带模式都以参与企业组建联盟为前提，联盟内部的个人信息携带较为便利，而联盟内外之间的个人信息携带阻力反而变大，容易造成新的垄断。

归根结底，个人信息可携带权的全球实践表明，如果不能解决来自安全存储、可信传输、协同生产三方面的挑战，就无法有效发挥个人信息可携带权的作用。

04

个人信息可携带权的中国路径倡议

基于数据新基建的解决思路

现有个人信息可携带权的实践模式所面临的挑战，本质上仍与数据要素安全存储、可信传输、协同生产这三大核心命题息息相关。因此，要实现更完善的个人信息可携带应用，仍可从这三方面着手寻求解决方案。

· **安全存储方面，**需要给予用户选择如何存储的权利。现有模式以市场机构或政府为主导者，用户的选择权利被忽视，这与个人信息可携带权主动性的特性不符，也就难以发挥个人信息可携带权的作用。为此需要用户较深入地参与到整个个人信息携带的过程当中，充分发挥用户在行使个人信息可携带权时的主动性，减少过度授权、强制授权等情况的发生，减少数据泄露等方面的风险；

· **可信传输方面，**需要解决个人信息验真、个人权利保障和信任机制问题。个人信息可携带的前提是携带信息真实可靠、权利保障机制完善、信任机制健全，可以利用技术工具，建立个人信息验真机制、用户权利保护机制以及个人信息传输中的信任机制，满足跨机构身份认证、数据溯源和可信数据流通的需求。

· **协同生产方面，**需要解决个人信息在跨行业多场景情况下的协作问题。对于接收者来说，理想的个人信息可携带权模式应当具有跨行业、跨场景、广泛适用的数据传输标准，且该标准应当具有良好的可扩展性，以便新的加入者能够很容易地参与其中，从而满足大范围数据协作的需要。

探索与启发：粤澳健康码互认项目

如何有效解决上述个人信息携带权落地应用中的安全存储、可信传输、协同生产问题，区块链技术作为新基建信息基础设施有望发挥特殊作用。

2020 年 5 月，广东和澳门两地政府部门运用基于区块链技术，推出的粤澳健康码跨境互认项目，为构建个人信息可携带权模式提供了参考。众所周知，新冠疫情造成了人员流动不便问题，如何实现健康码跨地互认互转存在较多的困难。尤其是，在跨境场景下居民的个人隐私信息限于当前法律难以实现跨境传输，如何进行用户健康信息的真实互认就变得十分困难。在 FISCO BCOS 区块链开源底层平台的技术支持下，广东和澳门两地政府部门运用基于区块链的实体身份标识及可验证数字凭证技术，推出了粤澳健康码跨境互认项目，助力两地居民正常跨境通关。

该项目的思路是让用户成为个人信息传输的核心角色，自主携带申报个人健康信息，通过数据指纹上链，实现数据验证及健康码互认互换。在经过用户同意授权之后，所在地区的政府部门开始启动健康数据转码；在后端，个人健康数据文件的哈希值和用户的数字签名将记录在区块链上，数据原文信息则仍保存在健康码发行机构的本地数据库中；在前端，用户无需在多个平台重复填写复杂信息，只需简单授权后，产品将自动为用户转为前往地区的健康码，从而实现了合规前提下的个人健康信息的跨境携带。截至 2021 年 6 月，项目已服务超 9500 万人次在粤澳两地跨境通行。

图 7 粤澳健康码互认系统前端界面

个人主导的个人信息携带模式：分布式数据传输协议（DDTP）

受粤澳健康码互认项目的启迪，本白皮书提出一种新型的分布式数据传输协议（Distributed Data Transfer Protocol，DDTP）。该协议旨在让用户成为关键参与者，由用户主动发起个人信息数据传输并自行上传，从而实践个人数据可携带权。协议方案基于区块链技术，通过区块链的全流程追溯、防篡改、传递信任等特性，叠加引进权威机构的参与，助力更安全、可信、易协作的个人信息携带应用。与其他模式不同的是，该协议强调以用户个人为主导，遵循分布式理念，不依赖于数据提供者和接收者双方合作，也不依赖中心化机构推动，可支持跨机构、跨行业、跨场景协同。

如下图所示，主要分两个主要步骤行使个人信息可携带权。第一步是用户从数据提供者处下载

个人信息数据，并存储在个人指定的位置。存储位置可以是本地，也可以是云或其它位置。为了确保个人真实意愿、防止真实数据被篡改、保持传输给接收者的个人信息与提供者提供的个人信息一致，经用户授权后，可进一步引入权威中立的第三方机构参与见证该个人数据文件的存储过程，并获取相关文件的哈希值（而非源文件）作为“数据指纹”存储于区块链上。

第二步是用户将已下载的个人信息数据传输给数据接收者，并对使用范围和使用目的等进行授权。数据接收者在收到个人信息数据文件之后，可以通过区块链进行基于哈希值的可验证数字凭证——“数据指纹”的核验，从而完成验真的过程。与此同时，个人的所有授权记录、数据接收者的具体使用情况也皆可在链上进行记录，便于个人未来追溯相关文件的流转。

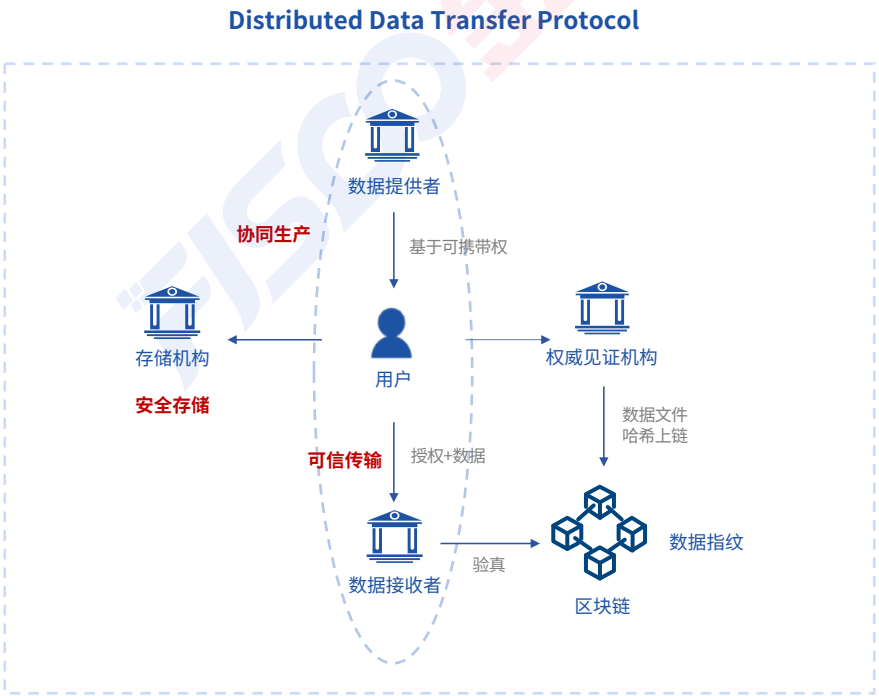


图 8 分布式数据传输协议（DDTP）示意图

该协议可以满足相关各方关于个人信息可携带权的基本需求。在安全存储、可信传输、协同生产三方面，具有明显的优点：

从应用效果来看，通过引入用户作为核心参与者，DDTP 建立了用户主动行使个人信息可携带权的模式，由于是用户直接向接收者传输数据，按照《个人信息保护法》相关条款，接收者不能索取不必要的数据，因此也不会出现过度授权和信息滥用，成功保障了用户行使个人信息可携带权；通过使用区块链技术，DDTP 将个人信息存储、传输和验证分离，成功解决了验真、溯源、审计、信任机制传递等方面的问题；而用户自主发起并结合基于哈希值的可验证数字凭证——“数据指纹”上链验证的方式，既符合政策的合规要求，又能解决跨机构、跨行业、跨场景数据协同生产的问题，可以用于个人信息可携带权的中国实践。

表 4 DDTP 协议的优点

	优点
安全存储	• 用户自行发起传输，可选择存储位置 • 存储和验证分离，避免数据的不必要复制，安全性高
可信传输	• 利用区块链不可篡改性实现数据验证 • 用户授权记录上链，可溯源、可审计
协同生产	• 用户自主发起，可支持跨机构、跨行业、跨场景协同 • 同样适用跨境协作场景

未来展望：更广泛的跨行业、跨场景分布式数据传输设施

值得一提的是，DDTP 协议运作模式在前期可能是分散运作的，不同机构或将采用不同的区块链生态网络来构建细分行业或领域的个人信息携带应用。而展望未来，基于公众联盟链理念的区块链跨链技术，可以将所有分散的细分领域应用平台链接起来，构建更广泛的分布式数据传输、核验和协作的新生态。届时，数据接收者只需要在任意应用平台中一点接入，就可以在接收个人自主上传数据的同时验证所有来源的个人信息数据。

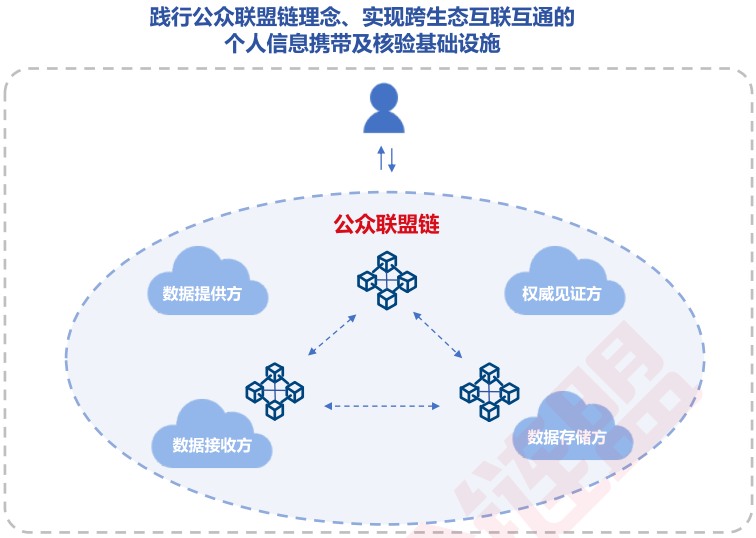


图 9 践行公众联盟链理念的分布式数据传输设施示意图

综上所述，对于用户而言，整个过程中均由用户主动发起，充分保障了用户在行使个人信息可携带权过程中的主动权，个人携带的信息种类和携带形式也不受限制，用户可以通过 API、邮件、H5 等多种形式发起、携带多种个人信息。

用户执行可携带权时，可以仅授权接收者下载数据并验证，相比直接的“提供者—用户—接收者”模式，不需要每次执行可携带权都向提供者提出申请，从而优化了用户体验。

而对于信息接收者来说，只要在任意核验平台单点接入，就可以在获得用户授权的基础上，进行个人信息核验，而不必一一处理来自分散数据源的数据，大大简化了数据处理的过程。

据此，DDTP 协议既体现了个人在整个过程中的核心作用，实现了个人信息可携带权将个人信息价值还于个人的愿景，又为数据使用者节省了处理数据成本，可以激发相关各方参与的积极性，从而能够解决个人信息流转的难题。相信 DDTP 协议未来会在实践个人信息可携带权、解放数据生产力方面发挥重要作用。

关于我们

金链盟

金链盟成立于 2016 年 5 月，由微众银行、腾讯、前海金控、深证通、顺丰控股等二十余家金融机构和科技企业共同发起，2019 年 11 月正式注册为社会团体法人。至今，金链盟成员已涵括银行、证券、基金、保险、地方股权交易所、科技公司等六大类行业的 150 余家单位，已是国内最大的区块链组织和最具国际影响力的区块链联盟之一。

金链盟下设的金链盟开源工作组于 2017 年推出了安全可控、稳定易用、高性能的金融级区块链底层平台 FISCO BCOS。该平台获得了 2018 年度深圳金融科技创新专项奖一等奖，并于 2019 年入选成为国家级区块链服务网络（BSN）中的首个国产联盟链底层平台。目前，FISCO BCOS 开源生态圈已汇聚了超 4 万名个人开发者、超 2000 家机构与企业，在政务、金融、公益、版权、供应链、教育等不同领域已有 120 余个落地应用，已发展成为最大最活跃的国产开源联盟链生态圈。

观韬中茂律师事务所

观韬中茂律师事务所成立于 1994 年 2 月，是总部设于中国北京的专业化、综合性大型律师事务所。经过与创设于上世纪五十年代的香港王泽长 · 周淑娴 · 周永健律师行，以及创建于上世纪九十年代的上海市中茂律师事务所、上海市申达律师事务所的合并，观韬中茂现拥有 800 余名律师、200 余位合伙人，在法律服务、专业建设和律师团队等方面已成为中国优秀律师事务所之一。

王渝伟律师数据合规团队是观韬中茂律师事务所专注网络安全、数据隐私合规法律服务的专业团队，在大数据、人工智能、互联网、金融科技、云计算、物联网等领域拥有为头部企业提供涉及复杂技术与商业场景项目提供全面数据合规服务的丰富经验和卓越能力。

金融科技·微洞察

“金融科技 · 微洞察”是微众银行运营的金融科技研究品牌，聚焦国内外金融科技领域的技术发展、标准制定及产业应用，把握当下金融科技热点话题与政策动向，洞察未来领先的金融形态和商业模式。

微众银行作为国内首家互联网银行，自 2014 年成立之初即将“科技、普惠、连接”作为银行的三大发展愿景，将积极运用科技创新探索普惠金融新模式、新业态作为银行重要的发展方向，致力于为普罗大众、微小企业提供差异化、有特色、优质便捷的金融服务。自立行至今，微众银行在金融科技“ABCD”（人工智能、区块链、云计算、大数据）等四大领域积极探索，2017 年即已成为国内首家获评“国家级高新技术企业”的商业银行，截至 2020 年末共申请国家及国际专利数超过 2300 余件，拥有自身所有重要业务和技术系统的知识产权，有效实现了银行业信息化安全可控的战略目标。

免责声明

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，本报告所载的资料、工具、意见及推测只作参考之用，并非作为或被视为出售或购买证券或其他投资标的邀请或向人作出邀请。在任何情况下，报告的编著机构不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然我们已致力提供准确和及时的资料，但我们不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

FISCO 金链盟

金融科技 · 微洞察