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

基于区块链技术的数据协作网络金融应用研究

The Research Report on Financial Industry Application of Data Collaboration Network Based on Blockchain Technology

北京金融科技产业联盟

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

版权声明

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

编制委员会

主任：

潘润红

编委会成员：

聂丽琴 彭 晋

编写组成员：

胡达川 王 硕 昌文婷 魏长征 余逸荣 张晓蒙 王 暄
李辉忠 王朝阳 景梦园 邓小珊 陈林燏 王绍刚 肖 凯
祝轶群 杨桐权 帅斌成 陈 凯 高文俊 杨玉冰 王子健
田一鸣 王欣明 王晴晴 李克鹏 刘 江 杨文锋 姜 涛
黄步添 罗春凤

参编单位:

北京金融科技产业联盟

蚂蚁科技集团股份有限公司

中钞信用卡产业发展有限公司杭州区块链技术研究院

深圳前海微众银行股份有限公司

招商银行股份有限公司

杭州溪塔科技有限公司

工银科技有限公司

交通银行股份有限公司

上海浦东发展银行股份有限公司

中国光大银行股份有限公司

北京银行股份有限公司

拉卡拉支付股份有限公司

腾讯云计算（北京）有限责任公司

神州数码信息服务股份有限公司

杭州云象网络技术有限公司

摘 要

数据作为数字经济的核心生产要素，在我国推进数字化转型、实现高质量发展过程中发挥着重要战略性作用。开展数据协作有助于金融业构筑多维网络，形成动态、立体、多维度的大数据体系，充分挖掘数据潜力，以安全可信的技术手段筑牢数据协作基石。但是，当前金融业开展数据协作仍面临数据产权不清晰、要素定价复杂、要素价值易稀释、数据孤岛、用户自主权不可控等痛点。因此，本文提出基于数据全生命周期流程的数据协作模型及整体系统架构、参与角色、业务流程、功能、安全要求、网络形态等参考实现，具备数字身份安全可信、用户数据自主可控、数据目录多方共享等特点，最后通过典型数据协作实践案例，为金融业进一步数据协作场景应用提供借鉴。

目 录

一、 背景研究

1.1 政策与标准

政策层面。数据作为数字经济的核心生产要素，在我国推进数字化转型、实现高质量发展过程中发挥着重要战略性作用。2020 年以来我国陆续出台相关政策，促进数据要素市场发展。

表 1 数据要素相关政策

时间（基于政府网站发布信息）	**发布主体**（基于政府网站发布信息）	**政策名称**	**主要内容**（基于政策原文整理）
2020 年 4 月	中共中央 国务院	《关于构建更加完善的要素市场化配置体制机制的意见》	数据成为继土地、劳动力、资本、技术后的第五大生产要素，明确了数据要素的经济主体地位。
2020 年 5 月	中共中央国务院	《关于新时代加快完善社会主义市场经济体制的意见》	加快培育发展数据要素市场，建立数据资源清单管理机制，完善数据权属界定、开放共享、交易流通等标准和措施，发挥社会数据资源价值。
2022 年 1 月	国务院	《“十四五”数字经济发展规划》	数据要素是数字经济深化发展的核心引擎。到 2025 年，数据要素市场体系初步建立。
2021 年 12 月	国务院办公厅	《要素市场化配置综合改革试点总体方案》	探索建立数据要素流通规则。完善公共数据开放共享机制，建立健全数据流通交易规则，拓展规范化数据开发利用场景，加强数据安全保护。
2022 年 3 月	中共中央 国务院	《关于加快建设全国统一大市场》	加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。
2022 年 6 月	中央深改委	《关于构建数据基础制度更好发挥数据要素作用的意见》	要建立数据产权制度，推进公共数据、企业数据、个人数据分类分级确权授权使用，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行

			机制，健全数据要素权益保护制度。

标准层面。为建立完善有序的数据市场规则，提升数据流转效率及安全性、可控性，近年来我国陆续发布了一系列数据分类分级、数据安全和数据交易等方面的国家标准和行业标准。

表 2 数据相关标准

领域	类别	编号	名称	主要内容
数据分类分级	国家标准	GB/T 38667—2020	《信息技术 大数据 数据分类指南》	大数据分类过程及其分类视角、分类维度和分类方法等。
	行业标准	JR/T 0158-2018	《证券期货业数据分类分级指引》	该标准给出证券期货业数据分类分级方法概述及数据分类分级方法的具体描述，并就数据分类分级中的关键问题处理给出建议。
	行业标准	JR/T 0197—2020	《金融数据安全 数据安全分级指南》	金融数据安全分级的目标、原则和范围，以及数据安全顶级的要素、规则和定级过程。
	行业标准	JR/T 0171—2020	《个人金融信息保护技术规范》	该标准规定了个人金融信息在收集、传输、存储等全生命周期各环节的安全防护要求。
数据安全类	国家标准	GB/T 37988-2019	《信息安全技术 数据安全能力成熟度模型》	从数据全生命周期安全和通用安全两部分，将数据安全能力成熟度分为 5 级，给出了 10 项通用安全要求和 6 项数据生命周期安全要求。
	国家标准	GB/T 37932-2019	《信息安全技术 数据交易服务安全要求》	该标准规定了通过数据交易服务机构进行数据交易服务的安全要求。
	行业标准	JR/T 0223—2021	《金融数据安全 数据生命周期安全规范》	规定了金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架。
数据交易	国家标准	GB/T 37728-2019	《信息技术 数据交易服务平台 通用功能要求》	规范了数据交易服务平台的功能框架，以及用户管理、平台交易、平台管理、开发测试环境和基础技术支撑五个方面的基本功能和扩展功能。
	国家标准	GB/T 36343-2018	《信息技术 数据交易服务平台 交易数据描述》	规定了数据交易服务平台中交易数据描述的相关信息及这些信息的描述方法，交易数据描述信息包括必选信息和可选信息两部分。

1.2 金融业数据协作的必要性

1.2.1 多维网络释放数据价值

金融服务涉及的社会分工环节单一，没有形成网状结构，无法真实体现社会分工关系，且单一环节的数据造假成本低，真实性大打折扣，无法有效释放金融数据实际价值。只有将分散在社会化分工各处的数据联合起来，形成动态、立体、多维度的大数据网络，才能发挥数据的最高价值。

1.2.2 协同开发挖掘数据潜力

大数据本身具有非均质、价值密度低等特性，因此需要多方共同参与投入资金、时间、人力等资源，协同挖掘数据潜力，进行数据价值的提取、加工及分析，建立丰富的数据价值社会化的分工模式，打造“原始数据-粗加工数据-精加工数据产品-融合专家经验的数据服务"的多层次数据价值流通体系，以协同开发挖掘数据潜在价值。

1.2.3 安全可信共筑协作基石

在传统的中心化模式下，多方的数据汇集到一个中心节点开展计算与应用，容易带来权责混乱、单方风险过高等问题，同时中心节点机构需要承担数据安全责任与数据泄漏风险。因此需要建立多方参与并共识的数据协作机制，多方之间以平等的身份进行协作，并确保协作前数据源的合规性、真实性，在数据协作中做到数据用途用量的严格管控，在数据协作后实现数据开放协作过程的可查、可证和可溯源，充分实现数据使用过程的审计，建立端到端的可信协作机制和安全流

通渠道。

1.3 金融业数据协作的痛点

1.3.1 产权机制不清晰

与传统的资产不同，数据资产往往不具备固定的形态，数据本身具有较强的流动性和时效性，容易被复制和转让，使用者可以在数据使用过程中将数据存储下来，从而在未来加以再次利用和转让，进而可能引发企业间无序竞争、企业和用户间基于所有权认知差异而产生的纠纷。因此在数据协作过程中，存在数据产权不清晰、产权认知存在差异、产权易丢失等痛点。在数据使用过程中，保护数据的所有权不丢失，保持数据资产标识与数据权属所有者之间唯一确定的关联关系，对于数据协作的应用而言是一个较大的挑战。

1.3.2 要素定价复杂度高

数据要素定价面临定价模型复杂以及数据要素价值易稀释的痛点。一是数据要素定价模型复杂。金融业数据协作面临着复杂的应用场景，包括数据查询、数据分析、机器学习等。在数据使用过程中将产生大量的分割数据、中间数据和最终结果数据，对不同粒度、不同环节的数据资产定价和价值评价是当前面临的一大挑战。二是数据要素价值易稀释。数据使用率越高证明数据应用价值越高，在传统模式下，数据复制性强的特点使原始数据转化过程中价值稀释显著。高效的数据协作需要保障在不交换原数据的前提下输出数据蕴含的知识，如何使数据资产价值以市场化的方式计量，并保障数据资产权属利益，

是另一大挑战。

1.3.3 数据孤岛普遍存在

目前，不同金融业机构之间或者同一机构不同部门之间，存在数据无法连接互动情况，易形成数据孤岛。一方面金融机构无法有效获得工商、税务、征信、经营等数据。如企业注册信息需要从工商部门获得；企业纳税信息，需要从税务部门获取；企业征信信息，需要从三方征信公司获取；企业经营信息（如进销存、销售数据）存在于和上下游关联的相关企业及各电商平台，甚至物流系统中。另一方面机构在信息化建设中投入建设的各业务管理系统独立运行，分属不同部门。内部实现真正的数据共享需要做到高效系统集成。数据孤岛问题严重影响金融服务的数字化转型进程。如何打破壁垒，实现数据权益与数据提供者的安全、高效科学匹配，是一大挑战。

1.3.4 数据监管需进一步完善

金融业存在数据要素跨地区、跨行业、跨层级流通的监管需求。有效的监管体系是数据要素协作市场得以运行的基本前提。近年来，随着我国金融市场日益发展壮大，金融业逐步形成数据要素市场的统一规范化管理机制。但是，由于数据协作在权属流转层面的情况复杂，因此需要在数据协作过程中进一步加强个人隐私保护和财产权交易等方面的监管。

二、 模型分析

数据协作的过程可以分为三个阶段，分别是数据协作前制定开放

策略达成协作共识、协作中开展数据流转计算以及协作后配合监管审计。

图 1 数据协作阶段示意

2.1 数据协作前

金融机构进行数据开放以及多个数据拥有方之间进行数据协作之前需要解决数据资源采集、确权等问题。

2.1.1 数据采集

数据采集是指金融机构在提供金融产品和服务、开展经营管理等活动中，直接或间接从个人金融信息主体，以及企业客户、外部数据供应方等外部机构获取数据的过程[1]。数据采集过程包括采集与提取、转换与标准化、信息上传等步骤。机构进行数据协作之前，可通过区块链记录数据源的合规性和真实性，确保获得采集数据的主体授权，明确数据采集范围、频率、类型与用途等。

2.1.2 数据协作策略

为了保障数据安全，在数据开放前，需要对数据进行分类分级、敏感词识别、风险监测等，便于数据使用方进行精细化的安全策略定制。使用区块链不仅可以不可篡改地记录安全策略，而且多方共识网

[1] 参考资料：T 0223—2021《金融数据安全 数据生命周期安全规范》关于数据采集的定义。

络可以高效、真实地将协作策略同步给数据协作网络中的其它参与方。

2.1.3 数据传输和存储

数据传输是指机构将数据从一个实体发送到另一个实体的过程，存在数据传输中断、篡改、伪造及窃取等安全风险[2]。利用区块链可以记录源数据的指纹或哈希值，用于接收方核验数据的真实性和完整性。

数据存储是指金融业机构在提供金融产品和服务、开展经营管理等活动中，将数据进行持久化保存的过程[3]。存储需根据数据安全等级灵活使用加密技术与权限控制确保数据的完整性和安全性。利用智能合约可以实现数据的访问控制权限管理，避免管理人员等内部攻击造成数据泄露。

2.1.4 数据确权

数据要素确权是为了明确各个协作参与方的权利及义务，是整个流转得以有序有据、合法合规的基础。中共中央国务院《关于构建数据基础制度 更好发挥数据要素作用的意见》提出了数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制。数据资源持有权体现了对数据资源持有者的权益保护，既是对数据控制事实状态的确权承认，也反映了促进国家数据资源登记汇总和强化数据分类分级保护的公共利益。数据加工使用权是包含加工权、使用权的复合权益。数据产品经营权是包含收益权、经营权的复合权益。

借助区块链的数字身份和智能合约特性，首先可以将这些权属关

[2] 参考资料：0223—2021《金融数据安全 数据生命周期安全规范》关于数据传输的定义。
[3] 参考资料：0223—2021《金融数据安全 数据生命周期安全规范》关于数据存储的定义。

系使用智能合约的程序化语言定义，接受各方的查验和审计。随后，在智能合约中将数据要素生命周期节点与权属进行关联，实现链上管控。最后，各方使用自己的区块链数字身份签名在链上登记注册，实现身份-权属-数据要素的确认，开展数据协作。

2.2 数据协作中

数据协作中的阶段主要包含数据要素全生命周期中数据的使用过程，包括数据访问、共享、加工、托管、聚合等常见操作。

2.2.1 数据访问

数据访问是指金融机构内外部各类主体对数据进行查询和变更的过程[4]。在数据要素流通的过程中，为保证数据的隐私性和安全性，数据可能会存储在多个参与主体中，对外以数据目录的方式进行展示，访问方可通过数据目录存储的内容了解数据的基本信息，在数据所有方授权之后即可通过数据目录访问数据。在数据协作网络中，因参与主体众多、链路复杂，如何设计安全灵活的权限控制体系，做好数据授权和鉴权工作，确保数据访问的安全可控是数据使用过程的核心。

各参与方将数据资源描述提交至区块链，可形成数据目录链。该数据目录链可视化的展示了流通中的数据资源，各参与方可对流通数据进行检索查询，提供流通数据的各项指标统计。数据目录链以数据所有者为核心制定数据开放策略，数据目录同步上链，原始数据哈希上链，在链上保留摘要信息不可篡改，各协作节点可查可申请。

[4] 参考资料：JR/T 0223—2021《金融数据安全 数据生命周期安全规范》关于数据访问的定义。

2.2.2 数据共享

数据共享指在满足数据隐私安全条件下，数据主体方在不同机构、不同参与方之间进行数据分享[5]。数据托管是指金融业机构因金融产品或服务的需要，在不改变相关权利和义务的前提下，将数据托管给第三方机构进行处理，并获取处理结果的过程[6]。数据加工聚合是指金融机构基于市场分析、业务优化、风险管控等需求，对数据进行清洗、转换、分析、挖掘等操作。

在数据协作网络中，根据不同的场景设定，会对数据进行共享、托管和加工聚合等不同的操作，实现按需操作，加快数据的流通。在此过程中，需要灵活、安全的数据协作机制，连通数据存储方与数据加工方、隐私安全分析方、数据使用方等第三方机构，在数据多方协作过程中提高从数据资源到数据资产再到数据价值的转化率。

区块链可以链接隐私计算、数据安全等技术，使用智能合约编排、调度，按照数据的安全等级和协作策略等调度不同的算子，实现从数据分类分级导入、发布注册、授权计算到价值流转分配的全链路的可信、可证和隐私安全。

2.2.3 激励分润

数据要素的流通通常伴随资金的交易流动，在这个过程中，我们需要公平、合理、高效地把数据要素产生的价值分配给各个角色，让每一个参与者的投入和产出成正比，激励各方，提升数据要素流通和

[5] 参考资料：JR/T 0223—2021《金融数据安全 数据生命周期安全规范》关于数据共享的定义。
[6] 参考资料：JR/T 0223—2021《金融数据安全 数据生命周期安全规范》关于数据托管的定义。

协作的意愿，形成正向循环。其本质上是对数据收益权的保障和实现。激励分润机制一般是各方在事前约定好数据要素定价、分润比例和结算时间等，但是在实际执行过程中是否按照约定执行是难以监管的，给协作带来障碍。针对这个问题，在业务上，可以将数据交易放在具有权威的地方性或区域性数据交易中心，一定程度上更有保障；在技术上，可以借助区块链或智能合约，将协议约定数字化，实现“一手交钱，一手交货”。

激励分润中一个关键问题是需要对提供数据要素的价值、质量、贡献进行量化评估。数据要素的价值以自评为主，数据的所有方根据行业实践经验及自身成本付出，在市场化的机制下，综合评估价值。数据要素的质量以他评为主，在数据协作的过程中，各参与方可使用自身数据对其他参与方的数据进行评估，如评估预测准确率、数据交叉验证等。数据要素的贡献度则需要参与协作的各方共同评估，按照生态重要度、技术和业务投入、数量质量等综合确定。在整个数据要素评估过程中，区块链智能合约全程记录，并可基于相关数值做权重、平均分等计算，以实现可信的数据交叉评估的公平聚合，用于最终的激励分润。

2.3 数据协作后

2.3.1 数据删除

数据删除指在金融产品和服务涉及的系统及设备中去除数据，使

其保持不可被检索、访问的状态[7]。在数据协作网络中，数据删除操作需要确保留痕可追溯，并实时同步给数据协作网络的相应参与方。

在数据开放协作后，针对数据使用的审计也尤为重要，结合区块链技术，相关的数据使用记录可全流程记录于区块链，相关记录不可篡改，实现数据开放协作过程的可查、可证和可溯源，充分实现数据使用过程的审计。

2.3.2 监管审计

2021 年 11 月 14 日国家互联网信息办公室发布《网络数据安全条例（征求意见稿）》，规定了数据处理者的自主审计和强制外部审计义务，其中强制外部审计一方面可以利用外部独立机构的专业知识和能力，帮助数据处理者更客观、全面地发现、识别合规问题，加强数据协作；另一方面外部审计机构的审计结果也可以为监管机构开展进一步的执法活动提供依据。

技术上，现阶段数据标签与数据分析等大数据技术已经在审计中广泛使用，而作为强化数据协作的基础设施，区块链多方参与、多方共识、共享账本的特性大大提高了审计与监管机构接入的灵活性，同时区块链技术的可追溯性也让审计工作变得更加高效。

三、 参考实现

3.1 系统架构

区块链用于形成数据协作网络中的信任网，用于对数据协作计算

[7] 参考资料：JR/T 0223—2021《金融数据安全 数据生命周期安全规范》。

中的关键数据（如参与者身份、计算输入、关键中间结果、输出）进行存证审计，以实现计算参与者与计算任务的互信互认。区块链节点既可以由协作计算的参与者分别部署，也可由各参与方信任的权威机构部署。

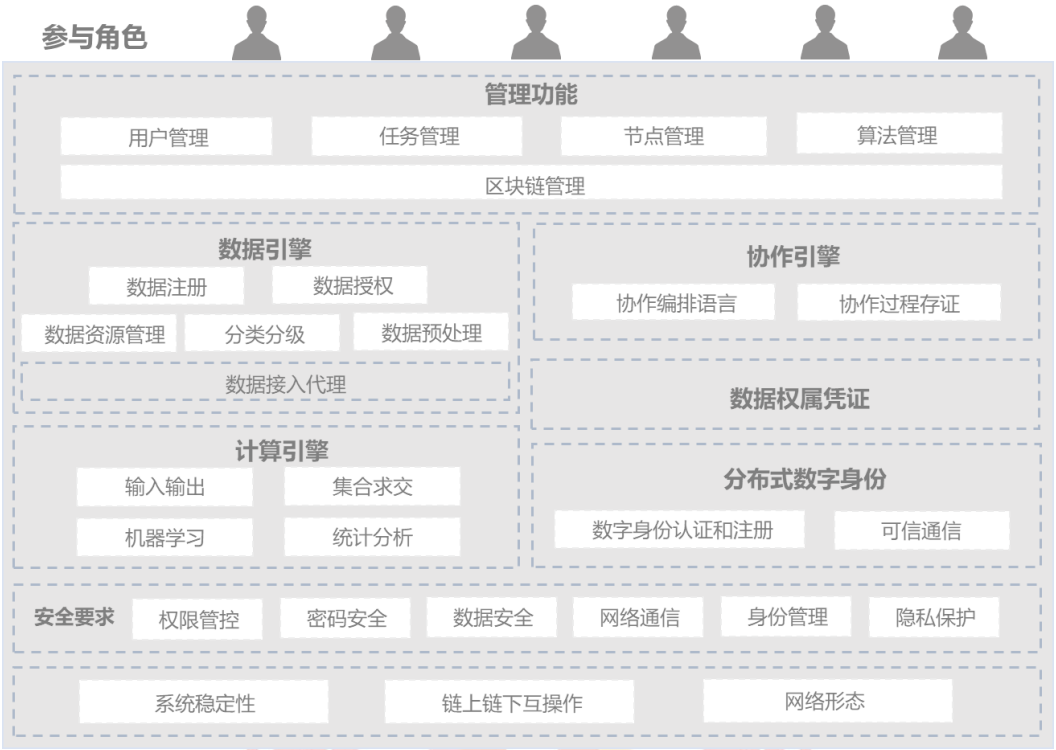

图 2 基于区块链的数据协作系统架构

3.2 参与角色

根据数据协作计算的资源提供、任务调度、任务执行、存证审计等过程，参与数据协作计算的角色主要有以下几类。

（1）平台运营方

平台运营方负责在代理计算模式下实现非隐私数据的维护和同步、计算任务的协调，包括存证信息的同步、参与方的权限管理、数据协作计算任务的推送、计算结果的转发等。计算平台运营方可以接入任意多个算力方、计算源方（包括数据提供方、算法方）与数据使

用方。

（2）算力方

算力方需在平台运营方注册，提供数据协作计算节点参与计算任务。

（3）数据提供方

数据提供方是数据协作计算所需数据的持有者，需在平台运营方注册，负责向各算力方安全地分发计算数据，即数据提供方需将自身的明文数据在本地转化为隐私计算数据后分发至各算力方。

（4）算法方

算法方是数据协作计算所需算法的持有者，需在平台运营方注册，并将算法上传至平台运营方。此处的数据协作计算算法指匿踪查询算法、报表交叉统计算法、联合建模算法、联合预测算法、自定义数据协作计算算法等。

（5）数据使用方

数据使用方需在平台运营方注册，负责提交数据协作计算任务、获得数据协作计算结果。

（6）审计方

审计方可基于区块链实现存证审计，区块链节点既可由上述角色的参与方参与部署，也可由外部多个权威机构部署。

3.3 业务流程

3.3.1 数据确权流程

由于确权流程在各个数据要素生命周期节点基本一致，如下图所示，主要包含获取身份、准备信息、发起申请、确认权利、行使权利五个步骤。下面以数据要素使用权为例，论述典型的确权过程。

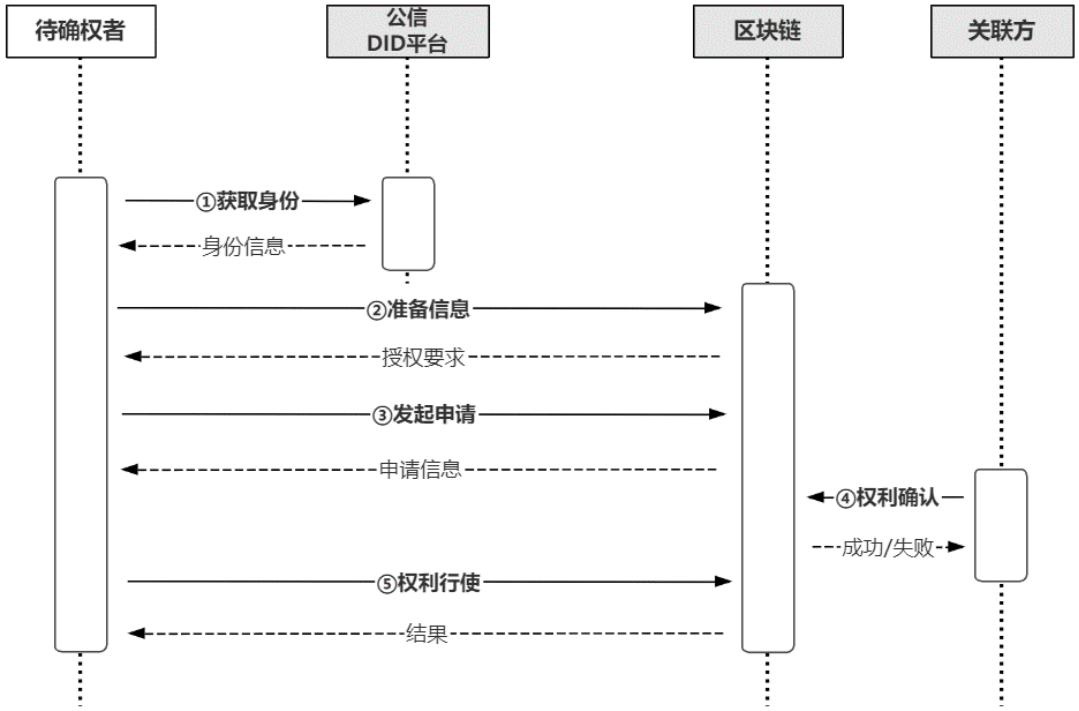

图 3 数据确权流程示意图

第一步，获取身份：准备使用数据的个人或机构需要在分布式数字身份（DID）服务平台申请数字身份，该身份将同步登记至区块链网络；第二步，准备信息：使用方在区块链的数据目录检索，查询到数据要素及其对应的合法管理方（可能是所有权方或者托管方）和申请要求，准备相关信息和材料；第三步，发起申请：以自己的 DID 向管理方发起数据要素使用申请，相关申请信息在区块链传输、留痕；第四步，确认权利：数据管理方审查申请信息，用自己的 DID 身份授

权同意；第五步，行使权利：使用方凭借授权凭证，在链上发起取数动作，通过智能合约管理方鉴定后，获得数据要素。

3.3.2 激励分润流程

从数据要素流通的渠道划分，数据要素协作模式主要分为两类，一类是数据要素链上流转模式，另一类是数据要素专线（链下）流转模式。不同的数据要素协作模式，与区块链的交互也不同，这也让激励模式有所差异。

数据要素链上流转模式。数据要素经过脱敏、加密等预处理加工后，上传到区块链网络，数据要素使用方通过智能合约，进行查询、授权、付费等流程后，直接在区块链网络获取到数据要素，同时积分被扣除，奖励给数据所有者。以数据要素使用方获取数据为例，激励模型流程如下图所示。

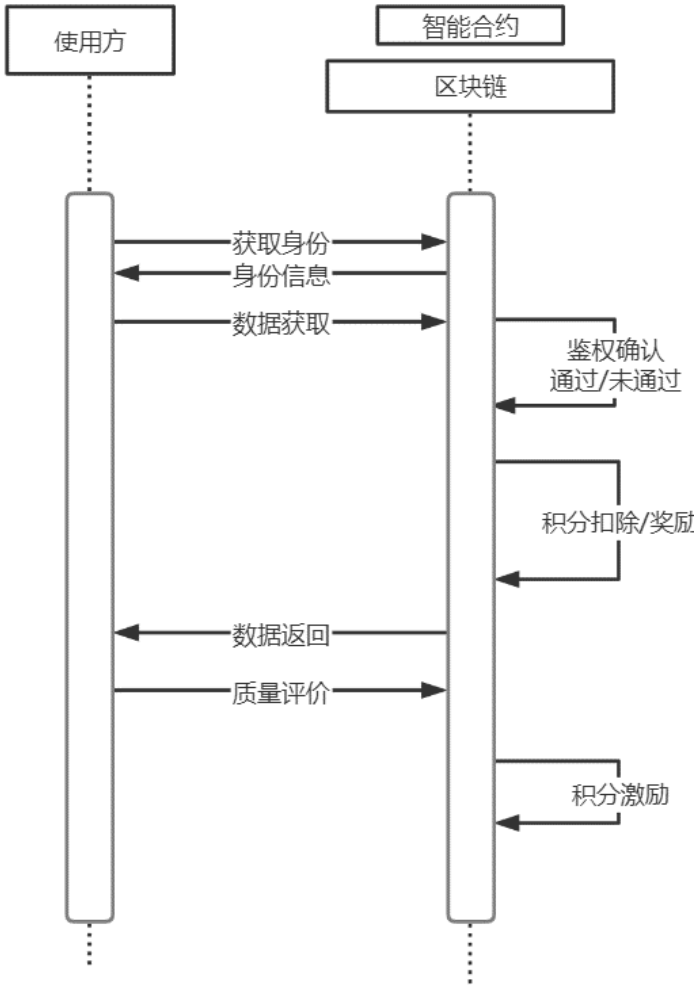

图 4 数据要素链上交易

第一步，获得初始积分。数据监管者为参与成员发放初始积分；第二步，获取数据请求。数据要素使用方向智能合约发起获取某一类数据的请求；第三步，智能合约鉴权。验证数据要素使用方授权情况与积分。通过数据要素使用方的交易签名获得其区块链数字身份，根据数字身份获取请求数据的授权情况，如果授权验证不通过，驳回交易请求，授权通过后验证数据要素使用方积分额度，将交易需要的积分从其数字身份账户扣除，给数据所有者积分奖励，然后将数据返回给数据要素使用方；第四步，数据质量评分。数据要素使用方消费数据后，可以为数据进行打分，通过打分，数据监管者会定期披露数据

质量排名，并对排名靠前的数据所有者/使用者进行积分激励。

数据要素专线（链下）流转模式。数据要素所有方仅将元数据信息上链（如数据指纹、标识，一般不包含数据要素关键信息），数据要素使用方通过智能合约获取基于元数据的授权，数据所有方确认授权后通过专线将数据给到消费者，在这个过程中，交易双方将操作记录发送给智能合约，智能合约根据记录对双方激励。简化过程如下图所示。

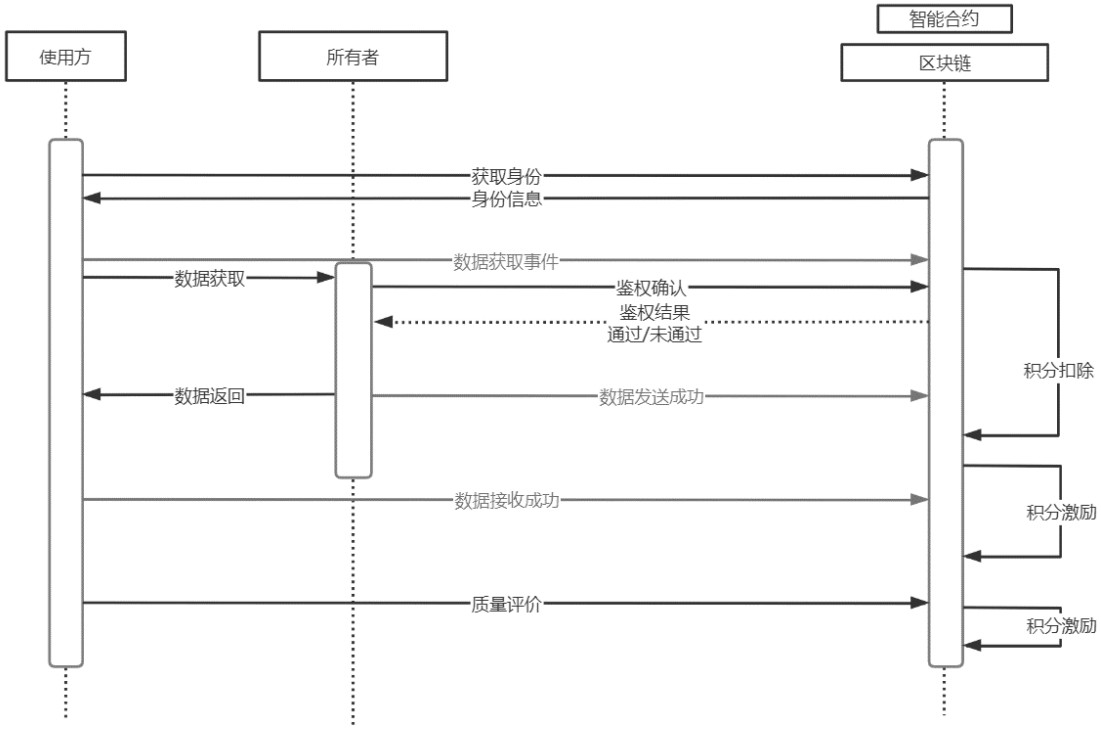

图 5 数据要素专线流转

初始步骤监管者向参与方发放初始积分。第一步，数据获取请求。数据要素使用方将数据获取请求记录上链，同时向数据所有者发送数据获取请求；第二步，数据鉴权及数据交易。数据所有者向智能合约获取数据要素使用方的鉴权情况以及积分额度是否能够支付此次交易，鉴权通过后，数据所有者将数据返回记录上链，同时将数据发送给数据要素使用方，此时智能合约对消费者账户进行积分扣除，待接

收到消费者将数据接收成功的记录后，将积分激励给数据所有者账户；第三步，数据质量评价。为了确保数据要素链上元数据和专线数据的一一对应，数据要素使用方可以在链上发起基于元数据的验证，并且给出一致性评价。

3.3.3 区块链数据协作流程

基于区块链的数据协作流程如下图所示，整个计算由区块链系统编排、调度、驱动和记录。

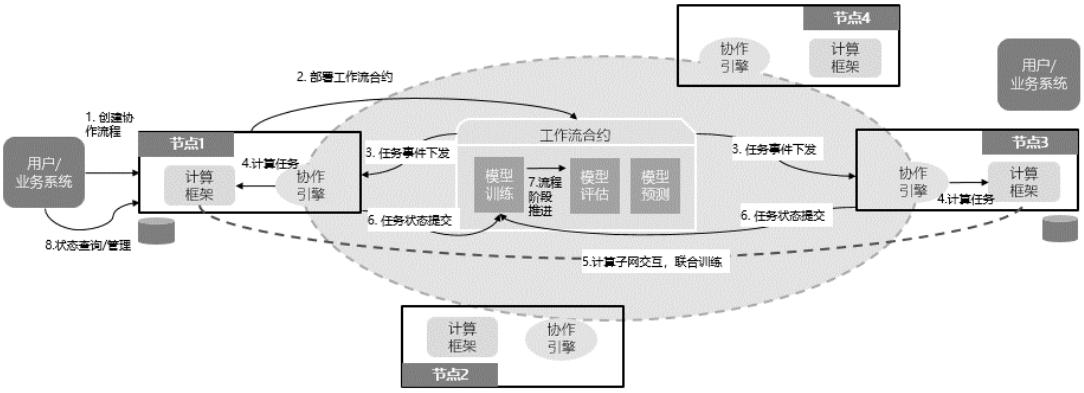

图 6 区块链数据协作流程示意

用户业务系统提交创建协作流程的请求到本地部署的协作节点，协作节点将协作流程转换成智能合约，并部署到区块链上，部署完成后合约自动触发执行。协作引擎解析链事件，包括计算输入、算法选择、算法参数、任务参与方以及计算输出等，转换成计算请求，调用计算引擎执行任务。各计算引擎根据计算任务进行多方协作计算，包括数据准备阶段、各方对齐阶段、计算阶段以及结束清理阶段。协作节点之间在计算子网内交换密文数据，执行计算任务。计算引擎计算任务结束后，计算结果保留在协作节点本地，协作引擎将协作任务结

果状态上链提交到协作流程合约中。

前一步的协作任务结果如果为成功状态，则协作流程合约推进执行下一步骤流程，继续协作任务事件下发步骤。如果前一步协作任务结果为失败，则整个协作流程实例状态置为失败，流程合约下发任务终止信号到各个参与节点，终止正在执行的协作任务。用户业务系统调用查询任务状态接口，获取协作任务最新状态和最终计算结果状态，并根据协作流程约定获取结果数据。

3.4 功能描述

基于区块链的数据协作计算网络、系统或平台具备以下基础功能要求。

3.4.1 数字身份

数字身份可以是分布式数字身份（DID），也可以是基于公钥基础设施（PKI）的中心化身份。其中，分布式数字身份旨在将分布式账本技术与身份治理融合，建立一个以密码学为基础的隐私保护与数据安全的数字身份认证系统，将数字身份的所有权和数据流转控制权归还所有者。分布式数字身份的 DID 标识符、可验证凭证技术、DID 消息协议（DID Comm）等技术，可以作为数据协作网络的信任基础设施。

3.4.1.1 数字身份认证和注册

在数据协作网络构建之初，可以为平台运营方预置可信的数字身份，生成身份标识，并将必要的身份信息公布在区块链上。平台运营方为其他参与方进行身份认证，并生成相应的身份标识。将各参与方

公开密钥、验证方法、对外服务地址等信息组装成文档，并记录在区块链上。平台运营方可以为参与方颁发可验证数字凭证，包含参与方的具体身份信息（参与方类型、参与方权限、参与方详细信息等），由各参与方保存和保管。

3.4.1.2 可信通信

数字身份使用身份认证和安全通信协议，来保护消息的真实性、完整性和机密性。

基于挑战-响应模式（Challenge-Response）的身份认证方式框架，可与不同的数据格式、传输机制和协议相结合，用于认证对方是数字身份的拥有者。基于挑战，身份所有者紧接着构造一个响应，以证明对其数字身份的控制。

完成身份验证之后，参与数据传输的各参与方对传输数据内容进行签名，然后双方均根据己方私钥和对方公钥协商计算得出一个相同的共享密钥，对数据内容进行加解密。在这个过程中，通过数据提供方签名确保了原始数据未经过修改，即报文的完整性；共享密钥加解密确保了数据的机密性，只有正确的数据使用方才能解密数据，防止通信过程的中间人攻击。

3.4.2 管理功能[8]

3.4.2.1 用户管理

用户管理模块为用户提供注册、登录、退出、密码管理等功能，支持用户进行添加、删除、停用等管理功能。

[8] 参考资料：T/CCSA 410-2022 《区块链辅助的隐私计算技术工具 技术要求与测试方法》中的 6.1

3.4.2.2 节点管理

节点管理模块提供数据协作计算网络中的节点的添加、删除、停用等功能，进一步可对数据协作计算节点的运行状态进行监控，在节点异常时可提示告警。

3.4.2.3 区块链管理

区块链管理模块提供区块链网络中的共识状态、区块信息、交易信息等链上信息查看功能，还可提供合约部署、合约销毁、权限管理、区块链节点管理等功能。可支持数据协作计算网络中数据资源目录的确权、发布和维护过程，便于数据协作的各参与方共享数据、算力资源。区块链管理模块可通过区块链智能合约实现对于数据协作计算的协调功能，包括协调数据协作计算的任务触发、任务配置、任务流程控制、信息同步、任务终止等。

3.4.2.4 算法管理

算法管理主要管理接入数据网络的算法程序，使得数据按照预先定义的使用目的参与计算。算法管理模块支持算法方从数据网络中获取数据的基本信息，确定数据的基本结构信息，支持算法方按照数据格式进行算法代码开发，并从数据网络获得测试数据并进行算法测试，支持算法方将开发好的算法元信息（算法标识、编译器信息、代码指纹、算法参数信息等）签名后发布到区块链中。

3.4.2.5 任务管理

任务管理模块包含交互界面为用户提供进行数据协作计算任务的创建、停止等全流程管理功能，支持数据协作计算多任务并行执行。

进一步结合任务的特点，支持任务优先级设定或任务队列等方式，对计算任务进行统一调度和管理。该模块还支持数据协作计算任务状态监控，在任务异常时支持告警提示，支持计算任务在异常中断或手工中断时，可以恢复执行任务。

3.4.3 数据引擎

数据引擎主要面向数据方，涉及数据的注册、使得要共享的数据处于可以被发现的状态，同时数据方可以对数据的使用请求进行授权。该模块主要承载数据源的桥接、数据导入导出的管理、数据注册发布、数据分类分级、数据脱敏、授权鉴权等能力。

3.4.3.1 数据注册

数据注册模块支持数据提供方将数据的元信息（数据标识、数据访问地址、数据结构等）签名后发布到区块链上，并支持其他参与方浏览数据网络中发布的数据集。

3.4.3.2 数据授权

数据授权模块支持数据提供方收到来自其他参与方的数据使用请求，请求中包含要数据使用方标识、使用的数据标识、使用目的等，支持数据提供方审核数据使用方的基本信息、请求使用的数据和数据的使用目的，通过后数据方对请求进行签名授权，并将授权信息发布到区块链中，数据使用方获得授权后取得数据的使用权并按照使用目的使用数据。数据协作计算任务和链上数据授权合约签订记录需可关联、可审计。另外为了增强灵活性，数据授权可以支持单次计算任务授权、也可支持按时间周期授权等多种授权方式。

3.4.3.3 数据资源管理

数据资源管理模块提供数据集的新增、删除、查看等功能，为每个数据集提供元数据管理功能，即数据集名称、简要描述、字段类型、字段长度、样例数据等信息。数据集的查询可支持扩展的关联查询功能，如数据集被授权的机构列表、数据集被引用的计算任务列表等。

3.4.3.4 数据预处理

数据预处理通常包含字段名规范化、重复数据识别及处理、日期格式规范及字段衍生、缺失值识别及规范化、数据集行和列的删除处理、自动数据类型识别等操作。数据预处理模块提供数据集的自动识别处理，或基于 Web 交互方式、自主定制编程方式的手动数据预处理等功能。

3.4.3.5 分类分级

分类分级模块提供数据治理规则和分类分级等功能，帮助用户在业务协作中能高效找到数据。每个链上数据条目都带有类别/级别/共享规则信息，分类分级模块支持数据提供方对每个数据条目设置类别/级别/共享规则信息。

3.4.3.6 数据接入代理

数据接入代理模块提供文件接入、数据库接入、流式接入等多种数据接入方式，实现数据源接入。进一步地，文件接入方式包含但不限于 CSV、TXT 等，数据库接入方式，包含但不限于 MySQL、Oracle、Hive、HBase、MongoDB 等。

3.4.4 计算引擎[9]

3.4.4.1 输入输出功能

在计算开始前，确定两方或两方以上的数据输入，数据输入保证基于数据处理能力实现的多种数据接入方式。在计算结束后，需要支持结果的输出，其中结果输出的形式包含数据协作计算得到的算式结果、数据集合、规则模型等。

3.4.4.2 数据基础协作计算能力

数据资产的协作计算需涵盖以下计算能力：基础计算、集合求交、统计分析、复杂机器学习计算等。在基础计算方面，可支持两方或两方以上的多方隐私数据算术运算、关系运算、逻辑运算等基础运算功能，支持两方或两方以上的多方隐私数据集的交集、并集、差集等数据集合计算。在集合求交方面，可支持两方以上隐私数据集合操作时，每两方数据对齐的 ID 列是不同列的应用场景，在数据集合操作的统计、分布信息等非泄露数据隐私的信息应作为计算结果回执存储在链上，支持上层业务应用计费或对账使用。在机器学习方面，可支持多方特征工程处理，如：特征处理（最优分箱）、特征分析（相关系数）、特征筛选（iv 筛选、相关系数筛选、变量重要性筛选）等，可支持机器学习算法进行模型训练和预测，包括但不限于：回归模型、分类模型、聚类模型等。

[9] 参考资料：T/CCSA 410-2022 《区块链辅助的隐私计算技术工具 技术要求与测试方法》中的 6.3 计算能力。

3.4.5 协作引擎

3.4.5.1 协作编排

协作引擎接受使用协作编排描述语言描述的协作实例，完成协作网络的服务治理，身份映射，计算流程和协议编排以及其他节点管理工作。包括:

1） 环境描述：即整个流程所执行的工作空间;

2） 流程描述：即整个流程需要执行的任务列表和任务之间的前驱后继关系图。任务之间的依赖关系由输入输出依赖关系唯一决定。即如果任务 B 的输入列表中引用了任务 A 的输出，那么任务 B 依赖于任务 A;

3） 参与方描述：每个任务的具体参与方和他们的角色。允许发起实例的成员列表（initiators);

4） 数据描述：即整个流程需要从加载输入的外部数据源以及需要发布输出的数据结果;

5） 参数描述：即每个流程运行实例和每个任务的具体参数;

6） 其他描述：包括授权管理，运行方式其他元数据描述等。

3.4.5.2 协作过程存证

具体地，数据协作计算的执行过程应将必要的关键环节在区块链上通过存证合约进行哈希存储，在保证链上存储数据结构的合理设计的前提下，实现计算过程的全程可审计，包括:

1） 数据协作计算的参与方公开信息，包括但不限于：参与方的名称、公钥、数据协作计算节点 IP、端口地址、注册时间等;

2） 数据协作计算的过程数据哈希存储上链，包括但不限于：计算的中间结果、计算涉及的数据维度、计算规则或模型的指标等，以区块链的区块数据不可篡改特性增强数据协作计算的数据信任;

3）数据协作计算的部分关键计算过程上链进行，包括但不限于：模型贡献度的计算、模型指标的计算等，以区块链的智能合约逻辑公开透明增强数据协作计算的计算信任。

3.4.6 数据权属凭证

基于区块链技术实现数据权属凭证的系统或平台具备为数据提供方提供发行数据权属凭证，数据使用方交易数据权属凭证，算力提供方及算法方可根据数据权属要求协作参与计算任务、获取分润，为平台运营方提供管理数据权限凭证模板，为审计方提供审计交易的基础功能。

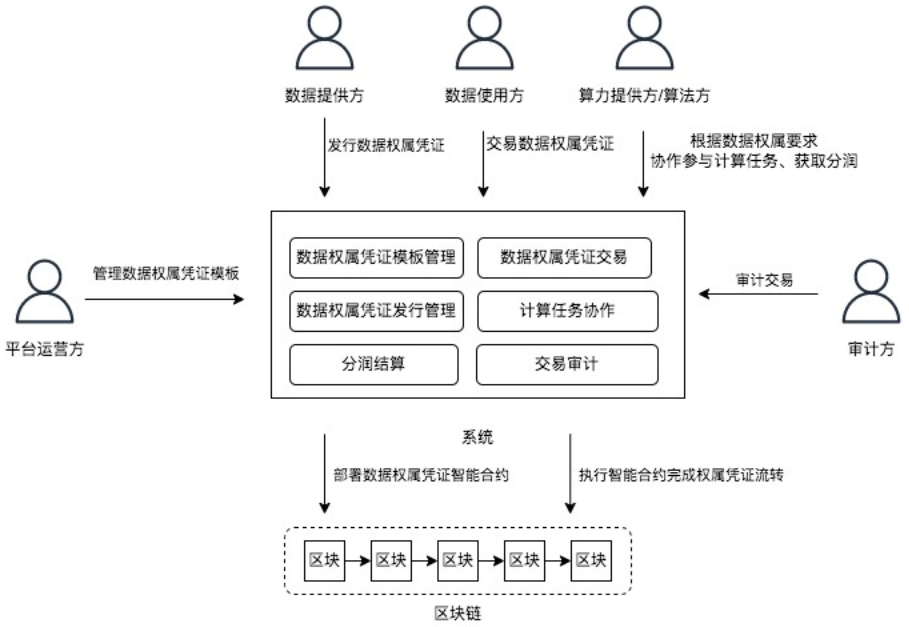

图 7 数据权属凭证流转流程

3.4.6.1 模板管理

管理方发布可使用的数据权属规则，根据区块链智能合约的类型生成相应的数据权属模板，从而以合约代码的形式定义了数据权属的要求与规则。

3.4.6.2 发行管理

数据提供方应用数据权属模板发行数字化的数据权属凭证，输入数据权属的元数据，如数据类型、数据源、权益范围、协作分润比例、定价等，系统根据数据权属凭证所对应的智能合约模板，在区块链上部署为所对应的智能合约实例，并设定数据权属凭证的所有者为数据提供方的链上账户地址；数据权属凭证发行后可供数据使用方查看与交易。

3.4.6.3 凭证交易

数据使用方对数据权属凭证进行交易，系统通过执行智能合约完成权属凭证变更。

3.4.6.4 计算任务协作

算力提供方及算法方根据数据权属凭证的要求完成计算协作任务。

3.4.6.5 分润结算

若在数据权属凭证中定义了数据协作要求，在数据协作任务完成履约后按智能合约中的要求提交证明，通过智能合约完成验证，根据合约中定义的分润比例进收益结算。

3.4.6.6 交易审计

审计方通过系统可对数据权属凭证模板、数据权属凭证模板智能合约、数据权属凭证、数据权属凭证交易等内容进行审计。

3.5 系统稳定性

数据协作计算系统应满足参与方之间稳定的网络传输、安全计算执行，宜支持在网络抖动、硬件故障等异常情况下的断点恢复执行功能。

区块链网络宜设计基于自身共识机制的容错方案，支持在阈值范围内部分节点异常的情况下，继续保持链上计算任务的正常执行和验证，链上数据存储正常打包进区块。

3.6 链上链下交互

链上链下交互是指区块链系统实例和链下的数据系统之间交换信息，并对所交换信息加以使用的能力，主要表现在区块链系统和外界数据系统之间进行安全交互的过程。区块链的多方共识、难以篡改等特性可保证链上数据的安全存储与共享，但对与链下系统交互过程中的数据安全可信、隐私保护、安全使用等方面还需借助其他技术。因此该过程涉及的关键问题包括数据可信、隐私保护、安全监管等。

3.7 安全要求[10]

建设区块链数据协作网络前，需要达成建设区块链的共识。各参与方应共同组成治理委员会，制定联盟治理章程、定义治理框架涉及

[10] 参考资料：JR/T 0184—2020 《金融分布式账本技术安全规范》。

的要素以及区块链网络的运行和结束相关的内容。可以借助中心化的治理系统或链上的智能合约机制，管理提案以及投票流程，达成相关方的共识并在区块链网络执行。

区块链数据协作网络的建设总体需要遵循《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》要求以及相关国家、行业标准，对数据安全进行保护。

3.7.1 权限管控

接口调用应采用权限控制，对登录用户应进行身份标志和鉴别，防止未授权的接口调用和数据访问。私有链或联盟链应配置相应的访问控制策略，限制不同类型的用户对链上信息的读、写、修改等权限，实施最小授权原则。对一定时间内的接口访问次数应设置上限，以保证整体区块链性能。

3.7.2 密码安全

密码安全遵循现有国家相关法律法规标准要求。例如，《区块链密码应用技术要求》（GM/T 0111—2021）中对密码算法的相关要求，如公钥密码算法应采用 SM2 椭圆曲线公钥密码算法，符合 GB/T 32918 要求；密码杂凑函数应采用 SM3 密码杂凑算法，符合 GB/T 32905 要求；分组密码算法应采用 SM4 密码算法，符合 GB/T 32907 要求；随机数生成算法所产生的随机数，符合 GB/T 32915 等要求。

3.7.3 数据安全

在数据协作过程中，数据提供方和使用方都应具备明确的数据分

类分级、数据生命周期管理体系。区块链节点之间的数据交换，原则上不应明文传输，应采用数据完整性校验技术或密码技术保证重要数据在传输或存储过程中的完整性。

1） 参与数据协作计算任务的数据提供方原始数据，在数据协作计算任务执行过程中，不应以明文形式或可被其他参与方解密后导出数据协作计算作用域的密文形式将数据交互给其他参与方；

2） 在数据协作计算任务执行过程中，数据协作计算过程的中间结果、链上计算过程的中间结果、链上存储的数据内容均应不包含原始数据、不能反推得到原始数据，实现数据隐私的保护；

3）数据协作计算采用的设计方案或协议原理应满足各自技术领域的安全模型设计，并结合具体业务场景需求，满足不同层级要求的抗恶意攻击行为能力；

4） 在区块链上存储的数据协作计算过程信息、结果信息，需要通过智能合约的权限控制，只允许必要的参与方有权查看；

5） 数据协作计算任务的结果仅允许使用方获取，非使用方无法直接查看或反推计算结果。

3.7.4 网络通信

网络通信保障数据、信息在传输过程中的安全性。数据协作计算节点间的通信报文应采用协议层加密交互，报文内容宜进行应用层加密，确保报文内容安全。报文数据结构设计可支持区块链上非对称加密秘钥签名等完整性验证方式。通信节点间建立安全传输通道，保证数据传输的保密性、完整性和不可篡改性。数据和信息采取相应的防

护措施，保证其能抵抗篡改、重放等主动或被动攻击。

3.7.5 身份管理

应实现有效的用户身份管理，应能保障身份信息的安全性，并对身份进行监管审计。应保障参与实体的真实性，可使用数字签名等密码技术生成可靠的电子签名来保障实体行为的不可否认性。

3.7.6 隐私保护

对个人信息，特别是个人敏感信息可采用安全存储（如不存储在公开链上）、脱敏变换等技术手段，以实现数据保护。涉及个人信息的数据交换，应依法获得个人信息主体的授权，将数据交换的使用目的和使用的数据类别明示告知个人信息主体。根据场景不同，上链的数据应进行数据脱敏、去标识化或匿名化处理。建议结合隐私计算、联邦学习等技术，实现“数据可用不可见”，在最小授权的情况下进行数据协作。数据协作网络内的所有操作行为都应被记录系统日志，不可更改且可被查询，确保过程的可审计性和可追溯性。

3.8 网络形态

在当前区块链生态中，无论是国际还是国内，多种类、多环境、多功能的异构区块链网络并存发展。这种情况一方面给基于区块链的数据协作网络设计引入了复杂性，需要充分考虑多网、子网、平行网之间在网络层的协同交互；另一方面，这种多形态的网络模型也可以为我们所用，可以达到功能解耦、负载均衡、安全隔离等效果。

3.8.1 单网络

单网络即数据要素的全生命周期、参与的各个角色都在同一个区块链网络上。单网络是最简单、高效的架构模式，但是相对其他网络形态而言，在可扩展性、隐私安全性方面较弱。这种网络形态适用于参与方相对固定、数据应用模式简单的场景使用。

3.8.2 母子网络

母子网络，即存在上下派生关系的网络，这种网络常用于映射现实世界的管理关系或总分关系。母子网络由多个不同的底层链构成。通常，母链承担统筹管理职责、子链承担操作执行职责。具体到数据协作网络汇总，可以将母链用于数据要素生命周期的身份体系和确权凭证环节，子链则用于数据的流通、使用、交易环节。同时，子链还可以再派生出新的“母子链”，这样形成树形的网络形态。各层职责划分清晰、管理交互有序，数据安全互不直接相通，这种网络形态适用于有 G 端或监管方参与、参与角色多层丰富、数据应用隐私安全要求高的场景使用。

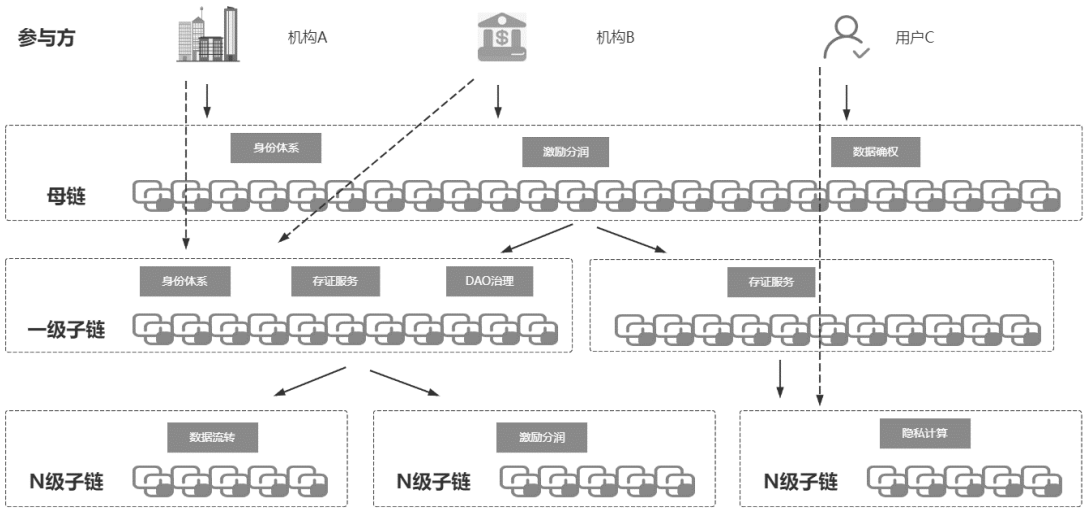

图 8 母子网络模型

3.8.3 平行网络

平行网络即关系对等的区块链网络，任何两个区块链网络，无论同构还是异构，都可以构成平行网络关系。使用区块链的跨链技术可以让平行网络之间进行通信协作，进而实现数据协作网络的构建。相比于母子网络，平行网络更加自由灵活，只要相互之间约定好一套标准即可开展业务。这种网络形态适用于各参与方已有区块链网络或定制化需求的场景使用。

3.8.4 立体网络

利用区块链可以构建多层次立体化的隐私协作网络，包括数据计算网络、共识协作网络等类型的子网。数据计算网络包含了多种隐私计算算法能力以及标准化的数据引擎完成数据的确权、授权和计算转化。在业务协作网络层通过动态子网的划分，实现数据使用和流转的边界清晰可控。共识协作网络实现数据流转和授权记录的可信可审计。共同构建了数据全生命周期的流转和计算管理能力。

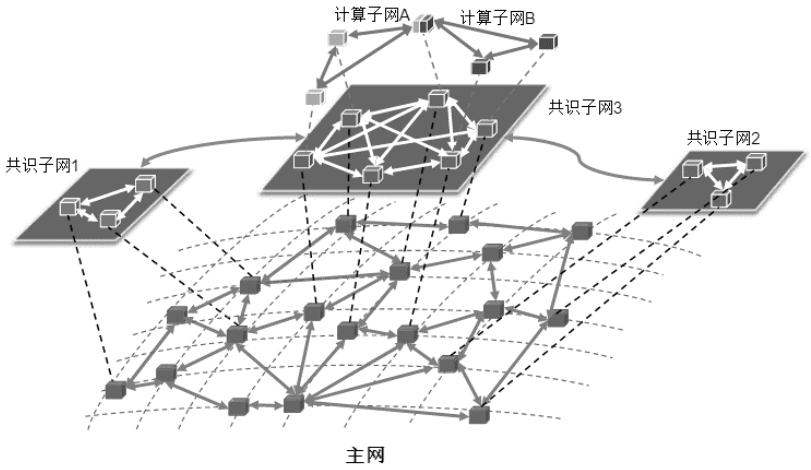

图 9 立体网络模型

综上所述，在数据协作大场景中，每种网络形态都可能存在，甚

至相互交融、演进。例如，单网络因为要和外部的数据要素市场网络对接，就变成了母子网络或平行网络的一环。平行网络因为数据共享业务的调整改变，又可能拆分为两个单网络。数据协作业务开展时，应根据效率、安全等实际需求来进行选择。

四、 方案特点

本文提出的参考实现具有数字身份安全可信、用户数据自主可控、数据目录多方共享等特点。

4.1 数字身份安全可信

数字身份是数字化的用户属性集合，可将其理解为用户实体在数字世界的映射，用于对用户行为产生的数字信息进行绑定、查询和验证。基于区块链的分布式数字身份（DID）体系通过区块链特性及密码学技术，可以为数据协作网络中的不同主体提供安全可信的数字身份。技术上 DID 与区块链结合，业务上引入公信力机构参与数字身份认证和管理，可以高效地让个人和机构在数据协作网络中证明“我是谁”这个问题，这也是数据确权能够得以实现的基础前提。

区块链可作为分布式注册表用于第三方数据托管方和数据所有方、数据使用方的数字身份的登记。通过区块链上发布的数字身份元数据及公开密钥等信息，各参与方可对其他参与方身份进行认证并通过加密、签名和密钥交换等机制建立安全的消息通道，杜绝身份仿冒，降低数据在传输中泄漏的风险。

4.2 用户数据自主可控

基于区块链的数据协作网络，将数据的持有者也就是企业和个人，引入了数据协作模型，区别于目前的数据发行方直接将数据发送给数据使用方，数据发行方将数据发送给用户，由用户自行选择使用方，以及需要的数据内容和尺度。这样的协作模型，解决了数据的权属合规问题，因为数据本身就是用户的。其次，用户是业务的直接参与者，最清楚使用方需要的数据类型，提高了数据共享的匹配和精准程度。再次，用户直接授权使用方使用数据，不需要数据发行方承担数据泄露的风险和责任。最后这样能满足不同用户多样化的共享尺度，解决了数据协作使用中“一刀切”的问题。

4.3 数据目录多方共享

在数据要素流通的过程中，为保证数据的隐私性和安全性，数据可能会存储在多个参与主体中，对外以数据目录的方式进行展示，访问方可通过数据目录存储的内容了解数据的基本信息，在数据所有方授权之后即可通过数据目录访问数据。在多方参与的数据协作网络中，利用区块链可以串联众多参与主体、简化数据目录共享的链路。在链上不仅可以实现高效、多方可查阅的数据目录，而且利用智能合约建立安全灵活的权限控制体系，做好数据授权和鉴权工作，确保数据访问的安全可控是数据使用过程的核心。

4.4 数据确权可信一致

区块链可通过哈希算法为数据生成“指纹”，数据内容不同，所

生成的“指纹”也会相应变更，由此建立起数据与“指纹”的对应关系和完整性；在链上不同的“指纹”对应的数据内容不同，所以确保了数据的唯一性；链上数据生成绑定了相应的时间戳，使得数据具备了一定时间属性；通过非对称加密技术保护数据的所有权归属，从而实现数据确权，为数据的所有权归属提供了技术解释和手段。

通过基于区块链的数据权属凭证实现数据可信资产确权，解决数据权属凭证的一致性、真实性、可支配难题，具备不可伪造、不可篡改、验证可信等独特优势，完成数据要素化，使得数据可成为生产要素参与市场化配置。

4.5 数据流转合规透明

为了防止数据被篡改，可以利用区块链不可篡改的特性，将原始数据的摘要在区块链上进行存证。参与方在使用这些数据前，可以通过获取区块链上对应的存证进行摘要比对，以验证数据的完整性和真实性。更进一步，如果数据需要被长期存储并且变更频率较低，区块链可以直接作为数据的载体。用户可以将加密后的数据存储在区块链上，利用区块链不可篡改和分布式的特性进行数据托管。

数据发行方通过区块链定义共享数据的标准和管理已发送数据的生命周期，数据持有方也就是用户可以通过区块链进行身份的注册和多种数据的关联，数据使用方通过区块链验证数据发行方、数据持有者身份以及数据格式和有效性。区块链可以匹配数据要素确权和流通过程中的协作有据、串联多方、信息可信不可篡改和智能合规要求。

数据在协作过程中使用非对称加密、同态加密、零知识证明等密

码学技术保证数据在各环节的安全和隐私，降低了数据在中间环节泄露的风险；最后，利用区块链分布式、不可篡改的特性，能够记录用户数据的全生命周期链路，保证数据真实有效性，数据使用方可以通过自己的节点来验证数据的有效性。

4.6 激励分润智能便捷

开发者将事先制定好的激励机制通过智能合约代码进行实现，避免因为对激励机制理解分歧而导致的纠纷，可以低成本的方式达成共识。代码对所有参与方透明，可以让参与方安心、安全的进行数据要素交易。智能合约一旦部署到区块链上，就会按照既定的流程执行，数据交易一旦成立，激励就会实施发放。

4.7 监管审计灵活高效

现阶段数据标签与数据分析等大数据技术已经在审计中广泛使用，而作为强化数据协作的基础设施，区块链多方参与、多方共识、共享账本的特性大大提高了审计与监管机构接入的灵活性，同时区块链技术的可追溯性也让审计工作变得更加高效。在数据开放协作后，针对数据使用的审计也尤为重要，结合区块链技术，相关的数据使用记录可全流程记录于区块链，记录不可篡改，实现数据开放协作过程的可查、可证和可溯源，充分实现数据使用过程的审计。

五、 应用实践

5.1 区块链智慧汽车经销商融资服务

申报单位：交通银行股份有限公司。

技术领域：物联网、大数据等。

技术产品：Hyperledger Fabric，ThingsBoard。

应用时间：2018 年 10 月。

5.1.1 案例背景

交通银行智慧汽车经销商融资服务依托区块链技术打造了汽车产业链电子化金融服务产品，数据协作方面，主机厂、银行、经销商、监管方多方将合格证状态等信息上链通过修改合格证的状态，其他参与方可以实时追溯合格证的变化状态，同时参与方都无法篡改信息。该产品实现了汽车合格证监管全生命周期可追溯、合格证状态多方协作同步，解决了场景参与方众多、合格证状态转换频繁、监管难度大等业务痛点，提升汽车金融整体融资业务效率，进一步降低业务风险。

5.1.2 创新成效

主机厂、银行、经销商、监管方多方将合格证状态等信息上链，同步修改合格证的状态，其他参与方可以实时追溯合格证的变化状态，参与方之间无需通互相对接来更新相关合格证的信息，通过数据多方的协作，提升业务办事效率。

该服务以一套标准化接口方案实现业务对接。对于每个业务模块可以通过标准化接口快速接入体系，依托标准化接入模板、开发测试

等流程进行区块链的接入，保证业务应用与区块链技术分离。

对于基础服务开发注重适用性，与业务逻辑解耦，使其适用于系统内所有业务模块，在服务层封装方法供业务模块调用，如文件下载、发票自动查验与结果反馈、线上三方协议签署。

图 10 智慧汽车经销商融资服务技术架构

（1）技术创新。

数据上链保证了数据的不可篡改性，在数据协作方面，主机厂、银行、经销商、监管方多方对现有汽车合格证录入、提证、盘库、出库等数据状态同步上链更新，同时，其他参与方可以直接通过链上查询合格证全生命周期记录，包含合格证更新时间、更新主题等信息，进一步提升了合格证监管可信度，通过数据多方的协作，提升业务办事效率。

该服务将监管的 30 万辆车辆信息接入物联网系统，跟踪车辆生产、运输、销售等状态，使用流计算技术实现车辆数据的实时计算及预警。同时，聚焦客户经营场景数据，形成数据模型。目前在汽车经销商领域逐步形成了包括客户经营评价、客户融资履约评价、客户合规评价、客户效益评价等四大类 39 个子类指标维度。这些分析模型有助于提升风险识别和处置能力，提升客户体验。

该服务将合格证全流程的信息保存在链上，保证了汽车合格证流转信息的完整性，数据信息经过系统同时需要业务审核之后才触发上链，保证了数据的准确性和真实性以及数据要素的价值，同时产业链多方上链的数据涉及业务是为汽车产业链金融服务，其特殊的应用场景同样也决定了该数据要素的价值。

通过对汽车合格证信息和质押物环境信息进行 API 服务化，对经销商、核心企业和银行多方提供相应服务。对数据进行分析提供经销商融资情况，其中核心企业和银行等参与方可以通过此数据，判断经销商的经营情况以及在当地的规模，对质押物环境信息分析，判断储存环境是否适合，可以及时的调整相应策略，以达到风险管控和保障的目的。

（2）业务创新。

实现汽车金融产品全流程线上化，主机厂、银行、经销商、监管方多方数据协作对现有合格证信息录入、提库、盘库、出库等信息上链更新，并通过合格证追溯查询功能来获取合格证全生命周期，包含合格证更新时间、更新主体等，进一步提升了合格证监管可信度，提

升了业务办理效率，促进了外部合作机构加入交行联盟链体系，完善汽车金融生态建设。目前，智慧汽车经销商融资服务年业务量已突破百亿元，累计上链监管近百万张汽车合格证，金额超百亿元。

5.1.3 产业价值

提供主机厂、银行、经销商、监管方多方更新的汽车合格证流转的详细数据，包含客户信息、合格证状态变更等信息，对链上信息进行查询分析，可以判断相关企业的规模，提供预警提醒等相关服务，并及时做出相应对策。

通过对合格证状态变化频率和合格证数量的分析，能够快速提升经销商融资管理的效率，减少经销商私售、逾期等情况，降低坏账风险和企业经营风险，并及时根据分析结果进行相关的应对措施，保障了金融行业汽车产业链生态的健康性。

5.2 多方可信计算智能银行网点选址服务

申报单位：上海浦东发展银行股份有限公司、北京百度网讯科技有限公司。

技术领域：Hyperledger Fabric、可信执行环境。

5.2.1 案例背景

浦发银行与百度进行可信计算技术合作，在数据“可用不可见”、不暴露用户隐私的前提下，基于区块链和可信执行环境技术联合多方数据进行协作，在银行网点选址业务场景上开展探索，利用将现存的银行网点历史数据、客户画像数据、营业数据与消费数据以及地图数

据、人口数据等放入可信执行环境中进行模型训练与计算，预测得出银行网点选址推荐。

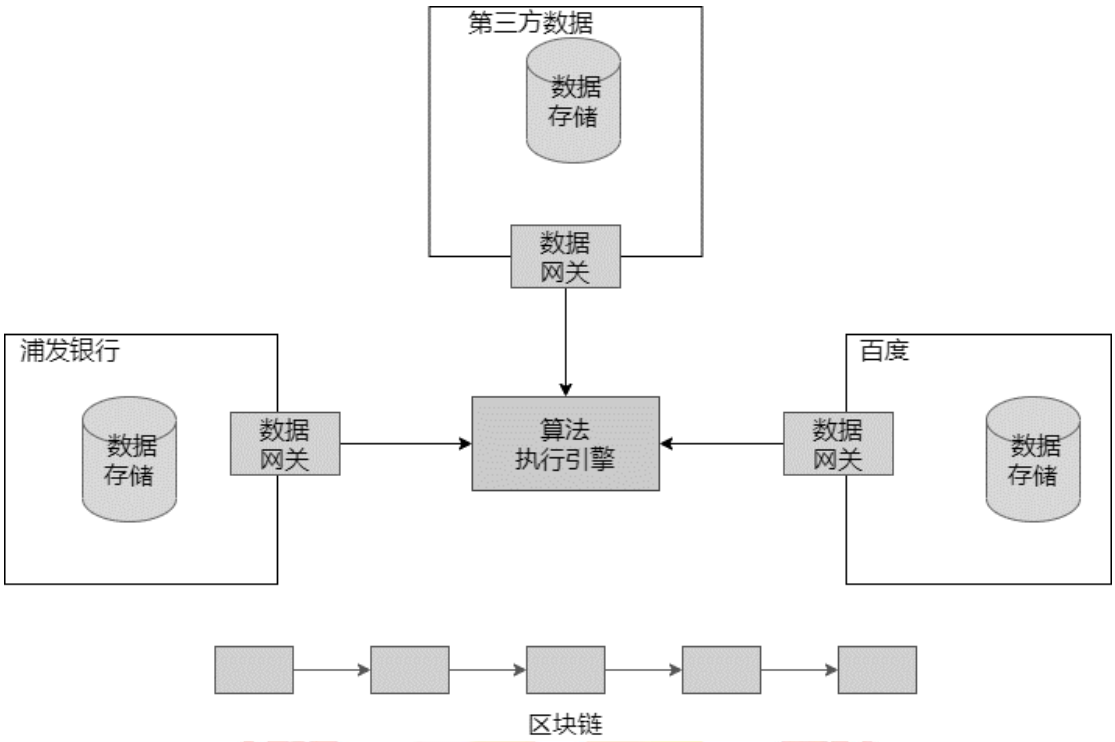

图 11 5.2 多方可信计算智能银行网点选址服务技术架构

5.2.2 创新成效

浦发智能银行网点选址服务已成功应用于深圳和武汉两地。该服务结合区块链技术和可信计算技术，构建了多方参与的隐私计算平台，与传统的银行网点选址服务对比，基于数据可信共享的智能网点选址方案能够让不同类型的数据持有方参与其中，在安全、高效的环境中共享数据，训练出更精准的预测模型，实现人工智能的跨越式进步，使得银行网点选址决策时间大大缩短；量化选址结果的指标项，使选址依据更明确、合理；根据选址需求，合理调整指标项重要度，精准定位服务人群。同时，这一选址服务模式可复制，可横向扩展，可以

落地至更多行业，提供多样化的选址服务。

5.2.3 产业价值

确保各参与方数据安全。基于数据可信共享的智能网点选址方案可确保各参与机构不泄露用户数据，安全合规地进行数据合作。

数据使用降费增效。改变传统的数据一次采购、终生使用模式。通过数据的“可用不可见”，保证了原始数据明文不泄露、数据所有权的确认。从而促使数据使用按量及次数计费成为可能，降低了数据使用费的同时提高了数据使用效率。

降低网点选址失败率。采用大数据计算模式，与优质数据机构打通数据，利用多维度数据训练模型得出网点选址推荐结果，有效规避人为干预影响，降低选址失败风险。

5.3 多方大数据隐私计算平台

申报单位：深圳前海微众银行股份有限公司。

技术领域：区块链、隐私计算、安全多方计算。

技术产品：FISCO BCOS、WeDPR。

应用时间：2020 年 12 月。

5.3.1 案例背景

广袤的数据资源散布在不同实体之间，为将数据资产价值最大化，需各实体进行数据融合、协作计算与使用。在金融业务营销场景，金融机构往往需要联合众多机构实体以获取海量数据支撑业务体系，如银行希望通过企业客户信息库与外部平台进行数据合作，识别双方平

台共同客户，找到更精准（交集客群）的目标客群，提升借贷与理财广告定向投放的精准性；测算外部合作平台客户分布情况判断合作价值。然而各实体进行数据协作时面临数据隐私保护与合规风险，亟需隐私计算方案来降低工业大数据流通的风险，加强数字监管能力建设。

借助微众银行场景式隐私保护解决方案 WeDPR，金融机构与合作机构可在保证客群信息原文不出私域的前提下，完成多方数据的隐私撞库、匿踪查询、画像补全、营销模型建设等，实现精细化交叉营销。

5.3.2 创新成效

WeDPR 隐私计算平台已集成联合统计、联合建模、联合预测、匿踪查询、隐私求交等隐私计算能力，构建了一套银行、互联网机构、政务机构等进行多维数据用户画像构建与营销的隐私协作机制。

基于 WeDPR 的联合营销技术架构如下图。隐私计算参与方角色包括数据方、计算方、用数方（即结果接收方）、审计方（可通过区块链实现）。所有数据方的私密数据（包括原文数据、模型参数等）都通过安全多方计算协议先进行加密和拆分，再发送给多个计算方（如果数据方同时为计算方则无需此步骤）。每个计算方只拥有各数据方隐私数据的密文分片，无法通过密文分片逆推出原始隐私数据，但可与其他计算方进行密文交互计算，获得计算结果的密文。最终由各方约定的结果接收方解密获得计算结果。

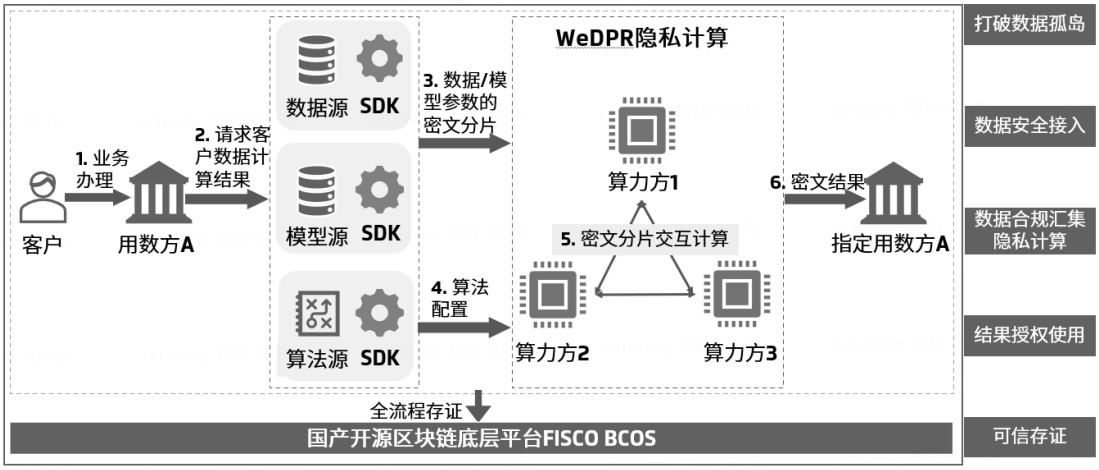

图 12 微众银行区块链融合安全多方计算的隐私计算解决方案架构

上述整个过程中，金融机构及其合作机构的身份、权限，客户信息的属主、使用范围、使用方、使用期限，数据流转的关键过程、计算结果及结果接收方的身份等信息都会通过区块链进行存证与同步，实现营销数据全生命周期的隐私保护与监管审计。

技术创新点主要包括以下三方面。

（1）融合区块链构建隐私计算协作互信底座

WeDPR 将区块链和隐私计算进行技术融合，区块链为分布式协作构建信任机制和数据流转枢纽，契合跨机构合作中的可信数据授权管理需求，结合分布式数字身份和密文对账技术，可以打消因数据敏感性而无法上链的难点；隐私计算为流转在区块链中的信息提供全密态数据计算能力，让链上数据实现可用不可见的效果。

（2）优异性能支撑海量数据计算

WeDPR 通过自研一系列简洁、高效的零知识证明、批量不经意传输等技术，实现对十亿级大数据集的处理、毫秒级的端到端快速响应、对隐私数据与计算过程的高效验证，全面满足工业级性能、安全性及稳定性要求。

（3）支持任意数量机构同时参与

基于安全多方计算、零知识证明、监管审计、国密算法等核心技术能力，WeDPR 支持任意数量机构同时参与各类隐私计算任务，全面适配实际业务中的多方平等协作模式并提供完备的计算功能。

业务创新体现在 WeDPR 依托区块链等分布式可信智能账本技术，兼顾用户体验和监管治理，围绕金融营销应用场景提供针对性技术方案，提供结合联合统计、联合建模、隐私求交、匿踪查询、联合营销模型建设等功能的一体化场景解决方案，打消企业担心客户信息明文出库的顾虑，增加其业务接入意愿，共同构建更多维的用户画像，促进金融业数据流通与价值提升。

同时，基于 WeDPR 的联合营销解决方案中的功能组件也可扩展运用在除金融外的政务、公共健康等领域，在联合风控、反欺诈、反洗钱、数字化个人与企业服务等场景议题中，促进隐私数据有序流通，实现跨域价值融合创新。

5.3.3 产业价值

金融机构借助 WeDPR 隐私计算平台，有效打破产业内多中心数据壁垒，且保证各机构客户数据均不会暴露给对方与任何第三方，通过对多方客户信息进行去标签化处理，利用更多维度的数据为客户做更精准的画像，助力金融机构对客户进行加白、去黑、促活、拉新，从而提升精准营销的效果，促进业务增长。将之前由于担心隐私泄露而无法开展的业务以更安全合规的方式开展，冲破业务发展瓶颈；同时借助 FISCO BCOS 联盟链，一方面促使参与机构与数据形成信任网

络，另一方面机构身份、权限、数据元信息、关键计算过程、计算结果的上链存证，也为金融行业监管提供可行之路。

作为金融行业的隐私计算案例实践，基于 WeDPR 的联合营销方案结合区块链数据可见不可得和安全多方计算可用不可见的优势，实现金融营销数据在授权、共享、使用、审计的全生命周期管理下数据价值的合规流通，赋能金融机构释放多源数据的融合价值，助力推进隐私计算在普惠金融、金融监管、联合风控等更多金融场景的应用落地。

5.4 基于区块链+隐私计算/AI 数交所可信协作平台

申报单位：蚂蚁区块链科技（上海）有限公司。

技术领域：区块链、数据流转、隐私计算。

技术产品：蚂蚁链数据可信协作平台。

应用时间：2021 年。

5.4.1 案例背景

数据交易所连接数据提供方和数据使用方，为其提供供需磋商和场内算力等服务。数据共享及价值挖掘需要解决隐私保护、数据可信等问题，“区块链+隐私计算"是目前业界认可的有效解决方案。传统直接共享原始数据的方式，无法对共享出去的数据进行有效的管控和保护，既不利于保护数据资产权利，也不利于防止数据滥用和个人信息泄露，该方案结合了隐私计算和区块链的优势，能在数据共享过程中有效保护个人信息，并为数据真实性、数据确权等问题提供可行解

决方案，实现全流程可记录、可验证、可追溯、可审计的安全、可信数据共享网络，实现“数据不动模型动”，并为进一步建设高效、高安全和高流动性的数据要素交易市场打下基础。

5.4.2 创新成效

蚂蚁链数据可信协作平台将区块链、多种隐私计算能力融合成一个整体方案，面向多样化的数据以及差异化的数据应用场景需求，提供全生命周期的安全管控服务。在大规模的数据开放场景中，单一的隐私计算能力不足以解决不同的管控需求，设计实现该技术方案，将不同的数据分类分级管理，并智能化地通过链上智能合约（数据协作任务定义文件）调度到不同的参与机构的数据资产、计算资源以及符合数据安全等级要求的不同计算引擎资源中执行数据处理和服务化输出，提供了面向联盟网络的多方数据可信安全协作与数据可信开放的能力，有效保证了数据安全的前提下最大化释放数据价值。

以区块链+隐私计算技术为依托，针对传统数据中台及大数据平台明文数据流转、裸数据流出等数据安全问题，进一步将不同安全等级的重要数据分级分类管控，采用加密入库的方式在隐私数据库（数据隔离区）中独立存储、重点保护。针对不同安全等级的数据，制定相应的数据流转规则、共享开放规则，采用密文流转、加密计算、模型计算等方式，避免明文数据流转引发的安全问题，真正做到重要数据全生命周期安全管控，高敏感数据可用而不可见。

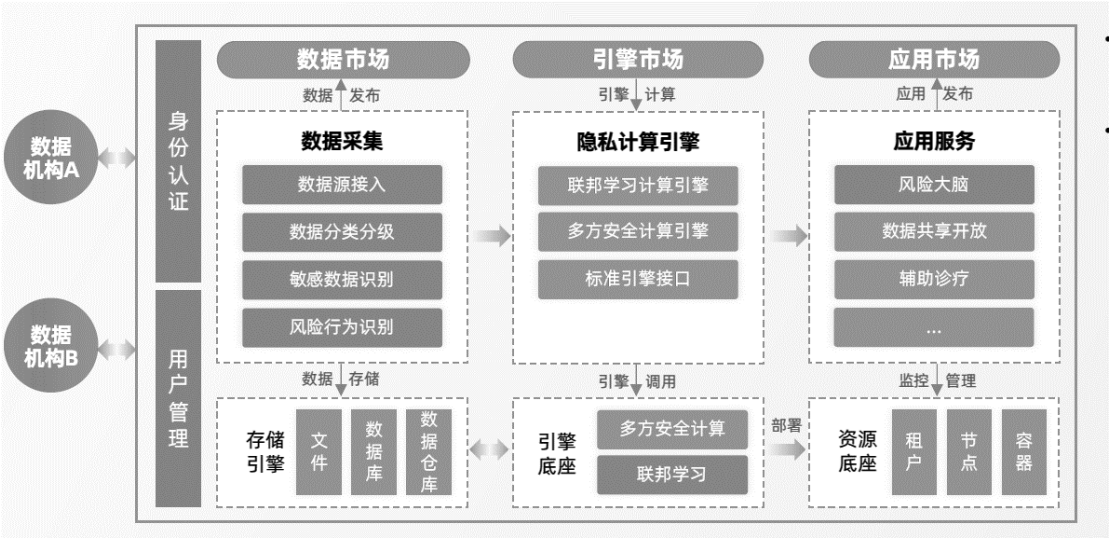

图 13 蚂蚁链数据可信协作平台架构

5.4.3 产业价值

通过该平台使得之前无法流转开放的数据可以安全、放心地开放使用，实现了政务、制造业、医疗等行业数据开放的基础设施建设，在安全和高可用方面弥补传统大数据软件的不足，满足数据要素市场培育的政策要求，节约数据开放管理的人力成本，提供用户友好的协作应用搭建工具、可视化交互界面，能够提高数据协作的效率。

基于蚂蚁链的数交所可信协作平台产品依托“区块链+隐私计算"等多种数据安全、隐私技术领域的技术积累，可帮助数交所连接不同行业的企业。目前已帮助部分区域性数据交易所链接数据的上下游厂商，券商、银行、信托、基金、会计事务所、律师事务所等，构建“审批流”、“行为流”、“数据流”三大数据安全保证流程，形成接入、开发、使用等全生命周期数据安全管理体系。

5.5 区块链+隐私计算供应链金融数据协作方案

申报单位：腾讯云计算（北京）有限责任公司。

技术领域：供应链金融、隐私计算。

技术产品：腾讯云数链通产品。

应用时间：2021 年 11 月。

5.5.1 案例背景

在家电领域的供应链金融中，零部件供应商、家电生产商、经销商需要从银行进行融资贷款，以提升产能。这些供应链上下游的企业之间，需要对生产、销售、经营、财务等数据进行共享，银行基于输入的数据，结合风控模型，评估供应链上下游企业的信贷额度，进行信贷业务处理。传统的数据共享方式给数据所有方带来很大挑战，一方面数据明文或者密文要出域，另一方面共享出去的数据的所有权和控制权无法有效保障，迫切需要新的数据共享方式来实现对数据计算安全、数据权属的保障。

通过区块链隐私计算平台，可以实现对数据隐私安全及所有权的保障。家电领域的上下游企业，可以将他们的数据加密以后输入到隐私数据协作平台里，银行基于风控模型和输入数据，进行风控评估和信贷业务处理。

5.5.2 创新成效

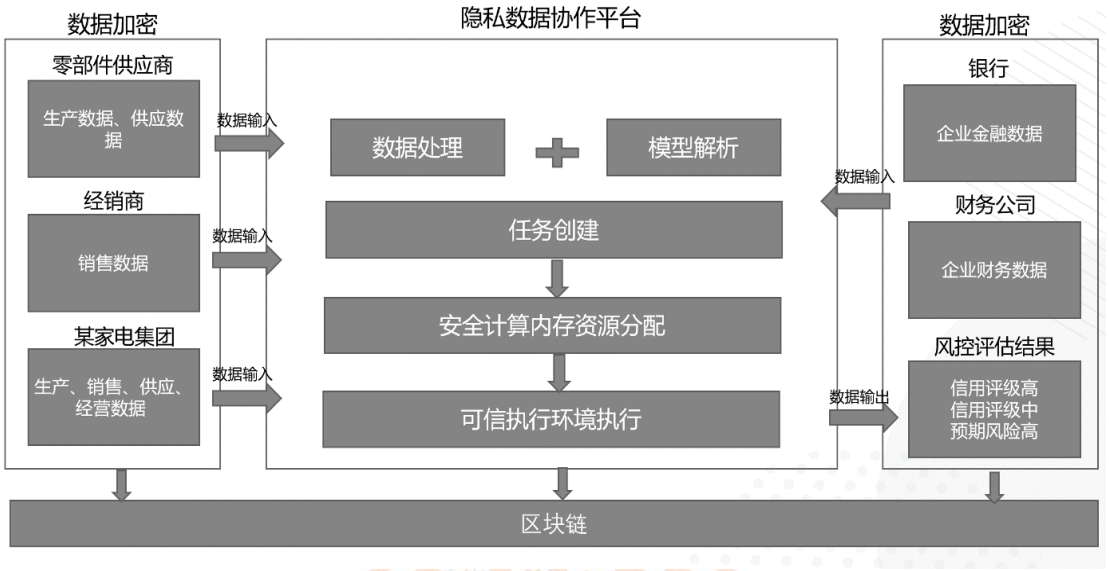

图 14 技术架构

基于腾讯云区块链数链通平台，结合区块链和隐私计算技术，实现对数据隐私安全及所有权的保障。其中区块链技术用于实现数据的存证，隐私计算技术用于保障数据共享过程中的可用不可见。

零部件供应商的生产、供应数据，经销商的销售数据及集团的生产、销售、经营数据加密以后输入到隐私数据协作平台里，金融机构、财务公司把企业金融数据、财务数据等加密传入隐私计算协作平台，风控评估算法模型发布到隐私计算环境中，在隐私计算协作平台中，对加密传入的数据进行处理，结合发布的模型，进行风控模型任务的创建、执行，最终将企业的风控评估结果给到金融机构或者财务公司，然后根据风控评估的结果进行信贷业务处理。

通过在家电集团及金融机构分别部署隐私计算 TEE 节点，金融机构发布经过双方审计的算法模型，家电集团将己方数据加密传输到隐私计算节点中，金融机构将己方的数据加密传输到己方的隐私计算节点中，双方的隐私计算节点通过远程证明构建起可信传输通道，将中

间计算结果进行交换，最终将预测完成的风控结果给到金融机构。

（1）技术创新

通过平台建设，将家电领域中生产、销售、经营、财务等供应链各个环节的数据，进行加密数据的共享管理。通过使用区块链技术、可信计算技术，实现技术的组合创新，打造数据可信协作平台，实现上链数据的可信存证，保证平台在行业内竞争力。通过隐私计算技术，在数据不出域的前提下，准确识别信贷风险，提升信贷风控治理水平，促进供应链金融业务开展。

（2）业务创新

通过平台建设，将家电行业的供应链上下游数据进行共享，将数据、模型在可信的执行环境下高效运算，实现数据隐私保护，更好地通过供应链金融赋能产业，更好的实现产业价值，让数字经济在链上流动起来。

5.5.3 产业价值

通过该业务场景建立供应链金融可信数据协作基础设施，促进了供应链金融中数据的高效流动和业务流动，让数据更加安全的实现应用价值。

经济价值主要体现在，区块链实现可信存证改善产业环境；通过信息可追溯确保供应链金融中上下游企业的高效协作，提升供应链上下游企业的信贷效率，促进产业协作，同时提升银行的信贷风控水平，降低信贷风险；通过隐私计算，则实现供应链上下游企业的高效数据共享，保障各企业的数据安全。

应用价值体现在区块链、隐私计算与供应链金融的结合，实现了供应链金融的创新模式，发挥了区块链可信存证、隐私计算可用不可见的技术特性，可以提升供应链金融的业务效率，促进产业链各方高效协同。

5.6 基于区块链的产融数据协同服务平台

申报单位：拉卡拉支付股份有限公司。

技术领域：区块链、大数据、隐私计算。

技术产品：拉卡拉区块链即服务平台、拉卡拉数字化协作平台，以及拉卡拉数字资产服务平台。

应用时间：2022 年 5 月。

5.6.1 案例背景

本项目基于拉卡拉支付公司在商户支付服务基础上，综合应用了区块链、大数据、隐私计算等技术，通过科技手段帮助小微企业对经营性流动资产（应收应付账款）进行数字化、可视化、可控化改造，确保底层数据场景完备、客观、真实、不可篡改、可溯源、可交叉验证，形成可被市场各方广泛认可的，有优质底层实体资产做锚的数字资产形态，让企业能够自主可控的把数字资产对接到金融机构端，获取更低的资金成本或者更快的对接速度。同时应用人工智能和大数据技术对行业数据和企业的经营数据进行智能分析，快速生成企业经营画像和分析结果，提供给企业进行风险自评和金融机构进行辅助风控决策。

5.6.2 创新成效

拉卡拉产融数据协同服务平台中应用的核心技术包括了区块链即服务、隐私计算、低代码开发、大数据分析、智能语义理解等。

区块链即服务技术：底层基于超级账本和长安链双链研发，实现企业在现有的云基础架构之上对区块链核心资源进行虚拟化管理、支持动态分配和横向扩充。隐私计算技术：将联盟链与基于公钥证书体系（PKI）的实名账户体系结合，实现链上匿名、链下实名、身份可核验但不可见，在保护隐私的前提下实现联盟链的开放性与交易的主体溯源。低代码开发技术：支持数据协作模型的可视化拖拉拽开发，自动编译成可链上执行的智能合约。

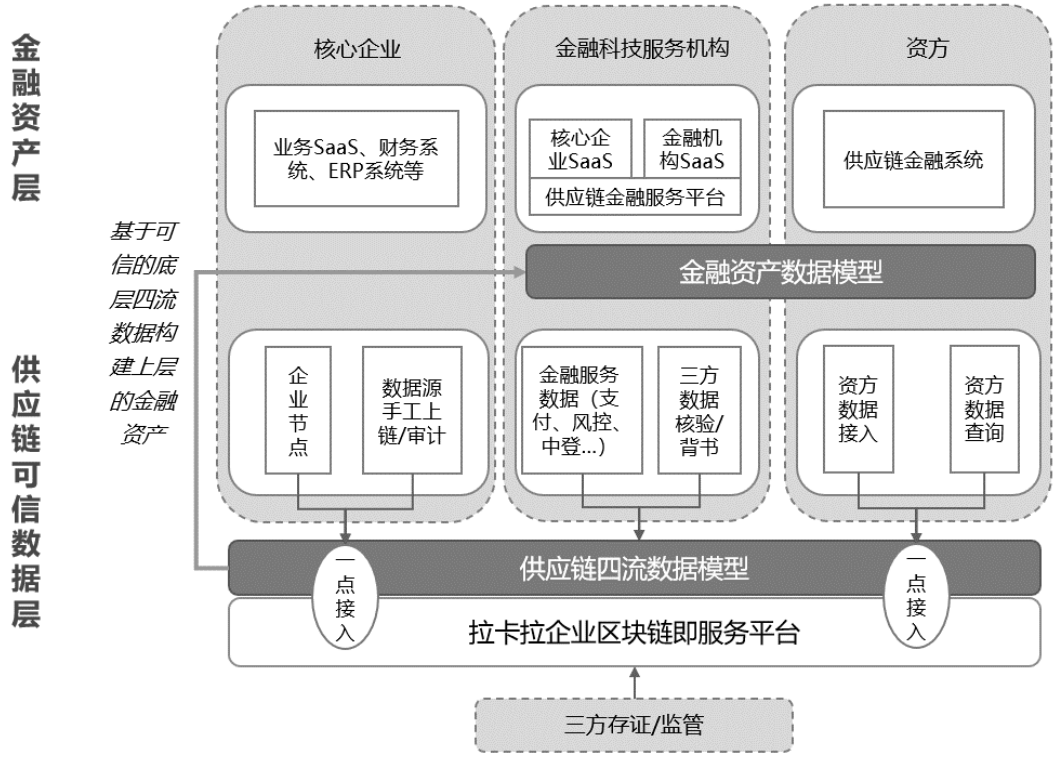

图 15 拉卡拉产业数字金融科技服务平台技术架构

产业金融的一个特点就是场景的多样性。各行各业的四流数据结构、风控模型均有很大差别，甚至同一行业中的不同客户也有很大差

别。大多数情况下，产品内置的功能和模型只能解决部分需求，剩下部分需求仍然需要进行定制开发。拉卡拉产融数据协同服务平台所应用的区块链、大数据等技术涉及较高的专业门槛。为此产品引入了领域驱动的低代码开发技术，让非技术人员也可以通过可视化界面对金融场景进行定制，系统自动生成智能合约或者专家规则，极大的提高了开发效率。

5.6.3 产业价值

拉卡拉产融数据协同服务平台提供了产业客户与金融机构之间进行数字化链接的一系列工具。目的是帮助产业客户实现数字化升级，将产业生态内的商流、信息流、物流、支付流水等数据与金融机构打通，数据实时同步上链，实现不可篡改，确保数据可信，进而形成有价值的数据资产，帮助产业链内的中小微企业在融资场景中更好的实现从主体信用到数字信用的转变。

5.7 基于区块链技术的数据要素确权流转平台

申报单位：杭州溪塔科技有限公司。

技术领域：数据流转、区块链。

技术产品：溪塔科技数据要素确权流转平台 RivTrust。

应用时间：2021 年 10 月。

5.7.1 案例背景

数据只有流转才能产生价值。实现数据共享与隐私保护平衡的重要前提是权属清晰。然而，由于数据所涉主体众多、所含利益多元，

因此，数据和信息的“非物”属性一直是数据确权的痛点。

一方面，个人以信息为载体的数字化存在是其在网络空间的自然延伸，个人信息不仅承载着人格价值，还具有财产属性，更与其作为社会人在智能时代作出行为和保护自己合法权益紧密相连。增强数据主体信息控制能力和保障个人信息安全的个人数据权利的构建，已成为保障个人信息所含合法利益的关键。另一方面，数据控制者进行数据交易的前提是数据产权清晰，但数据共享平台之间的利益相关性却导致各平台之间利益多元化。由于掌控的数据存在权利交叉情况，导致企业数据确权困难重重[11]。

5.7.2 创新成效

图 16 数据要素确权流转平台技术架构

[11] 参考资料：陈根，《隐私保护制约数据共享，二元平衡仍待数据确权》。

溪塔科技数据要素确权流转平台 RivTrust 是使用了云原生微服务架构，采用分布式部署，基于分布式数字身份，数字信封，可验证凭证技术的产品。

云原生架构。云原生应用的设计，可零修改部署到 Kubernetes(K8S)、openshift 等容器云环境；无缝衔接 IaaS、PaaS 和 SaaS 层相关云端基础服务。可直接使用云端统一的注册中心、服务网关、分布式数据库、分布式存储、分布式缓存、统一认证中心、依赖私服、日志系统等组件。云原生支持图形化部署和命令行部署两种方式；支持持续迭代开发交付，自动 CI/CD 构建发布，完整的 DevOps 过程。

微服务。整个应用由多个细粒度的微服务组成，每个微服务有单独的数据库 DB 与数据模型。微服务之间通过 REST API，事件流和消息代理的组合相互通信。

分布式部署。在微服务拆分的基础上，应用可以分布式部署。每个应用的微服务都可以启用多个实例，并且分开部署到不同的宿主机上。通过负载均衡器，调度使用。

分布式数字身份。基于 W3C DID 规范及 DIF didcomm-messaging 传输协议实现身份所有者自管理和授权，身份使用方在被授权的情况下使用而无法作其他用途。

链上存证随查随用。凭证上链存证，数据安全可见，无惧信息孤岛，随查随取随用。

权限分层数据加密。高可用性权限分层，非对称加密算法，链上

数据无篡改，数据披露可定向、可选择。

数字信封加密传输。采用数字信封传输技术，高隐私保障，密码、密钥加盐存储、密钥不传输，为客户提供稳定可靠的数据价值化流转一站式服务。

复杂凭证全面支持。支持各类复杂凭证类型，支持供应链、金融、能源、工商、税务等多凭证申领使用。

高度可靠无限扩展。基于 K8S 云原生技术设计、动态扩缩、广泛分布、支持多场景应用程序无限扩展。

某银行实施该方案后，可以方便解决银行里面需要开具资产等各种证明的需求，而且基于各类敏感信息问题，RivTrust 除了可以对原始值进行验证，还可以在只接受脱敏后的 hash 值的情况下完成验证工作。基于这种特性不光银行可以使用还可以提供给银行的合作伙伴使用。

5.7.3 产业价值

RivTrust 是基于区块链的数据资源价值流转的载体与数据可信共享平台。在保证数据隐私的前提下，产品可助力不同机构间的产业协同，完成数据资产的全生命周期管理，实现数据资产的确权、保护和价值转移。某银行实施该方案后，解决了纸质文件易伪造，难鉴别的问题。现在很多企业不允许使用外界的 U 盘，带证书的数字文件使用的诸多不变也不存在。

六、 总结

数据是时代发展与科技进步的产物，也是当下时代最重要的生产要素之一。区块链技术具有公开透明、不可篡改、可编程和分布式等技术特性，在实现数据确权与经济活动等方面具有显著的优势。区块链和分布式账本技术可构建多方信任的数据使用生产关系，分布式数字身份等技术能够实现数据的确权，助力构建数据要素协作信任底座。

该报告立足于数据要素流通，提出基于区块链技术的数据协作网络，分析了数据协作网络模型，提供参考架构，以应用实践清晰展示金融业基于区块链技术的数据协作网络应用现状。利用区块链、隐私计算技术实现多方机构间数据安全、可信、可追溯的流转，推动金融业数据更便捷、安全的流转及使用，促进数据要素跨地区、跨机构、跨层级合规有序流通，为探索数据要素化路径提供实践经验，为推动我国数据要素市场加速发展发挥示范先行作用。