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

基于联盟链技术的隐私保护金融应用研究报告

北京金融科技产业联盟

2022 年 7 月

版权声明

编制委员会

主　编：

潘润红

编委会成员：

何　军　　刘承岩　　聂丽琴

编写组成员：

强　锋	魏博言	昌文婷	姚　明	彭宇翔	李　力
裴　磊	钟　亮	杨文玉	张晓蒙	何　浩	靳　新
李　博	郑华祥	曾钰涵	孟　丹	唐仕豪	卞　阳
黄翠婷	杨天雅	李琦睿	王顺业	周　超	张子怡
张姗姗	高志民	王云河	时　代	何东杰	于雅楠
杨　彪	贾　澜	金银玉	单进勇	蔡超超	邵　兵
苏庆慧	刘　江	刘　姝	龚自洪	王光中	傅跃兵
薛瑞东	陈　剑	王朝阳	李辉忠	张海鹏	李瑞男
陈　凯	张骏雪	王　寰	毛小利	董　朦	铁　力
赵　红	纪崇廉	宋鑫磊	臧　铖	陈嘉俊	张敬之
徐　静	李　伟	汪小益	郭　栋	赵　伟	车春雷
王　东	邓飞陬	王　雪	李武璐	霍昱光	郭　林
陈　俊	王健宗	黄章成	卢春曦	艾轶博	陈　佳

主　审： 黄本涛　刘宝龙

统　稿： 郭　栋　魏博言

参编单位：

北京金融科技产业联盟秘书处

中国工商银行股份有限公司

成方金融信息技术服务有限公司

深圳市洞见智慧科技有限公司

同盾科技有限公司

蚂蚁科技集团股份有限公司

北京竞天公诚律师事务所

上海富数科技有限公司

深圳长亮科技股份有限公司

华为技术有限公司

华控清交信息科技（北京）有限公司

中国银联股份有限公司

北京百度网讯科技有限公司

北京数牍科技有限公司

腾讯云计算（北京）有限责任公司

矩阵元技术（深圳）有限公司

交通银行股份有限公司

北京融数联智科技有限公司

深圳前海微众银行股份有限公司

中国银行股份有限公司

深圳致星科技有限公司

光大科技有限公司

中金金融认证中心有限公司

浙商银行股份有限公司

杭州趣链科技有限公司

建信金融科技有限责任公司

网联清算有限公司

深圳壹账通智能科技有限公司

北京科技大学

目　录

一、 数据要素在金融业的价值与隐私保护

（一）数据要素价值

1.数据生产要素背景

21 世纪以来，信息技术的飞速发展彻底地改变了人类的生活习惯和社交方式。作为消费者，人们衣食住行的各个方面都在不断地向线上迁移，网络购物、网络订餐、网络订房、网络约车、网络购票、即时通讯、社交平台等人们日常生活中几乎每一个动作都会留下数字化的行为轨迹。

与之相适应，作为商品和服务的供应方，企业也紧跟着消费者习惯的改变而不断调整着自身的经营模式、获客方法和销售渠道。同时，随着财务电算化、ERP 系统、OA 系统等现代化办公系统的普及，企业的管理行为也日益变得信息化、数字化。两者相结合，共同形成越来越多数字化的企业管理记录和商业活动记录。

作为公共管理和服务机构，各级政府的窗口部门也不断推动网上报税、网上报关、网上备案、行政许可公示、行政处罚公示、企业信用公示等电子政务系统的发展；作为司法审判机关，各级法院也在不断推动法院公告、审判文书、执行信息、破产重整信息的公开公示系统。行政机关和司法机关的信息化建设，形成越来越多的政务数据和司法数据，而这些政务信息、司法信息无疑

对评估商业主体的经营管理能力、商业信用水平具有举足轻重的作用和价值。

作为经济活动的润滑剂和助推剂，以第三方支付、网络消费贷、网络理财为代表的互联网金融活动也快速地走向前台。一方面，互联网特别是移动互联网技术快速提高了金融服务的便利性和可获得性，推动了金融普惠性的发展。无论身处何处，无论是支付、借款还是投资，人们都可以很方便地从手机 App 上获得金融服务的支持。另一方面，货币资金的存款余额、清分结算、债券市场的簿记交割、股票市场的竞价撮合等几乎所有的金融资产簿记、金融交易活动也都实现了信息化和数字化。

事实上，人类社会已经进入了一个现实社会生活与数字化活动记录同步并存且紧密融合的时代。数据记录，一方面记录和映射着人们的行为轨迹和状态变迁，另一方面也日益成为生产经营活动的计划指引和决策依据。数字化时代的商业竞争，越来越依赖于对数据记录的获取控制能力和分析处理能力。

用户画像、智能营销、智能风控、智能投顾、高频交易等这一系列“时尚”的技术名称背后，无不晃动着数据的身影，深层次里都指向人工智能对数据记录的分析和处理。

数据，逐步进入了人们社会生产活动领域，成为与土地、劳动力、资本、技术并列的第五大生产要素，深刻影响着人们的日常生活和商业竞争。

2.数据要素在金融业的重要性

金融，表面上体现为借贷、投资、融资等以交换资金的“时间价值”为核心内容的经济活动，而实质上是以“风险”为对象的管理活动。

信用水平越低的主体，融资利率越高，因为借贷违约的风险更大；越是初创阶段的公司，股权估值越低，因为投资人需要承担更大的市场风险和经营风险；投决会上，需要对目标项目进行风险评估、信用评级，从而权衡项目的风险和收益是否匹配；投后管理，需要实时追踪市场信息、新闻资讯，紧密关注为标的项目设置的救济措施是否被触发，以便及时行权以阻断风险蔓延。

站在金融机构的视角，从信用评估、风险控制到产品研发、风险定价，从资产配置、投资决策到投后管理、贷后管理，几乎每一个流程和步骤都需要对风险进行评估和衡量，而风险评估衡量的基本依据则直接指向信息和数据。所以，数据必然是金融业不可或缺的战略资源和生产要素。

（1）横向机构间数据要素融合价值

金融业是典型的数据密集型行业，运营过程中会积累大量的数据信息。微观上看，这些信息往往以自然人、法人、其他组织等用户为权利主体，以各金融机构内设的账户为核心对象，按金融资产、金融交易的不同类别分别记录、跟踪和管理。一方面，这些微观的金融运营数据可以体现相关用户的身份特征、财产状

况、收入能力和信用水平；另一方面，微观运营数据的汇聚、统计和分析则可以推演出某地区、某行业产业布局、生产规模、金融资源流转趋势、就业状况等关系国计民生的经济金融情报。

网络技术的发展推动了金融便利化和普惠性的提升，同时也使得金融用户的信用水平下沉、金融风险传播速度和危害范围大大增加，从而对金融机构之间的横向信息交换和数据融合提出了迫切的要求。

一方面，这种横向的数据融合可以提高对同一主体或同类主体信用风险的识别能力和风险管理水平；另一方面，横向的数据汇聚与融合也有利于宏观经济金融政策的制定和监管。

（2）纵向行业间数据要素融合价值

金融业作为社会经济活动的润滑剂和助推剂，与国民经济各实体经济部门、各行业、各领域都存在广泛且深刻的业务联系。或者说，金融行业的客户来源和服务对象，广泛地覆盖了全社会各个行业领域的各种层级的主体。因此，金融行业对于数据要素的需求，其实并不局限于金融业内部的横向融合，而是广泛地指向全社会各行各业，覆盖了从政务数据、市场数据、企业数据到个人数据的各个层面。

另一方面，金融行业非常重视对未来情况的前瞻性预测，这就决定了金融行业对数据要素的需求不但包括对静态数据的横向关联性分析，还包括对动态数据的纵向关联性分析，对状态数

据变迁过程的规则和规律分析等等。

不同于土地、资本等传统生产要素，数据要素并没有“竞争性”属性。就是说，一方主体对数据要素的占有和使用，并不会减损其他主体对同一数据占有使用的效用。同时，数据要素价值的汇聚、分享，反而能创造出统计、模型分析等方向上更大的价值。数据越多，边际价值越大；数据越分享，总和价值量越大；数据越跨行业、区域、国界，越多样化，综合价值越大。

所以，对于金融行业来说，充分融合跨行业、跨领域、跨层级的动态数据，不但有利于金融行业本身的数字化转型和业务创新，而且有利于全社会数据要素的质量提升和价值增长。

（二）数据要素隐私保护

1. “隐私”的不同含义

隐私保护计算的“隐私”与一般法律意义上的“隐私”存在很大区别。前者更多指数据控制者不愿公之于众的保密信息，这里的数据控制者既可能为自然人，也可包括法人、其他组织、政府机关，甚至是代表社会公共利益的国家；而法律法规语境中的“隐私”则更多指向自然人隐私权的客体，即“自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”[1]。

从数据流通合规性角度探讨，其实“个人信息”的概念要比

[1] 《民法典》第 1032 条第 2 款。

“个人隐私”更契合一些，因为当今与数据合规相关的法律规范，其实是围绕着“个人信息”的概念展开的。

按照《民法典》的定义，个人信息是指“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等”。而按照《个人信息保护法》第四条的定义，个人信息是指“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”。

从字面含义来分析比较，明显后者的范围要比前者大很多，不但包括“可用于识别身份”的信息，而且还包括虽然不能用于识别身份但与自然人存在“关联”的信息；不但包括与“已识别”自然人相关的信息，而且还包括与尚未识别但技术上“可识别”的自然人相关的信息。这其实就把很多在大数据时代人们无意识留下的行动痕迹数据，一并纳入到了“个人信息”的保护范围中了。

从种类和来源区分，金融应用所涉及的数据信息，可能包括来自金融机构和其他行业企业在经营过程中收集、形成的涉及商业秘密的企业信息，可能包括来自行政机关、司法机关的政务信息、审判信息，还可能包括自然人在申请或使用各类产品或服务时自主提供或被动形成的个人信息。

然而，不论是政务信息、司法信息、企业信息还是个人信息，

牵涉到“隐私保护计算”的，首先要属于“保密信息”，也就是控制主体对其采取了保密措施、主观上不希望未经授权的主体非法访问的信息。从这个意义上说，像法院裁判文书、法院公告、执行信息、企业工商信用档案、行政许可公示信息，或者行政处罚公示信息等公开、公示信息就不在“保密信息”范畴之列，自然也不应属于需要保护的“隐私”信息了。

所以，从法律意义上说，数据要素流通中可能涉及的数据种类可划分为个人信息、企业商业秘密、国家秘密三个不同的类别，远大于“个人隐私”的范畴。这几类不同层级的信息，分别由不同的法律体系进行规制和保护。但是，无论信息类别归属如何，如果其自身属性上体现“公开、公示”目的，那么就不应被包括在“隐私保护”的范畴之中。

2.关于个人信息保护的法律框架

在个人信息保护方面，我国的法律框架日臻完善，从全国人大表决通过的最高层级的法律，到最高人民法院颁布的司法解释，到国务院颁布实施的行政法规、国务院各部委颁布执行的部门规章，到行业组织制定的推荐性国家标准，各个层级的规范制定机构都在着力推进相关规范的立法建设。同时，从一般法到特殊法，从指引性规范到强制性、禁止性规范，前述各层级的法律规范又从适用范围、强制性程度等方向上多维交织，共同构建了一个周密而有序的法律规范体系。

在法律层面，个人信息和隐私保护的规则，主要是通过民法、行政法、刑法三个层次的法律维度构建的，如图 1 所示。

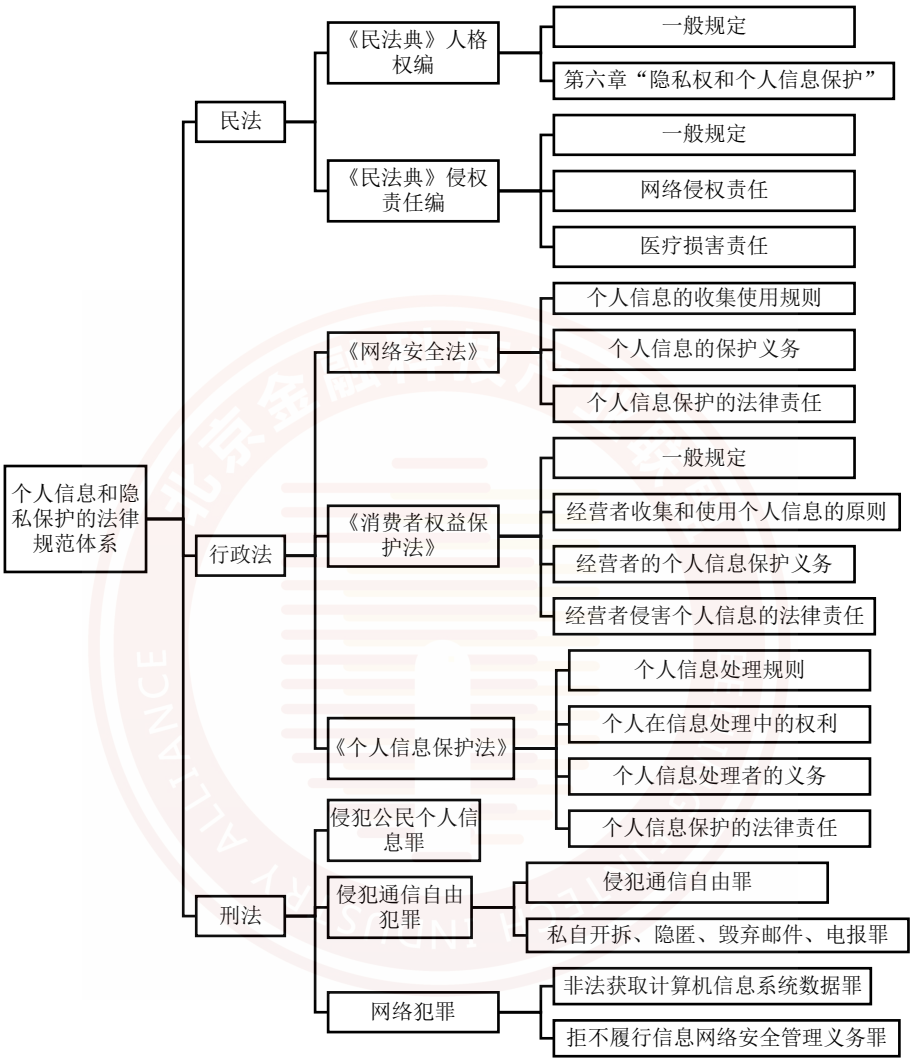

图 1. 个人信息和隐私保护的法律规范体系

个人信息和隐私保护立法具体内容如下。

（1）民法

2021 年 1 月 1 日起施行的《民法典》专章规定了“隐私权和个人信息保护”，具体内容有：明确“个人信息”的定义和范围，确立个人信息处理的基本原则，确立自然人对其个人信息的查阅、复制、删除等权利，要求信息处理者采取技术措施和其他必要措施以确保其收集、存储的个人信息安全。

此外，《民法典》侵权责任编中的一般侵权责任、网络侵权责任以及医疗损害责任等条款，也适用于个人信息保护。个人可以通过向法院提起侵权之诉，以救济自己的权利。

（2）行政法

行政法从行政监管的角度，对个人信息的利用和保护须遵循的规范以法律的形式确认下来。

2017 年 6 月实施的《网络安全法》中，第 41-45 条明确了网络运营者收集使用个人信息的原则、个人信息保护义务、违反个人信息保护的法律责任等内容，为个人信息保护创设了法律基础。

2013 年 10 月修改的《消费者权益保护法》中规定了消费者“享有个人信息依法得到保护的权利”，在增加的个人信息保护条款中规定了经营者收集和使用个人信息的原则、经营者的个人信息保护义务及经营者侵害个人信息的法律责任。

2021 年 11 月 1 日起正式施行的《中华人民共和国个人信息

保护法》（以下简称“《个保法》”）是我国个人信息处理须遵守的基本法律。《个保法》明确了“个人信息”定义、以“告知同意”为核心的个人信息处理规则、个人在信息处理活动中的权利、个人信息处理者的保护义务、个人信息保护的法律责任，在个人信息安全及隐私保护上对银行等征信机构提出了更高的要求。

在行政法的这一法律部门下，除了法律之外，还有众多的部门规章、部门规范性文件等作出个人信息保护方面的规范。相关的部门工作文件、行业标准等，虽不是强制性规范，却也对具体问题的处理作出了指引。

在金融领域，中国人民银行制定了一系列部门规范性文件规范以确保个人信息保护，这些文件的内容包括技术规范与法律规范。其中，部门规章《中国人民银行金融消费者权益保护实施办法》（以下简称“《办法》”）中专章规定了“消费者金融信息保护”，规定了消费者金融信息的“处理”的定义、处理需经明示同意规则、使用不得超出约定范围等规则，这些规则基本上是《网络安全法》《信息安全技术 个人信息保护规范》中的个人信息保护规则在金融消费者权益保护领域的具体化。中国人民银行发布的行业推荐标准《个人金融信息保护技术规范》（以下简称“《规范》”）规定了广泛适用于金融业机构的个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，及安全技术和安全管理方面的规范性要求;《规范》

还将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三类[2]，并对不同级的个人金融信息的保护提出了不同的要求。

（3）刑法

《刑法》第二百五十三条之一规定了侵犯公民个人信息罪，对违反国家有关规定，向他人出售或者提供公民个人信息，窃取或者以其他方法非法获取公民个人信息，情节严重的，追究刑事责任。该罪的犯罪主体包括自然人和单位。

此外，《刑法》中还有一些罪名虽非专门为保护个人信息而设，但也可用于规制某些侵犯公民个人信息的行为。如：侵犯通信自由罪；私自开拆、隐匿、毁弃邮件、电报罪；非法获取计算机信息系统数据罪；拒不履行信息网络安全管理义务罪等。

3.关于企业商业秘密保护的法律框架

一项信息构成商业秘密，必须同时具备以下全部构成要件：（1）不为公众所知悉；（2）能为权利人带来经济利益；（3）具有实用性；（4）采取保密措施。[3]

---

[2] C3 类主要是用户鉴别信息；C2 类主要是可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息；C1 类主要是机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。

[3] 《反不正当竞争法》第 9 条第 4 款。

对于商业秘密的保护，也存在民事、行政、刑事三个层次的法律规范，如图 2 所示：

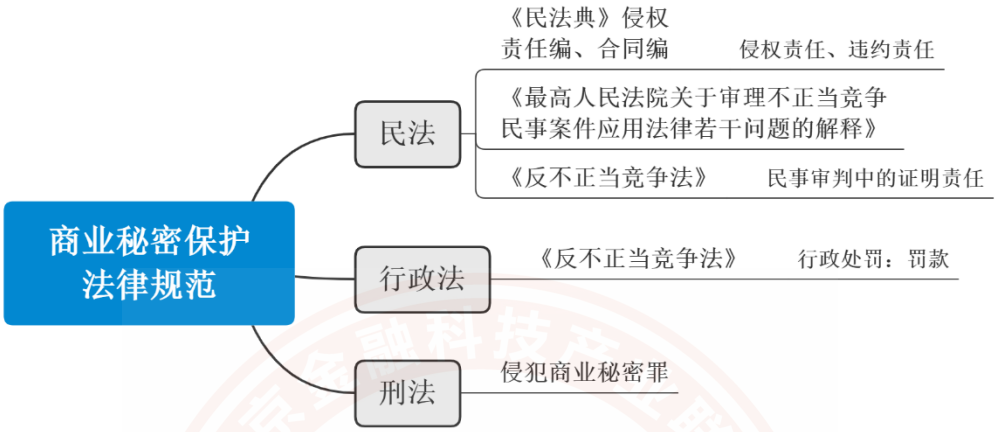

图 2. 商业秘密保护法律规范

4. 关于国家秘密保护的法律框架

国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项，密级分为绝密、机密、秘密三级，不同密级的确定主体、保密措施、保密期限不同。[4]对于国家秘密的保护，法律层面规定于《保守国家秘密法》《刑法》中，具体规定见于行政法规《保守国家秘密法实施条例》、部门规范性文件《国家秘密解密暂行办法》、机关工作综合规定《国家秘密定密管理暂行规定》等。

针对金融领域，原中国银行业监督管理委员会发布了《银行

[4] 《保守国家秘密法》第 2 条、第 10 条、第 13 条、第 15 条、第 21 条。

业金融机构工作中国家秘密范围的规定》（银监发〔2009〕105号），对银行业金融机构工作中的国家秘密范围作出规定并附相关目录。

值得注意的是，即使单个具体金融数据不是国家秘密，统计形成的统计数据、市场预测等信息也可能成为国家秘密。

二、 数据共享在金融业应用的问题

在大数据时代，一方面国家要建设数字经济社会，支持数据开放共享、互联互通；另一方面，数据的交叉比对使反推匿名化后的用户信息变得更加容易，因此，数据开放共享带来的隐私泄露问题，也不得不受到重视。构筑用户数据隐私保护和数据安全保护的屏障，在依法合规前提下实现数据共享，成为金融领域利用数据的重中之重。

隐私计算是指在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合，达到对数据“可用、不可见”的目的；在充分保护数据和隐私安全的前提下，实现数据价值的转化和释放。隐私计算实现了“数据可用不可见，数据不动模型动”、“数据可算不可识，数据可控可计量”、“不共享数据，而是共享数据价值”。隐私计算本质上是在保护数据隐私的前提下获取数据的价值。

大数据联合国全球工作组（Big Data UN Global Working

Group）提出，隐私计算是一类技术方案，在处理和分析计算数据的过程中能保持数据不透明、不泄漏、无法被计算方以及其他非授权方获取。这使得数据所有者可以在不直接共享原始数据的前提下让使用方获得数据计算产生的结果，或者让使用方能从更多来源的数据计算中获得更多更准确的计算结果和数据价值。在整个过程中，原始数据始终掌握和保留在数据所有者手中，不损害数据所有者的权益，而数据潜在价值却被安全地挖掘出来。

然而，基于隐私计算技术实现隐私保护的数据共享，在实际应用中也面临许多挑战与问题。

（一）数据要素确权问题

商品交易的前提是明确商品的产权归属，数据要素交易也是一样。然而，数据作为信息时代人们身份标识、生产生活轨迹、资产和交易簿记的对象和信息载体，其信息主体、数据来源、生成过程、法律属性和内容特点千差万别，很难界定其产权归属。

作为公共事务管理和权利救济机构，相关政府部门、司法机关和行业组织也在日常工作中生成和积累了大量的公共数据，这些公共数据很多从生成目的和基本属性上都具有公共属性，一般认为应当公开、共享，但经过处理加工后又可能产生经济利益和商业价值，由此产生了公共数据与数据产品、数据服务之间的产权划分问题。

数据之间的关联性分析、分类汇总后的统计分析、以数据为

基础的模型构建和修正，不同视角、不同维度、不同方法、不同路径的数据处理，可以得到不同的有价值的结果。一方的数据加工结果可能是另一方的要素来源，为了生产一个数据结果可能需要从多个方向采购数据要素，类似的分析结果可能采用完全不用的数据、算法和路径。隐私计算虽可以使多源数据应用变得便捷和安全。但随着数据要素产业链变得日益庞杂，如何界定数据产业链中不同数据要素、数据中间产品、数据处理服务的产权归属和价值构成，是现有技术无法解决的问题。所以，明确数据要素的产权归属，清晰划分原始数据、数据产品和数据服务的价值构成和权益归属，是构建数据要素市场的首要任务和挑战。

在能够识别界定数据处理行为主体的场景下，确认数据要素归属往往比较容易。然而在联邦学习、多方安全计算等场景下，确认隐私保护计算结果的数据产权归属就可能成为一个问题。多方提供原始数据，共同训练同一个模型，获得的算法模型应该如何确认产权归属、划分未来收益？这可能是一个很复杂的商业谈判问题。另外，权利通常与责任紧密关联。对于数据要素享有收益权、处分权的主体，自然需要对数据要素的合规性、清洁性、安全性承担责任。比如，在合法利用企业用户信息进行纵向联邦计算的场景下，提供数据要素进行模型训练的机构，必须要确保利用相关信息并不违反其与企业用户的相关协议，必须要确保数据安全和真实性。如果企业用户挑战某个联邦学习项目数据处理行为违约或违法，相关数据要素提供方就应当有义务参与相关法

律程序，维护其数据处理行为的合法性。

（二）数据交易定价问题

当前数据要素市场尚未完善，各方机构尤其是金融机构对高质量的数据诉求高，存在数据寡头对数据定价不合理、交易双方存在交易欺诈、交易价格不透明、数据质量难以保证等问题，从而引申出合理定价的必要性。

数据要素不同于其他生产要素，数据要素具有一些独有特性，例如易复制性、可加工性等。易复制性使数据要素的转移成本几乎为零；可加工性使得数据可以以不同的形态出现（如加工标签指标、算法模型、知识策略等），且加工过程中数据不会被消耗，反而能产生更多数据，这也会衍生出数据重新封装后二次倒卖的风险。这就要求数据要素在定价时需在传统定价方法（如成本法、收益法、市场法等）的基础上，融入数据质量维度、数据应用维度、数据风险维度等影响因素。

数据质量维度包含完整性、有效性、一致性、唯一性。其中完整性定义数据关键信息不缺失；有效性定义数据准确且无混杂数据；一致性定义数据间可互相验证；唯一性定义数据主体在业务上的唯一性。

数据应用维度包含数据规模、数据时效、数据稀缺性。其中数据规模定义数据广度和数据时间长度；数据时效定义数据在业务实际应用中的保质期；数据稀缺性定义数据在市场上独占程度

且对特定场景重要。

数据风险维度包含法律风险、道德风险。其中法律风险定义数据可交易的范围（例如，对数据进行分类分级或去标识化等加工后可合规交易的部分）；道德风险定义了数据交易双方中，其中一方未按约定的行为可能会损害另一方利益的风险(例如数据使用方在双方约定的范围之外对数据进行使用带来的风险）。

数据价值与数据质量维度、数据应用维度及数据风险维度皆有相关性。数据交易价值主要体现在三方：数据消费方、数据生产方、数据平台方；数据应用价值更多体现在数据消费方；数据成本或预期价值体现在数据生产方；影响数据价值评估的调用量或偏好量一般在平台方或生产方。如何做好各方信息获取的均衡，利用各方自身信息参与到数据定价中，使数据价值更公允，是亟待解决的问题。

在参与数据协作和联合计算时，各参与方对于数据交易的定价存在分歧。在数据定价方面，同样的数据，对于不同的用户，能产生的价值可能不一样，所以针对不同行业、不同用户应采取差异化定价。但是如何针对同样数据产品具体确定即合理又不同的价格，需要社会各界共同探索。再者，在隐私计算的机制下默认所有参与方都是可信的，无法规避某个参与方恶意提供虚假数据甚至有毒数据，从而对最终的训练模型造成不可逆转的危害。这时候对提供有毒数据的参与方如何索赔或者惩罚，也是需要考虑的问题。

（三）数据交易存证问题

数据要素具有体量大、实时性强、依赖电子介质、易篡改、易丢失等特性，这也使数据要素的流通共享面临存证方面的问题。

传统的存证方式有公证存证、第三方存证、本地存证等，这些方式本质上都是由一方控制存证内容，是中心化的存证方式。中心化存证下，一旦中心遭受攻击，容易造成数据丢失或被篡改。另外，存证原件也容易被单方修改。中心化的存证方式，原件都是基于当事人的凭证（如用户名、密码）下的行为记录，从而带来了操作风险。这种数据逻辑结构下，当事人对自己数据的删改，会使得数据的真实性和完整性存疑，不能保证相关存证的可靠性。

在传统的数据交易与协作模式下，数据源、数据加工方、数据使用方往往是分离的，数据二次交易没有手段稽核与管控，无法实时校验授权的真实性。授权存证可以被任意篡改，不具备公信力，无法确保数据权属的连续性和可追溯性。由于需要相应责任认定条款，每个业务方和数据源机构都需要单独签署协议。此外，查询授权记录需要单独开发接口，提高了数据交易存证的审计成本。

（四）数据交易监管问题

当前我国大数据交易处于快速发展阶段，但由于第三方平台数量较多且平台管理尚未形成统一成熟的机制，以及相关法律法规的缺失，即使是数据交付后也仍会出现当前难以解决的问题。

买卖双方对交付的数据质量产生争议以及如何处理该争端，便是其中较为有代表性的例子。该问题具体表现为当数据交易进入交付阶段时，数据购买方可能对数据质量不满意或者认为该数据未能达到理想效果而拒绝交付，与数据提供方产生交易争端。由于数据产品本身的特殊性，法律制度的不完善，以及技术层面的滞后，当前解决该争端的难度较大。数据质量交易双方无法达成共识，有多方面原因。

首先，数据平台对数据交易方的审核标准参差不齐，部分数据平台供应商的注册门槛较低，材料审核不严（例如仅需提供企业或个人基本信息，对用户资质暂无具体要求），容易导致不良企业在平台上提供低质量的数据，或者出现恶意的数据交易方等现象发生。

其次，数据供应商可能对数据进行夸大或片面宣传，该营销行为可能会误导数据购买者对数据使用效果的期望，增大了争议发生的可能性。

再者，数据平台本身权责不明而且缺乏完善的监管手段和争端处理机制，当争议发生时平台无法有效地保护交易双方的合法权益，这一漏洞可能会滋生某些不良交易者的恶意交易行为。

最后，数据本身的价值多变性与无成本复制性容易导致交易双方在数据作用上的理解有较大差异，以及交易过程中数据退换等售后服务的难以开展，进一步提升了争议发生后平台处理的难度。

（五）数据交易恶意节点问题

在数据交易的过程中，各参与方经常会面临着一系列的问题，其中，参与方是否可信是一个关键性问题，其关系到数据是否安全、模型是否准确、效果是否真实有效等，恶意节点的存在将会威胁数据共享的生态安全，对于恶意节点的识别、防范、处理等，均存在一定程度上的困难。

数据交易实质上是对数据价值的共享，而数据的价值的流通离不开隐私计算技术。在隐私计算技术中，根据参与方的可信程度可以建立以下几种安全模型:

Real-Ideal Paradigm（理想模型）：在理想模型中，每一个参与方都是可信的，一方将其信息发送给另一方，另一方不会去查看这份信息，只会根据规定计算出结果，并发送给下一方或者所有参与方。

Semi-Honest Security（半诚实模型）：半诚实模型就是参与方会诚实的运行协议，但是他会根据其他方的输入或者计算的中间结果来推导额外的信息。

Malicious Security（恶意模型）：恶意模型则可能不会诚实的运行协议，甚至会搞破坏。

在现实世界中，没有绝对的信任的前提下，理性模型是不存在的，多数情况是各参与方之间会基于半诚实模型，甚至是恶意模型。恶意节点就存在于上述两个模型中，威胁着正常的业务合

作。

1.恶意节点的危害

恶意节点作为隐私计算参与成员，可能通过诸如以下几种方式参与作恶:

下毒攻击:以数据或模型投毒的方式污染或者破坏模型的训练数据或者模型本身，从而达到攻击目的。

拜占庭攻击:拜占庭恶意参与方会随机或者故意改变自己的输出，致使模型无法正常收敛，同时每次迭代可以输出类似的梯度更新结果，使得自己难以被发现。

女巫攻击:攻击方伪装成多个隐私计算参与方节点攻击模型训练过程，导致模型效果显著降低。

2.恶意节点探查难点

参与方如果作为恶意节点，对其的探查存在以下难点:

（1）定义和发现作恶行为

因隐私计算对比传统数据合作最大的不同是原始数据不共享,在不获得原始数据的前提下,如何对参与方的行为予以审查,对隐私计算的结果予以评估,进而发现某参与方的恶意行为和目的，是难以解决的问题。

（2）相关的处罚和后期的规避措施

发现恶意节点的违规的行为后，必须配备相关的政策和措施，一方面是针对恶意节点予以惩罚，增加其后续的信任成本；另一方面是针对所发现的违规行为，制定相应场景下的规避方案。

（3）构建隐私计算生态的“恶意节点库”

金融黑名单对行业的风控场景具有重要意义，因此，恶意节点库的构建也具有很强的必要性。通过构建隐私计算的恶意节点库，可以促进隐私计算生态的健康发展，帮助隐私计算技术做到科技向善。

（六）可信第三方的“权责利”界定问题

本文的可信第三方指在数据要素流通（隐私计算）过程中与数据提供方和数据使用方（结果获得方）并行存在的一方，其一般不提供数据、不应用数据（接收计算结果），对数据本身没有控制权，其可以行使管理、服务、辅助计算等职能。

由于可信第三方的权威和中立地位，其不宜直接承担数据提供方和数据使用方这种和数据流通利益相关的角色。在实际应用中，通常难以找到足够公信力的机构来承担可信第三方的角色。

当可信第三方为隐私计算提供算力时，可实时监控数据流，防止数据以明文的形态进行交易流通，对监管需求容易达成。如果可信第三方不承担算力，则需要对外部计算节点的计算过程进

行审计，进而实现监管要求。因此，在隐私计算中，如果可信第三方提供了算力，承担了辅助计算的功能，那么该如何对其监管，以及界定其对数据价值流通过程中的“权责利”，也是棘手的问题。

三、 隐私计算技术与区块链结合的探索

区块链本质上具有去中心化、不可篡改、不可伪造等特性，可以有效解决无第三方背书情况下的信任问题。区块链技术在数字货币、金融交易结算、数字政务、数据服务等其他应用场景同样具有广泛的应用需求。

基于其上述特性，区块链可以对数据从产生到处理、从交易到计算的全生命周期进行记录和存证，保证过程的可验证和可信。进一步来说，区块链技术对隐私保护数据共享中所存在的挑战，例如数据确权、数据定价、交易存证、交易监管以及恶意节点探查等问题提供了技术层面的解决思路。

（一）区块链技术概述

1. 政策与标准

在政策层面，我国政府已将区块链技术作为战略性前沿技术进行前瞻布局。在《国务院关于印发“十三五”国家信息化规划的通知》《国务院办公厅关于积极推进供应链创新与应用的指导

意见》等政策性文件中多次提到要加强对区块链技术的创新研究及产业引导，鼓励地方政府出台优惠政策推动区块链技术的研究和落地。中国人民银行、国家网信办等部门先后出台了《关于防范代币发行融资风险的公告》《区块链信息服务管理规定》等文件，为区块链技术的使用和管理等提供了有效的法律依据，推动了我国区块链相关领域管理规定的细化落实。

在标准方面，中国人民银行发布了《区块链技术金融应用 评估规则》《金融分布式账本技术安全规范》行业标准，规定了在使用区块链技术的技术安全要求及评估方法，促进区块链技术在金融行业安全稳妥应用；北京金融科技产业联盟、中国信息通信研究院等也发布了区块链相关的团体标准；国际上，ISO/TC 307（区块链和分布式记账技术委员会）于 2016 年 9 月成立，旨在推动区块链和分布式记账技术领域的国际标准制定等工作，目前已发布多项国际标准。区块链技术相关标准详见表 1。

表 1 区块链技术的相关标准

时间	机构或组织	标准
2022 年 2 月	中国人民银行	《金融分布式账本技术安全规范》
2020 年 7 月	中国人民银行	《区块链技术金融应用 评估规则》
2021 年 4 月	北京金融科技产业联盟	《区块链技术金融应用 技术参考架构》
2020 年 7 月	中国信息通信研究院	《区块链辅助的隐私计算技术工具-技术要求与测试方法》
2019 年 11 月	W3C	分布式身份标识（Decentralized Identifiers ，DIDs）规范的首个公开草

		案
2020 年 8 月	ITU-T	《分布式账本技术平台测试准备》(Assessment criteria for distributed ledger technology platforms) 《分布式账本系统要求》(Requirements for distributed ledger systems)
2020 年 12 月	IEEE	《区块链系统的数据格式标准》
2021 年 4 月	ITU-T	《DLT 平台功能测试方法》（Function assessment methods for distributed ledger technology (DLT) platforms） 《DLT 平台性能测试方法》 （Performance assessment methods for distributed ledger technology (DLT) platforms） 《DLT 互操作技术框架》（Technical framework for DLT interoperability）

2.技术体系

区块链（Blockchain）最早在 2008 年被提出，本质上是一个去中心化的分布式账本（Distributed Ledger）技术。具体来说，区块链技术是采用块链式数据结构验证与存储数据、通过分布式节点共识算法生成和更新数据、利用密码学方式保证数据传输和访问的安全、并使用自动化脚本代码组成的智能合约来操作数据的一种全新计算范式。

区块链通常涉及以下基本因素:

交易（Transaction）：指使区块链分布式账本状态改变的

一次操作，如添加一条记录或者是一笔在两个账户之间的转账操作。

区块（Block）： 用于记录一段时间内发生的交易和状态结果。区块通常用区块头的哈希值和区块高度来进行标识。

链（Chain）： 由一个个区块按照发生顺序串联而成，是整个状态变化的日志记录。

常见的区块链技术体系如下图所示，从下往上依次分为数据层、网络层、共识层、激励层、合约层、应用层。

数据层： 包括了数据的存储结构、存储方式等，区块链作为节点共享的数据账本，任何分布式节点都可以将一段时间内接收的交易数据记录到区块中，并将该区块添加到区块链中，形成新的区块链。

网络层：包括了系统的 P2P 分布式组网方式、消息传播协议、数据验证机制以及节点许可接入机制等要素，系统可以根据应用场景的不同需求进行特殊设计；

共识层： 主要作用是使用共识机制，使各节点在去中心化的区块链网络中能够快速达成一致，维护共用的账本；

激励层： 主要作用是利用数字货币完成区块打包奖励、交易费用的收取等；

合约层：主要作用是负责将区块链系统的业务逻辑以代码的形式实现、编译并部署，完成既定规则的条件触发和自动执行，最大限度的减少人工干预；

应用层：主要作用是调用智能合约接口，适配区块链的各类应用场景，为用户提供各种服务和应用。

常见的区块链技术体系如图 3 所示。

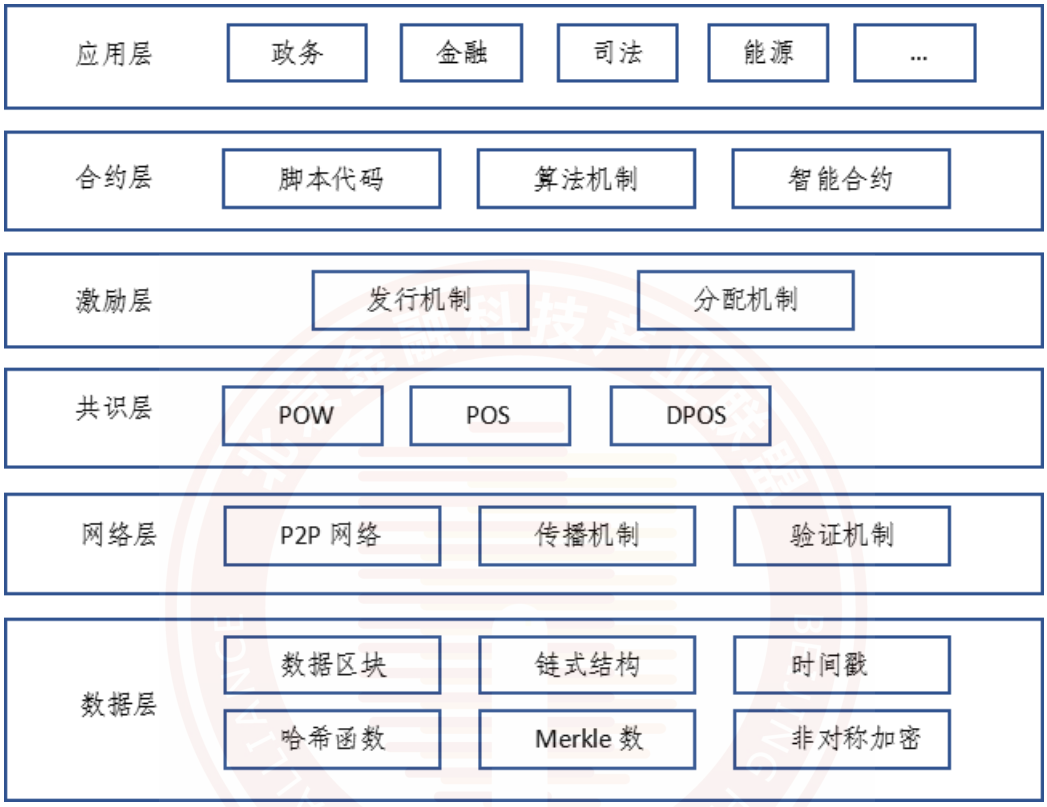

图 3. 常见的区块链技术体系

3. 关键技术

区块链由多种传统技术创新整合而成，包括分布式存储、密码学、对等网络、共识机制、智能合约等。

（1）分布式存储

传统分布式存储一般指将网络中分散的各个节点的存储资

源构成一个虚拟的存储设备，数据分散存储在网络中的各个节点中。区块链不同于传统的分布式存储，各参与节点拥有完整的数据存储，并且各节点是独立、对等的，当其中一个节点的数据发生变化时，其他节点的数据也会被同步。分布式存储架构不仅提高了区块链系统的健壮性，同时也加大了对链上数据进行篡改难度，实现了防伪认证和交易溯源的要求。

（2）密码学

区块链的安全主要依赖于密码学技术。密码学为区块链数据的不可伪造、不可篡改、可公开验证和隐私保护提供了基础保障。区块链中使用了哈希算法、加解密算法、数字证书与签名、零知识证明、同态加密等现代密码学的多项技术。

哈希算法：被用于生产区块链中各个区块的头信息，并通过在区块头中包含上区块头信息的方式来实现区块之间的连接。

加解密算法：根据加解密过程中使用的密钥是否相同，可分为对称加密和非对称加密。区块链主要应用非对称加密算法实现数据加密、登录认证等。

数字签名：可以证实某数字内容的完整性并确认其来源，实现链上数据的不可抵赖。区块链中采用的数据签名技术包括盲签名、多重签名、群签名、环签名等。

零知识证明：指在证明过程中不向验证者透露任何内部信息即可以获得希望的证明结果的过程。使用零知识证明技术可以实

现区块链的匿名性，将交易双方的敏感信息或隐私信息隐匿起来。

同态加密：加密后的密文可进行计算，计算结果解密后与基于明文数据的计算结果一致。使用同态加密技术，可以使得区块链上的智能合约等以密文方式进行处理，提高区块链的隐私安全性。

（3）对等网络

对等网络技术是区块链系统组建多参与方网络的技术基石。其具有去中心化、可扩展性、健壮性、隐私保护、负载均衡等优点。此项技术通过分布式计算模型完成数据的集体共享与维护。其中每个节点的参与者都可根据自己的需求和权限范围直接获取信息，而不需要中间平台传递。在整个对等网络系统中，没有居于主导地位的管理机构或单一的控制主体，节点彼此之间的地位完全平等，丢失任一节点对整个网络系统的运行没有影响。

（4）共识机制

共识机制是保证分布式系统所有参与者之间数据正确性和一致性的解决方案。其核心是在有限的时间内和某个协议（共识算法）保障下，使得指定操作在分布式网络中被所有节点一致承认。在区块链系统中，只有能够影响分布式网络中大多数节点时才能实现对已有数据的篡改。常见的共识机制包括:工作量证明/POW(Proof of Work)、权益证明/POS(Proof of Stake)、股份

授权证明/DPOS(Delegated Proof of Stake)、拜占庭容错(PBFT/RBFT)类 BFT 共识协议、RAFT 共识协议等。

（5）智能合约

智能合约可视作一段部署在区块链上可自动运行的程序，该程序能保存价值、存储数据、封装代码和执行计算任务。智能合约利用代码自动执行合约后端流程，包括托管、维护和触发等。一旦合约代码完成并发送至区块链，相关交易会严格按照合约代码执行。智能合约利用协议和接口完成合约过程的所有流程，都允许用户根据不同的业务需要在实现个性化定制。智能合约技术的应用有利于避免交易过程中的人为干预，提升工作效率。

4.技术分类

根据系统是否具有准入机制，区块链系统可以分为无许可的和有许可的区块链，前者被称为公有链（Public Blockchain），后者被称为许可链，许可链又可进一步分为私有链和联盟链。区块链分类对比如表 2 所示。

公有链：链上数据公开、透明，只要达成共识，将无法篡改。

私有链：其对读取权限或者对外开放权限进行了限制，一般应用于一个组织或团队内部，无需解决所有节点的信用问题，只需获得关键节点的信任，私有链具有更快的交易速度、更低的交易成本、更好的隐私保护等。

联盟链：介于公有链和私有链之间，是由多个特定的企业或

组织共同建立的区块链。每个节点通常对应一个实体机构组织，联盟链的数据只限于联盟内的机构有权进行读写与发送。联盟链具有成本较低、效率较高的特点，同时可以满足不同实体间的交易或协同需求。

表 2. 区块链分类对比

	公有链	联盟链	私有链
是否许可链	否	是	是
参与者	无限制	联盟成员	团体或公司内部
记账人	所有参与者	联盟成员协商决定	自定义
中心化程度	去中心化	多中心化	弱中心化
规模	全球性	多个企业、多个行业	一个企业、一个组织
交易速度	慢↓	快↑	快↑
信任度	低↓	高↑	高↑
可扩展性	低↓	高↑	高↑
交易数据	公开、透明	非公开	非公开
数据可篡改性	否	是	是
特点	信用的自建立	效率 vs 成本的优化	透明和可追溯性
网络	P2P 网络	高速网络	高速网络
典型场景	虚拟货币	支付、结算	审计、发行
代表链	比特币、以太坊、疫苗研发/生产/销售全过程	R3、超级账本、EEA、BSN	历链

（二）区块链技术金融应用现状

1.应用概况

根据 IDC 发布的《2021 年 V1 全球区块链支出指南》(2021)，2024 年全球区块链市场将达到 189.5 亿美元，五年预测期内（2020-2024）实现约 48.0%的复合增长率。而中国区块链市场规模五年的年均复合增长率（CAGR）将达到 54.6%，增速位列全球第一，其中第一大支出方向便是金融。据赛迪网统计，2019 年我国区块链应用落地项目 328 个,其中金融区块链应用落地项目 96 个，占比 29%。在同期应用落地项目中占比最高，较 2018 年同比增长 41%。

金融行业具有交易复杂、交易涉及主体多、业务链条长、交易频次高等特点，面临着诸如跨境支付周期长、费用高，结算环节效率低下，风险控制代价高以及数据安全隐患大等问题。区块链技术应用于金融行业，可以有效解决交易信任、价值流通等问题，降低金融交易成本、提高金融运行效率、提升金融监管和审计便易性。

金融也是区块链技术应用场景中探索最多的领域，除了数字货币，在供应链金融、贸易融资、支付清算、资金管理等细分领域均有具体的项目落地。国内从中国人民银行、大型股份制商业银行到城商行，相继部署了区块链应用。据工行金融科技研究院不完全统计，区块链金融应用情况如图 4 所示：

企业	基础平台	资金管理	供应链金融	贸易融资	支付清算	数字资产			延伸领域				
						ABS	票据	其他	数字存证	溯源	住房租赁	数字发票	电子证照
工商银行	•	•	•	•		•	•		•	•			
农业银行			•										
中国银行			•	•		•	•	•					
建设银行			•	•							•		
交通银行						•							
邮储银行		•		•									
招商银行				•	•	•						•	
平安银行	•		•	•									•
浦发银行							•		•				
度小满	•					•	•	•					
蚂蚁金服	•				•		•		•	•	•		
微众银行	•				•				•			•	
京东数科	•		•			•			•	•			

图 4. 国内金融区块链应用情况（部分）

2.应用场景

金融行业是区块链技术应用最广泛的行业之一。区块链在金融行业中的应用场景较其他行业更加广泛和深入，可应用于供应链金融、贸易融资、资金管理、数字资产等环节，并可为质押、融资、项目管理等环节提供可信平台服务。

当前区块链在金融的应用场景大体可以分为两类，基于金融数字货币和金融业务衍生的应用场景。

（1）金融数字货币应用场景

在所有的中国人民银行数字货币中，有80%以上采用分布式账本技术DLT（Distributed ledger Technology）作为基础承载。众所周知的比特币、以太币等以企业为主体的虚拟货币，均依托于区块链技术。

（2）金融业务衍生应用场景

供应链金融：基于区块链技术实现供应链上下游的信用穿透，为上游多级供应商解决融资难、融资成本高的问题。

贸易融资：基于区块链技术打造多机构参与的贸易融资平台，将交易过程中的货物、单据、物流、监管信息等数据流上链，让真实世界中的货物信息与电子单据信息进行相互验证，满足企业对在途和仓储实物商品融资的需要。

资金管理：应用智能合约技术的工作流引擎，通过灵活配置

资金审批流程，实现资金申请和审批支付自动执行，从而大幅提升资金管理和支付效率。

数字票据：依托区块链技术实现端到端透明化流程，解决票据业务中人工介入较多、交易需要第三方认证的问题，降低了操作风险，简化了交易流程，提高了交易效率。

机构对账：由多个机构共同建立一条联盟链，每个机构均拥有自己的节点，节点之间互联，每个节点都拥有全量数据，由区块链技术保证数据的最终一致性。并且，利用区块链智能合约确保数据处理逻辑的可信和可审计。

智能证券交易：在证券交易领域，应用区块链分布式账本技术，可以使交易过程公开、透明且不可更改；区块链技术的点对点交易模式，能够减少交易双方的信息障碍，降低交易风险；智能合约技术减少繁复的传统交易结算过程，提高交易效率。

保险智能化：区块链保险服务平台可对投保人信息快速整合、分析和审核，通过智能合约技术实现理赔自动化，从而实现区块链赋能保险行业。

（三）隐私计算与区块链结合可行性分析

隐私计算是以多方安全计算、同态加密、联邦学习和可信执行环境等为代表的现代密码学和信息安全技术，在保证原始数据安全隐私性的同时，完成对数据的计算和分析，实现数据的“可用不可见”。隐私计算保障了计算过程中原始数据的隐私安全，

但不可忽视的是，隐私安全的保护只是实现数据合规共享流通中的一环。在数据的流通与共享过程中，还存在着如前文所述的数据确权、数据定价、数据交易存证监管、数据交易恶意节点探查等问题，这些问题恰恰是隐私计算所不能解决的。想要让隐私计算中数据更高效、安全地互通互传，需要引入更多的安全机制。

利用区块链的去中心化、不可篡改、不可伪造等特性，可实现数据溯源、智能合约自动执行等能力，恰好可以提供隐私计算过程中数据全生存周期的全闭环管理，使过程更加安全、可信。

1. 匹配程度分析

隐私计算和联盟链的匹配程度可理解为研究隐私计算与区块链技术的相融度问题。下面将通过双方的网络拓扑、技术特性等方面进行探讨。

（1）网络拓扑与技术特性分析

网络拓扑分析：无论是隐私计算还是联盟链，他们的初衷都是解决在没有第三方可信机构的前提下如何合作共营的问题。因此，当使用这两项技术时，可以将他们都设计成分布式架构，如图 5 所示。

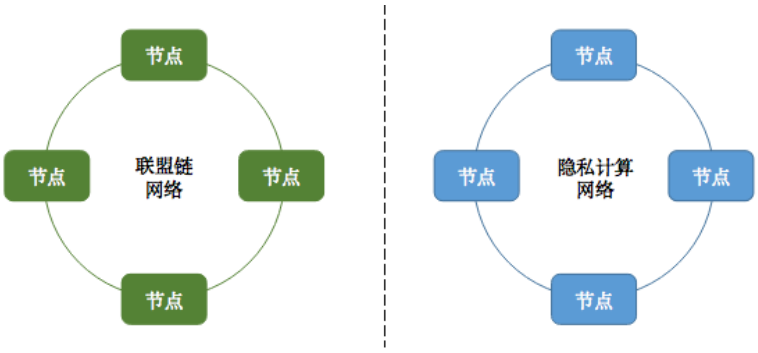

图 5. 联盟链与隐私计算的网络拓扑

在联盟链中，参与方拥有的节点一般称为区块链节点，他们之间组成的网络称为区块链网络；同理，在隐私计算中，参与方拥有的节点一般称为隐私计算节点，他们之间组成的网络称为隐私计算网络。

技术特性分析：在联盟链中，每个参与方拥有一个或多个区块链节点，这些节点可能承担共识、记账等工作。他们利用共识算法等机制保证节点间的最终一致性，利用哈希链状结构、冗余账本保证数据防篡改与可溯源，从而保证数据在链上是可信的。

在隐私计算中，每个参方拥有一个或多个隐私计算节点，这些节点可能承担计算、协调、数据提供、数据授权等工作。他们利用密码学算法、安全通信协议等技术，在不泄露数据隐私的前提下保证计算结果准确无误，计算过程安全可信。

综上所述，在技术特性方面，联盟链技术与隐私计算技术所关注的内容是不同的。前者侧重的是数据存储的存储可信性，而后者侧重的是数据计算过程的隐私性，详见表 3。

表 3. 联盟链技术与隐私计算技术特征对比表

	联盟链技术	隐私计算技术
数据存储可信性	通过哈希链状结构、共识算法、冗余账本等机制确保数据存储是可信的。	需要诚实的参与方提供数据。
数据计算隐私性	联盟链技术不支持数据运算，只能通过智能合约层面实现计算逻辑，且需要叠加其他技术保证数据的隐私性。	通过密码学算法、可信硬件等技术保证计算过程隐私性，在不泄露隐私数据前提下，计算结果准确无误，计算过程安全可信。

（2）隐私计算与联盟链的互补性

联盟链介于公有链与私有链之间，是多个组织或机构参与的区块链。即：联盟链是由多个私有链组成的集群，由多个机构共同参与管理的区块链，每个组织或机构管理一个或多个节点，其数据只允许系统内的机构进行读写和发送。联盟链具有准入机制，仅限特定某个群体的成员和有限的第三方参与。数据提供方和使用方等须经过资质审核后才能加入，且必须遵守约定的数据流通规则。联盟链还可以通过分级的权限控制及预先设定的智能合约更好地规范数据流通行为，进一步保障链上数据合法合规。

联盟链的运行机制与多方机构联合起来完成一个隐私计算任务的过程有很高的契合度。联盟链在数据授权、存证和交易记账方面有着天然的优势，能解决隐私计算所存在的数据难验证、交易难溯源、多方难互信、多方难协作等问题。联盟链使得隐私

计算过程可验证、可溯源、可信任、易实现多方协作。业内专家普遍认为，联盟链将成为隐私计算产品的标配。

（3）匹配程度总结

在网络拓扑方面，两者都是分布式架构；在技术特性方面，隐私计算与联盟链技术并不冲突，而是相辅相成、相互补充。此外，隐私计算与区块链去中心化的特性，以及解决数据安全问题的终极目标相匹配，但双方的实践方式有所不同。隐私计算保证的是数据的隐私性，而联盟链保证的是数据的一致性和可验证性。

两项技术的配程主要表现在以下三个方面:

数据流动和保护的统一。区块链构建全网统一账本，通过交易实现信息流动。隐私计算则实现数据隐私保护，为数据价值流动提供技术支持。

分布式体系架构的统一。区块链是分布式体系架构，各方自治协作保障事务一致性。隐私计算同样是分布式体系架构，各参与方通过协同计算完成数据价值的共享。

生产力与生产关系的统一。区块链构建参与方之间一致、稳定的生产关系。隐私计算则构建数据要素价值流通的规模化生产的生产力。

2.应用价值分析

在隐私计算应用中引入区块链技术，可凭借其去中心化、不可篡改、不可伪造等特性，针对性地建立起隐私计算所需的信任

桥梁，满足隐私计算过程透明监管的需求。

基于区块链技术，数据在计算、流通、使用、销毁等多个环节中，都可以做上链验证和保存，其记录可以结合相关管理手段对数据确权和定价做出有效参考；隐私计算的中间流通结果，可以通过智能合约进行验证，判断其有效性，防止计算过程中发生主观作恶行为，防范恶意节点的攻击；链上的记录公开、透明、不可篡改，可以满足数据溯源，为审计监管提供协助；签名算法的应用可以确保参与节点的真实可信。

在隐私计算无可信第三方参与的情况下，所有参与方可以在链上用智能合约来实现计算过程协调的相关功能需求，由参与方之间共同治理隐私计算过程，公开透明，权责对等，避免了中心化协调方参与带来的隐私泄漏的风险。

区块链技术和隐私计算技术的融合应用，能够很好满足未来大规模数据流通的安全、可信、可控需求，二者结合可共同构建一个算前、算中、算后的可信、可审计的数据要素流通系统。

计算前：可利用联盟链技术的防篡改性保证计算数据的真实性、一致性；

计算中：可利用隐私计算技术确保参与运算数据的隐私性，以及运算结果的准确性；

计算后：可利用联盟链不可篡改、不可伪造的凭证记录，实现监管机构对计算过程的审计、审查。

综上所述，隐私计算技术和区块链技术在数据合规共享应用

这一场景下，很大程度上做到了能力互补。既能在数据共享过程中有效保护数据的隐私性，实现数据的安全流通，又能为数据的真实性、数据确权等合规问题提供帮助，实现全流程可记录、可验证、可追溯、可审计，解决了双方技术在单独使用时面临的难点问题，达到“1+1>2”的效果，为建设高效、安全的数据要素市场提供技术基础。

四、 基于联盟链的隐私保护数据共享架构

（一）参与方角色

在基于区块链的隐私计算架构中按照承担的角色可以分为发起方、数据方、算法方、计算方、结果方、协调方、区块链能力提供方。在这种基于区块链的隐私计算中，一个参与方可以承担多个角色。

1.发起方（initiate parties）： 隐私计算任务的创建方，对任务进行启动执行、监控状态的参与方;

2.数据方（data parties）： 提供隐私计算任务所需私有数据的参与方;

3.算法方（algorithm parties）： 提供隐私计算算法（计算逻辑、参数等）的参与方;

4.计算方（computing parties）： 为执行隐私计算任务提供算力的参与方;据情况会按照多方安全计算协议或者联邦学习

的规则执行计算。

5.结果方（result parties）：获得隐私计算任务全部或者部分结果的参与方;

6.协调方（coordinate parties）：管理协调隐私计算任务配置和执行的参与方，非必要角色;

7.区块链能力提供方（blockchain service parties）：作为提供区块链服务能力的参与方,提供链上合约执行、数据存储、验证及多方共识服务。其中,区块链能力提供方并非指单一实体,可进一步包括区块链共识节点、记账节点等。

（二）双层框架

隐私计算加联盟链可采用链上链下双层异构框架(见图6)。其中链上层主要指区块链网络层(实现基于区块链的验证、审批、审计、存证、协调等)，链下层主要指隐私计算层。区块链网络以联盟链为主要形态,通过点到点的节点连接、全网分布式共识、不可篡改链表结构，构建统一的分布式账本，存储隐私计算网络所需保证一致性、可追溯性的关键数据。隐私计算层由数据节点、计算节点、服务节点等多种类型节点组成。数据节点和计算节点可以由同一实体节点来承担,也可以采用基于有代理计算节点的计算节点与数据节点分离模式。同时隐私计算网络可以是对等网络、星型网络、混合网络等不同网络拓扑结构，通过不同形式网络连接，实现基于隐私计算的数据价值流动。

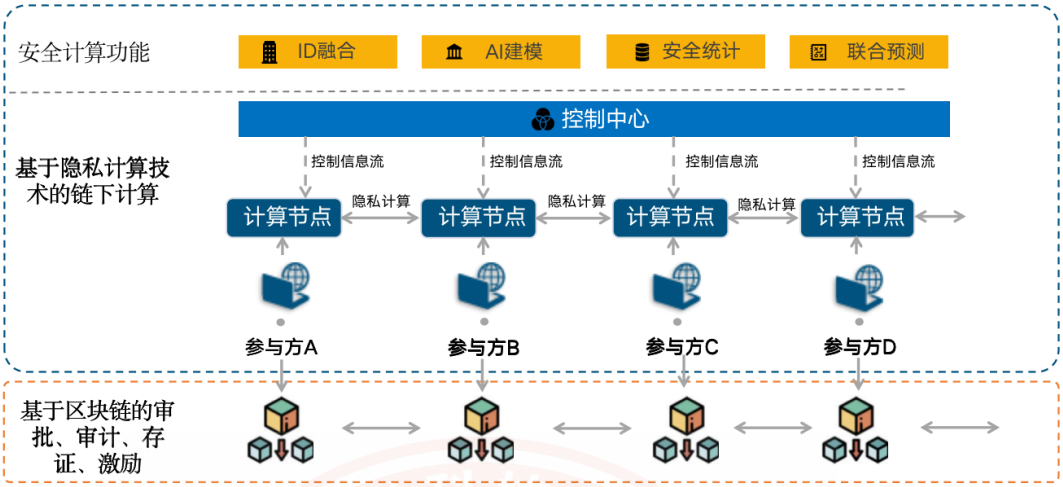

图 6. 基于区块链的隐私计算框架

在基于联盟链的隐私计算框架中，所有的参与方是经过所属联盟同意并授权的可信任的参与方。每个参与方都是一个联盟链的节点，他们可以在区块链中记录隐私计算的关键信息，例如原始数据集的哈希值、任务 ID、任务执行时间、任务执行日志、结果集的哈希值、关键中间结果的哈希值等。联盟链中拥有权限的成员们可对所有任务进行审批、审计和存证。

图 7 是区块链能力提供方的技术架构，主要分为六个层次：物理资源层、区块链层、基础服务层、核心服务层、接口层、应用层。

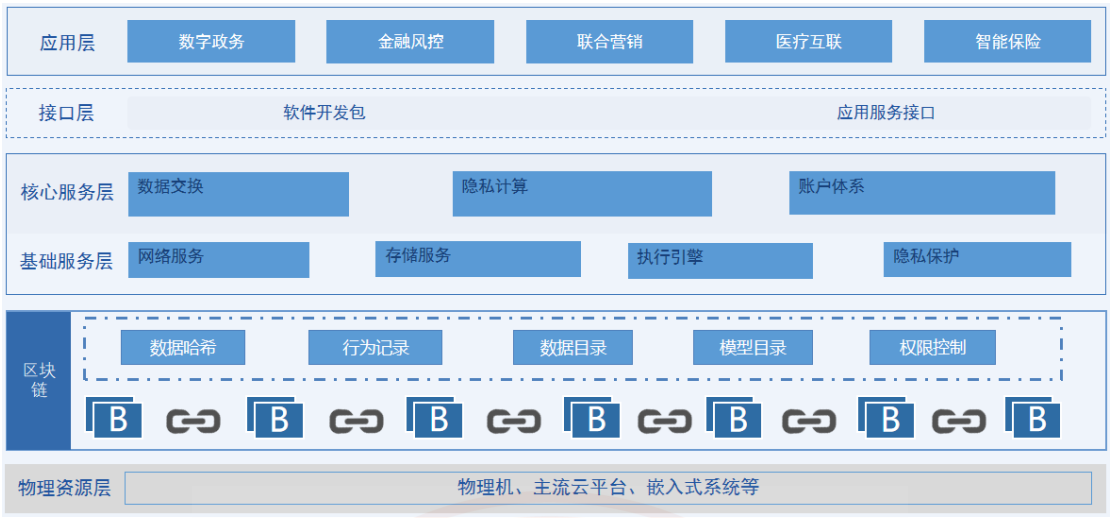

图 7. 技术架构图

物理资源层：是链下协作节点所依赖的物理基础资源，链下协作节点可以直接部署在通用物理机，也可以部署在如华为云，阿里云、腾讯云、微软云等云平台。

区块链层：由各个业务参与方本地部署的区块链节点构成，包括物理节点和智能合约。智能合约中主要定义了数据目录、模型目录、业务规则、权限控制规则等。

基础服务层：是链下协作节点的基础支撑，网络模块提供了链下协作网络中节点之间的互联互通能力；存储模块提供了单一节点的存储能力；执行引擎是智能合约的运行空间，通过沙盒化的形式运行动态可加载的数据或者业务模型。

核心服务层：是链下协作节点功能的主要体现，核心服务层由数据交换、隐私计算和账户相关操作组成。其中，数据交换模块使用本地资源管理、点对点数据传输、数据权限管控及数据共

享统计分析，进行全链路数据隐私保护前提下的分布式数据共享。链下形成点对点数据隐私计算网络；链上实现细粒度权限管控和全流程数据跟踪记录，实现数据使用可追溯、流转可审计。隐私计算模块通过使用多方安全计算，联邦学习以及 TEE 等技术提供多方联合求交、多方联合统计、多方联合建模、多方联合预测、多方安全查询等隐私计算能力，同时集成 LuaVM、WASM 等高性能虚拟机支持分布式可编程计算环境，通过隐私计算和可编程机制对外提供灵活的跨机构可编程隐私计算服务。

接口层：是链下协作节点和应用层之间的连接器，主要提供外部应用层访问链下协作节点的接口。他提供软件开发包 SDK 和 API 服务两种连接方式。

应用层：基于链下协作节点构建的分布式数据协同应用服务。

（三）运作机制

1.分布式数字身份

数字身份的发展，经历了中心化身份、联盟身份、以用户为中心的身份、以及去中心化身份四个阶段。传统中心化的数字身份由于容易出现身份信息泄露、信任成本高等问题，已经难以满足现阶段的数字经济发展需求。在政策、技术、市场因素的共同驱动下，产生了一种新的数字身份形态—分布式数字身份(Distributed Identity-DID)。他用分布式基础设施改变了应用厂商控制数字身份的模式，让用户控制和管理数字身份。通过将

数据所有权归还用户的方式从根本上解决隐私问题。

要使身份具有真正的自我主权，这种基础设施必然需要驻留在分散信任的环境中。区块链技术的出现让自我主权身份的实现终于找到了突破口，作为分布式体系里的代表性技术，区块链有望成为分布式数字身份的技术基础。哈希链的数据结构改变了电子数据易被篡改的属性；“区块+共识算法”解决了分布式系统的数据一致性问题；拜占庭容错能力保证了跨实体运行的系统不受少数节点恶意行为的影响，从而解决业务层面的信任难题，有望在服务商之间搭建互联互通的协议。

当前，不同机构间存在着大量用户数据流通的需求。然而，由于各个机构之间通常难以组建有效的信任合作机制，因此，各机构间难以将各自保管的用户数据安全可信地授权共享给其他机构。通过 DID 解决方案，可帮助机构间进行可信数据授权及共享，使得各机构可基于全面的数据为用户提供更高质量的服务。同时，由于分布式数字身份实现了用户直接对数字身份的管理，可以使得数据所有权与用户的强绑定，进一步帮助解决数据共享流通中的数据确权问题。

参与方包含用户，数据持有机构，数据使用机构，身份证明机构。解决方案及基本流程为：

（1）在身份证明机构、数据持有机构、数据使用机构间搭建区块链网络，机构作为节点接入并注册 DID；

（2）由身份证明机构为用户进行 KYC 并生成 DID；

（3）用户授权数据使用机构使用自己的数据;

（4）由身份证明机构为用户生成授权凭证(Credential)，标明授权对象、数据属主、有效期、授权内容等属性，并使用用户私钥进行签名，身份证明机构可选择将授权凭证生成摘要并写入区块链，达到增信目的;

（5）数据使用机构出示授权凭证给数据持有机构;

（6）数据持有机构通过凭证验证（Verify）接口，验证授权凭证;

（7）验证通过，数据持有机构将数据发送给数据使用机构。

2.基于区块链的群体激励机制

隐私计算技术通常用于解决多方协同计算的数据安全、隐私保护的问题。由于其两方或多方协作特点，参与各方需要按照相同的协议和规则执行，执行过程中的记录需要进行多方同步，协同产生的成果以及后续的收益需要通过互利共赢的模式进行分配。隐私计算多方往往依靠半诚实的安全模型，需要相互之间有较高的信任。对于这样一个复杂的多边关系，如果信任成本太高、合作摩擦系数太大，将导致合作无法建立，或者合作范围太小，无法达成规模效应，难以发展壮大。而区块链恰好适合多边信任关系的建立。由于是机构与机构之间的合作，因此可以选择联盟链来建立保护隐私的群体激励机制。

在隐私计算的协同生态系统中存在多个节点角色，包括服务

需求方（如金融机构）、数据贡献方、算法技术贡献方、建模贡献方、算力贡献方。联盟链可以部署多个标准化的智能合约，包括加密存证合约、元数据服务合约、协同学习服务合约、算法服务合约、算力服务合约、贡献激励合约、安全审计合约等。每一个节点可以根据自己的角色和需求，加入智能合约，也可以在标准化智能合约基础上，派生个性化的新合约。成果利益分配规则可以在链上约定，操作记录也可以在链上记载，实现加密存证，可信分配。

区块链在隐私计算的数据提供、结果查询、算力支持等环节，按各参与方的贡献量或消费量对与之捆绑的区块链节点账户进行数字 token 的奖励或惩罚，以此激励各节点贡献数据、模型或算力。具体可细分为贡献量计算和消费量计算:

（1）贡献量按各数据提供的数量和维度、参与方本地数据对最终模型效果的影响占比、每天计算参与次数等综合进行计算。

（2）消费量按每天数据查询次数、计算任务发起轮数等进行核算。

3. 可信协调方

隐私计算解决的是数据的隐私安全问题，虽然实现了在多方协作计算过程中对于输入数据的隐私保护，但是原始数据、计算过程和结果均缺乏可验证性。而且部分隐私计算的解决方案需要依赖第三方协调方来完成计算任务，而实际应用中难以找到足够

公信力的第三方来承担这样的可信协调方角色。

区块链是一种由多方维护，使用密码学技术保证数据传输安全和数据一致性、防篡改性的分布式账本技术。因此隐私计算可以利用区块链充当可信协调方，通过使用链上数据流通、链下数据计算的方式，来合理分配链上链下的计算能力和安全能力，从而高效可信地协调业务流程和计算过程，降低了多节点间大规模复杂计算的部署和使用成本。

（1）业务流程协调：数据持有者将共享数据目录、数据使用申请、数据使用审批、数据使用审计等功能在区块链上完成，利用智能合约技术来对业务自动化处理逻辑进行实现，提升数据共享流通、业务有序运转的协作效率。

（2)计算过程协调:针对一些特殊隐私计算技术进行协调。例如零知识证明，其证明过程计算性能低、算力消耗大，相比之下验证过程更加简洁，但需要各方的高度信任才被接受，因此采用链下计算链上验证的方法。由发起方先在链下计算出证明内容，利用硬件加速、可信执行环境、算法优化等手段来提升计算效率；接着将证明传递到区块链上的接收方节点，在链上验证该证明内容的正确性。在区块链上各节点的监督下，接收方给出的验证将更具有公信力和说服力。

（3）协调方可将关键信息和关键计算节点通过区块链进行可信存储。比如将任务配置信息上传至区块链，将各方无异议的计算合约上链，以及将任务最后的结果状态（执行是否成功）上

链等。

4. 数据目录共享及权限控制

基于区块链的目录共享是一种新型的数据共享，各参与机构将需要共享的数据资源进行编目，并发送到区块链的共享账本上。各参与机构之间构建起基于区块链的可信数据共享网络，后续基于这个区块链可信数据共享网络，可进一步根据各种应用场景的数据交换共享需求，建立跨机构之间的可信安全的数据共享交换机制。

利用区块链的不可篡改、可追溯、多方共识的特性，让数据共享交换的各方都参与目录的建设、存储和维护，增强了目录的可控性，提高数据治理能力和信息标准化服务水平。在数据目录共享过程中，先对目录信息进行清理和确认，然后将目录信息上链公布，并提供目录信息在链上的查询、管理、维护。区块链所提供的共享账本可避免数据提供方做出随意变更数据的行为；同时，所有记录到区块链节点上的数据，都保存了信息资源目录的历史发布和变更的全量记录，可根据时间戳来追溯历史记录，保证了目录数据在区块链的可控环境下进行数据交换。

在结合区块链的隐私计算框架中，隐私计算参与方成员之间可以签署多方协议，明确将所有操作记录通过区块链来记录，并跟踪数据交换痕迹。在这个过程中，通过对所有参与方的全量操作进行存证和审计，可以发现参与方的异常操作，从而达到探查

恶意节点的目的。

数据目录的权限控制通过智能合约实现。将目录权限和目录数据分开定义，避免了权限和目录的耦合，减少目录权限变更对目录的影响。使用数据时，根据数据的安全分级分类选择不同的共享交换方式。对于涉密、敏感、有条件共享的数据，选择采用“可用不可见，用后即焚”的可控交换方式进行交换共享，满足数据不能暴露、使用方不能直接获取源数据或者全部数据的要求。对于无条件共享、安全开放、完全开放类的数据，选择直接提供原始数据的方式进行交换共享。可以利用区块链形成数据安全分级分类的共识，通知智能合约定义权限的功能，通过合约语义定义参与方各自的权限，提高了权限控制的灵活性。

5.可信存证和审计

隐私计算任务执行过程中的存证环节可通过使用联盟链完成。存证内容至少包括存证主体的个人信息（身份）、任务标识（ID）、关键过程信息、签名信息等。主要的存证环节一般包括:

（1）任务配置与计算合约。协调方将任务配置信息发送给各参与方，参与方计算前形成计算合约。这意味着各方已经就共同执行一次隐私计算任务达成共识。将计算合约（一般包含任务配置信息）上链，为后期任务追溯奠定基础。

（2）数据输入。数据提供方基于计算合约进行数据输入，将该输入行为进行区块链存证，以便在后期证明其确实提供了数

据。

（3）计算。计算方在收到数据输入时、以及在计算结束后可分别对两次过程行为进行存证，以证实计算行为真实发生过。

（4）结果输出。结果方收到输出信息后进行存证，证实计算确实已经结束。

各参与机构作为区块链的联盟方节点，都保存着数据共享中的目录信息，权限控制信息，协调信息，存证信息，交易信息等，可根据审计要求追溯任意历史的变更记录。

6.链上数据流转隐私保护

传统业务中，数据直接以明文形式进行记录，这一方面便利了监管与业务人员对数据的溯源，另一方面也严重泄露了数据隐私。若对数据加密后记录其密文形式，又将给数据的计算、流转、追责、溯源、验证带来挑战。

依托区块链等分布式可信智能账本技术，融合学术界、产业界隐私保护的前沿成果，兼顾用户体验和监管治理，针对隐私保护核心应用场景提供了极致优化的技术方案，实现了公开可验证的隐私保护效果。

链上数据的隐私保护可以采用“链下计算、哈希上链”的轻量级实现方式。方案中，用于流转的目标数据保存在链下，基于目标数据的计算任务也在链下完成，而目标数据或计算任务对应的摘要信息、过程证明信息则保存在链上，并采用足够健壮的哈

希算法保证只有摘要信息但无法反推出原始数据或任何中间结果。原始数据在链下的存储可以采取本地化的物理存储基础设施，也可以采用联盟成员共同维护的分布式文件系统。

在数据共享环节，由链上智能合约发起，通过链下数据服务系统完成对应的信息传输。过程中，通过隐私计算系统完成共享数据价值的计算任务，并通过链上摘要信息完成计算过程的审计和数据的溯源，完成链上、链下资源相结合的数据流转。当进行共享的目标数据样本空间有限的情况下，为了避免链上公开的摘要信息被暴力穷举破解，链上摘要信息的生成可以采用加盐的方式进行处理。

“链下计算、哈希上链”的实现方式将原始数据和计算过程实现了链上和链下的隔离，链上仅保留验证的部分，提高了链上的隐私保护能力，联盟链上专注于数据和计算本身的可信，链下负责数据价值的流通和高开销的计算任务。

7.联盟链中心节点的功能与作用

在联盟链与隐私计算结合的框架中，中心节点可以由“盟主”节点来承担。中心节点通过向成员节点输出管控流信息对成员节点做出管理，数据流只存在于成员节点之间，不经过中心节点，如图 8 所示。中心节点的功能与作用主要有以下几点。

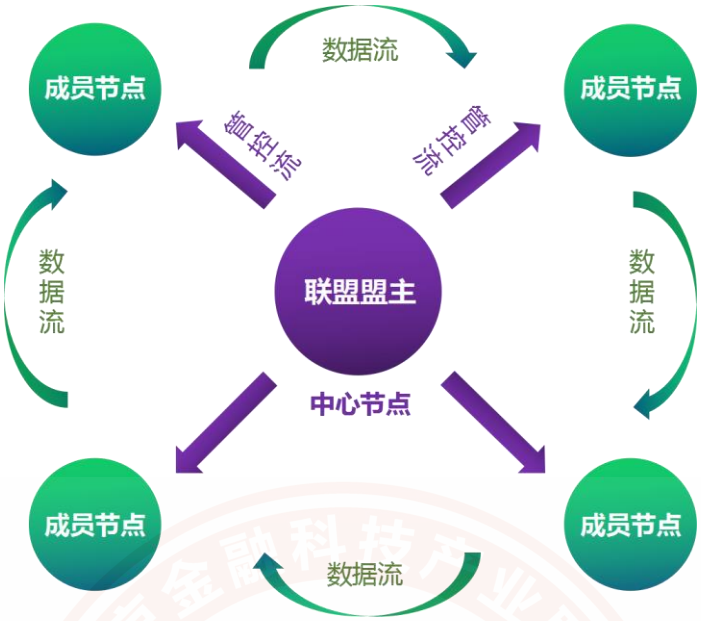

图 8 中心节点与成员节点的信息流

（1）对参与方的准入、权限管理

除了对数据目录的权限控制外，对数据流通中参与方也需要进行权限控制。在部分去中心化的联盟链中，中心节点可以承担权限管理的工作。例如，在隐私计算过程中基于区块链进行存证，并且通过存证信息探查到了不诚实的或恶意的参与方节点，那么联盟链的中心节点即可对其进行权限控制，避免其再次参与到联盟链内的数据流通中。此外，对于新加入的参与方，也需要联盟链中心节点对其进行审核与授权，保障联盟内其他参与方的数据安全。

（2）控制数据使用方的用途用量

数据流通最大的风险就是数据滥用，最大的难点是控制用途用量。防范数据泄露、保障数据安全的根本目的在于杜绝数据滥用。联盟链中的中心节点可以对数据共享过程中参与节点数据的使用记录进行监管和控制。结合其授权功能，中心节点对未合理使用数据的参与方可以收回部分权限，以防止数据的滥用。

（3）辅助决策数据定价

数据流通的本质不是数据本身或其特定使用权的直接转手或传递，而是一个通过市场配置与整合多方数据资源(包括数据、算法、模型、参数），利用算力进行加工，最终把计算结果交给结果需求方的过程。数据的价值仅仅体现在其所参与形成的计算结果的使用价值上。离开了数据的应用，数据作为计算原料无法独立确定价值。因此，数据的价值需要得到一个相对公允和透明的评估。中心节点由于既不是数据使用方，也不是提供方，只起到管理、服务等职责，因此可以结合链上所存证的数据交易、数据使用记录等信息，提供一个相对合理的数据交易价格供参与方参考和决策。

8.联盟链监管节点的作用

随着联盟链技术的发展和商业形态的探索，有必要对联盟链

平台提供配套的监管功能，满足第三方监管的必要性，避免联盟链系统脱离法律法规和行业规则。重点行业的区块链系统要为监管部门设立监管节点，提高监管的渗透力和时效性。监管人员通过监管节点监督联盟链的运作，并能接触到联盟链运作过程中的权限变更记录以及待审计的数据。

在隐私计算与联盟链结合的框架中，可以为监管节点提供功能接口，接入完整的、可验证的数据。监管机构将这些数据纳入大数据挖掘分析，实现端到端、跨机构、全流程的监管审计。进而实现风险预测、恶意行为识别判定的目的。

五、 应用案例

本报告中案例涉及数据均已获得相关数据主体的授权，个人数据满足个人主体“知情同意原则”，满足《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等相关法律法规、管理办法要求。

（一）联合风控建模

1. 案例背景

当前，我国低线城市、县域乡镇等下沉市场人群规模已超 6

亿，随着其生活消费水平不断提高，他们的消费升级需求不断凸显，成为新一轮消费升级的中坚力量。“业务下沉”成为商业银行获取流量增量、寻求新市场机会的重要来源。下沉市场前景广阔，长尾客户群庞大，但是客户信息的缺乏加剧了横亘在银企之间的“信息不对称”鸿沟，为商业银行金融产品的风险控制带来了新的挑战。

近年来频发的数据泄漏、数据非法交易、侵犯个人隐私等事件，正在给信息的采集和处理提出更高的安全要求，政府也出台了严厉法规，包括：《数据安全管理办法（征求意见稿）》、《个人金融信息（数据）保护试行办法》、《中华人民共和国民法典》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等。银行金融产品的风险控制希望能够尽可能获得更多的数据维度，或者联合其他实体通过协同计算的方式来共享数据资产的价值、获得无限逼近全局智能抽象的能力。区块链隐私计算技术既能保护数据隐私又兼顾数据安全，还能让数据正常发挥价值，结合针对银行业务设计的智能风控产品，成为解决银行业务下沉风险问题和保护数据隐私的解决方案。

银行出于风控质量考虑，建模和风控查询往往需要外部数据源参与，这涉及数据安全和信任问题。通过综合运用联盟链、隐私计算、大数据等技术构建基于区块链隐私计算的大数据智能风控产品，可以为银行提供安全的数据查询服务、风控数据分析、联合建模、多方数据规则和模型的部署与管理功能，联合外部大

数据帮助其进行中小微和个人经营贷金融产品信贷用户的风险评估和决策。

2. 解决方案

基于区块链隐私计算技术的大数据智能风控产品综合运用联盟链、安全多方计算、联邦学习、匿踪私密查询及切片规则引擎等技术构建智能风控平台，在保护个人隐私和数据安全的同时，实现大数据在数据合作方和银行之间的价值流通，为行方提供安全的数据查询服务、风控数据分析、联合建模、多方数据规则和模型的部署与管理功能，联合外部大数据帮助行方进行信贷用户的风险评估和决策，提升银行的风险识别能力和智能化水平，产品示意图如图 9 所示。

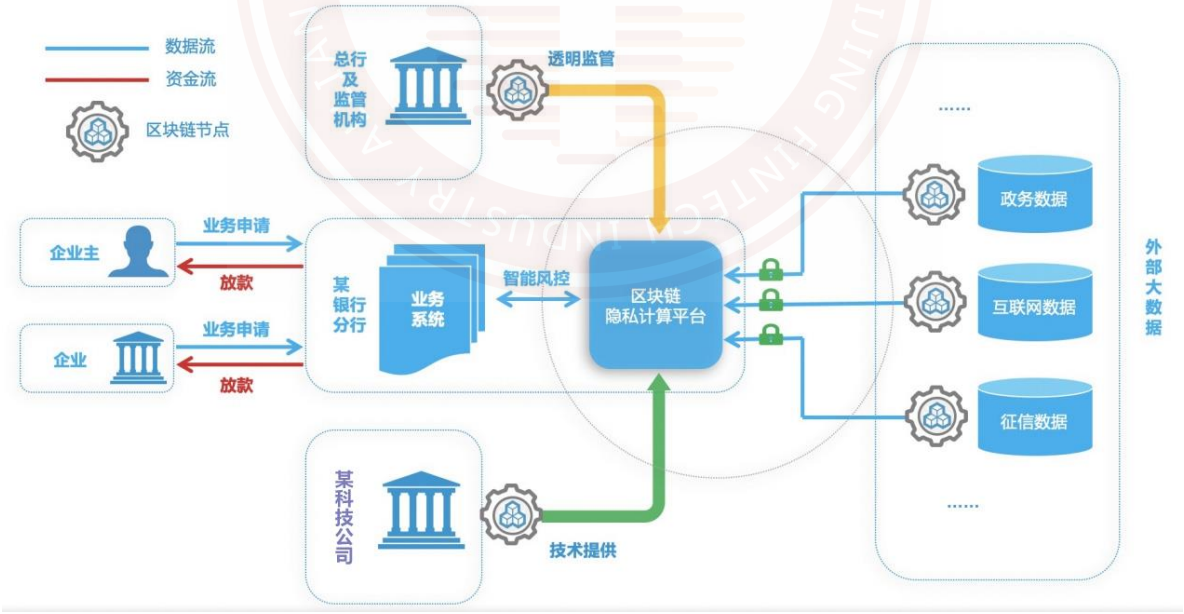

图 9. 基于区块链隐私计算技术的大数据智能风控产品

该产品在业务应用上:

（1）为银行提供外部大数据安全融合能力，解决外部数据使用过程中的合规难题，提升大数据风控应用能力。

（2）有效优化银行建模分析决策路径和信贷风控流程，提升风险管理水平。

3.技术架构

方案通过区块链上的存证合约完成关键业务流程的上链记录，使数据应用、模型结果可信存储，并支持对外开放接口提供给总行以及监管机构进行安全审计。

通过区块链隐私计算将行内信贷用户申请信息、存款、理财、行为偏好等数据和其他合作方数据进行安全融合，丰富信贷用户风控数据特征维度，扩大其他合作方数据开放程度。

通过基于区块链的安全多方计算和自动联邦学习技术实现在银行和其他合作方原始数据不出各自私域的情况下安全构建风控用户画像、风险规则和信用评分模型，帮助银行更加安全、更加全面、更加智能地评估信贷用户的风险状况。

通过区块链数字身份的建立，基于匿踪私密查询合约保护数据查询过程中行内信贷用户身份信息，采用切片决策引擎技术实现基于多方大数据的风控规则和模型的安全部署和管理，并提供可视化监控分析展示系统，帮助银行建立贯穿信贷用户全生命周期的安全智能风控平台，提升多方大数据在行内的风控应用价值

和效率。

通过基于智能合约的多方联合自动特征工程、自动算法调参、自动模型优化等联邦学习的智能建模技术，实现从银行和合作方数据中自动提取发现识别信贷用户风险的关键指标，降低了建模分析操作门槛，联合行外大数据构建预测性更强的全局模型，提升银行的风险识别能力和信贷审批决策过程的效率。

通过部署在不同区块链节点上的切片规则引擎技术实现全局总模型或总规则的安全部署，消除了独立子规则和子模型的效果误差，提升决策结果的准确性，同时保护了风控模型和规则的资产价值。

4. 应用价值

商业银行传统业务发展到达瓶颈期，一二线市场需求将逐渐趋于饱和，这需要商业银行尽快摆脱依赖于传统模式的惯性，寻找创新转型的突破口，在三四线及以下城镇农村发展“下沉业务”具有强大吸引力；商业银行进军“下沉市场”同时也是响应国家号召、发展“普惠金融”战略的需要，商业银行入局下沉市场，能够让金融服务、优质产品更好地惠及弱势地区，覆盖广大农民、小微企业、城镇低收入人群。

商业银行结合外部数据的引入，深度挖掘自身数据，将帮助银行有效、低成本地触达小微客户，有效识别信用风险，基于区块链隐私计算技术保护数据提供者和数据使用者双方的数据隐

私安全，使多方数据安全、合规、合理地应用于业务决策。

（二）反洗钱

1.案例背景

从近年来的《中国反洗钱报告》可以看出，在监管部门不断强化监管的压力下，金融机构在识别客户身份、报告大额和可疑交易、保存客户身份资料和交易记录三大基础工作中的投入逐年增长，虽然合规性问题大幅降低，但有效性问题逐渐显现，特别是以区块链技术为基础的虚拟货币，使不法分子很容易逃脱金融机构的审查，较快实现资金的转移分散。同时出于客户隐私保护、同业竞争等原因，监管部门与金融机构以及金融机构间尚未形成客户信息的共享机制，多家金融机构对同一客户均需开展身份识别，投入成本高，验证渠道单一，而且识别结果往往不一致。不法分子则利用金融机构间数据孤岛的漏洞，进行跨机构、跨区域的资金转移，增加了监管机构与金融机构对可疑交易监测的难度。建立反洗钱客户信息共享机制，可提高金融系统透明度，增强金融系统稳定性，提升尽职调查的工作效率，实现对可疑客户和可疑账户的整体管控，提升反洗钱系统的整体防御力。

2.解决方案

首先由监管部门与核心金融机构牵头，联合其他金融机构构建以区块链技术为基础的“联盟链”，通过智能合约来签订协议，

设立准则，从而明确联盟成员的权利与义务。如机构间的共识机制，约束各机构行为的同时也保证了其无法违约。还可以设置数据的读取权限，如监管机构可以读取查询所有金融机构的上链数据，而金融机构只能读取写入本机构的数据，对于非本机构的数据只有读取权限，且需要申请审批等。为了保证上链数据的准确规范，可以通过智能合约去约定必要信息与数据格式，如客户名称、身份证、手机号码、交易时间、交易金额、对手方信息等，同时也满足了监管对数据治理的要求。

其次每家金融机构内部按照区块链联盟约定的标准自行构建基于区块链技术的“私有链”。在私有链上，金融机构里的每一个客户都作为一个独立的区块，按时间顺序保存着客户所有的身份信息、交易信息、修改记录等，同时也会同步到整条链上所有客户的本地账本中，从而满足公开透明、不可篡改、可追溯的目标。

在联盟链上，每家金融机构与监管机构作为一个独立的区块，可以通过接口与各自的私有链网络相连。客户的身份信息、交易信息在内部私有链认证通过后，再通过联盟链分布存储在每家金融机构和监管机构的本地账本中，从而实现数据的互联共享且公开透明、不可篡改、可以追溯。

当 A 银行客户 C1 向 B 银行客户 C2 发起跨行转账时，首先 A 银行会将客户 C1 的身份信息和交易信息记录在私有链上该客户的独立区块中，并将此条信息在私有链网络中广播，其他区块通

过共识算法验证通过后，记录在私有链上的本地账本中，从而完成信息在私有链网络的同步。资金转账成功后，将此条信息向联盟链网络广播，各金融机构与监管机构通过共识算法验证通过后，记录在联盟链上的本地账本中，从而达成对资金来源和去向的全程监控与追踪，业务架构图如图 10 所示。

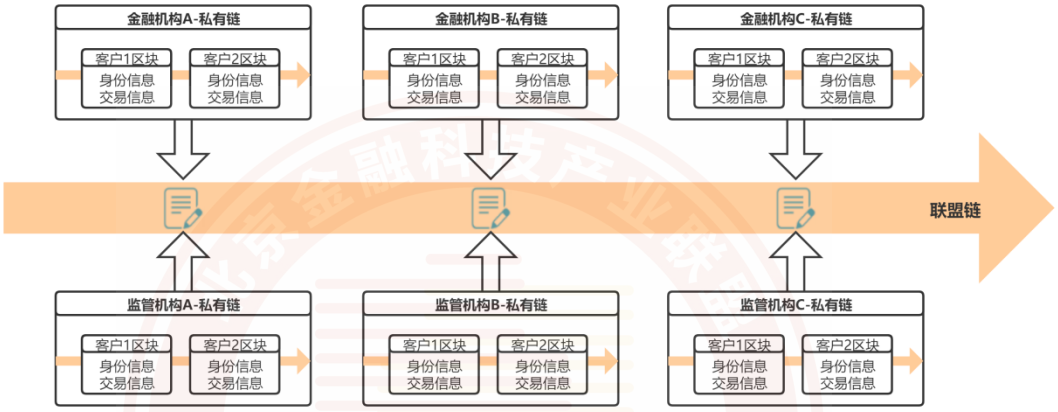

图 10. 反洗钱业务架构图

3. 技术架构

通过多方联盟链通信协议取得信任互通，接入区块链上的智能合约完成关键业务流程的数据上链，破除信息孤岛的壁垒，在数据隐私安全保护与打通信息共享链路的道路上，合力打造出精细化的共识生态体系，形成多方自洽的信息同步机制，进一步提升多方协同交互的管理效率，全方位激活信息的流通渠道。

通过底层大数据分布式存储的加持，为参与方提供高性能的读取与写入集成能力，通过进行多级别、多节点的分层存储，保

证了数据的可靠性和多副本的一致性，构筑兼具纵向扩展与横向扩展的弹性架构，为数据的容错与容灾提供了稳定的系统性载体。

通过将客户信息、账户信息、交易信息、命中交易、客户评级信息进行有机结合，坚持以业务为导向来完善交易数据及其他数据资产的评估感知度，融合隐私与安全计算，建立起安全可控的统一 KYC 视图信息与规则模型信息，聚焦拉升反洗钱监管的有效性，覆盖“预测-监控-处理“的全场景反洗钱机制，开拓可信可追溯的规范链上环境。

通过打通分布式、去中心化的集体维护平台，打造业务流程和数据的安全闭环，为参与方提供安全的模型规则设置与多阶段预警的弹性告警功能，形成助力参与方的跨平台统一预警信息视图系统，同时每个参与方又能进行自我管理和定向话题订阅，有效避免广播风暴带来的网络延迟与信息混乱。通过实现个性化的预警设定控制，系统模型规则模块深耕于规则的命中效率提升，拉升了策略的精确性与有效性。

通过节点准入机制和审计回溯机制，覆盖信息安全和隐私保护的全领域，利用支持国际与国家标准的多类密码学算法，构筑业务区块数据从生产、存储到传输的全通道安全保护。通过对基于角色的权限机制的有机结合，对数据与元数据访问的各个安全维度实现全方位约束。通过多语言接口支持，有效提升了开发人员的体验，为各个参与方的接入提供了优秀的平台能力，降低了开发成本。通过兼具便捷性和易用性的部署、升级、监控功能，

将持续敏捷迭代常态化，提升分布式网络的优化和交付便捷性。总体技术架构图如图 11 所示。

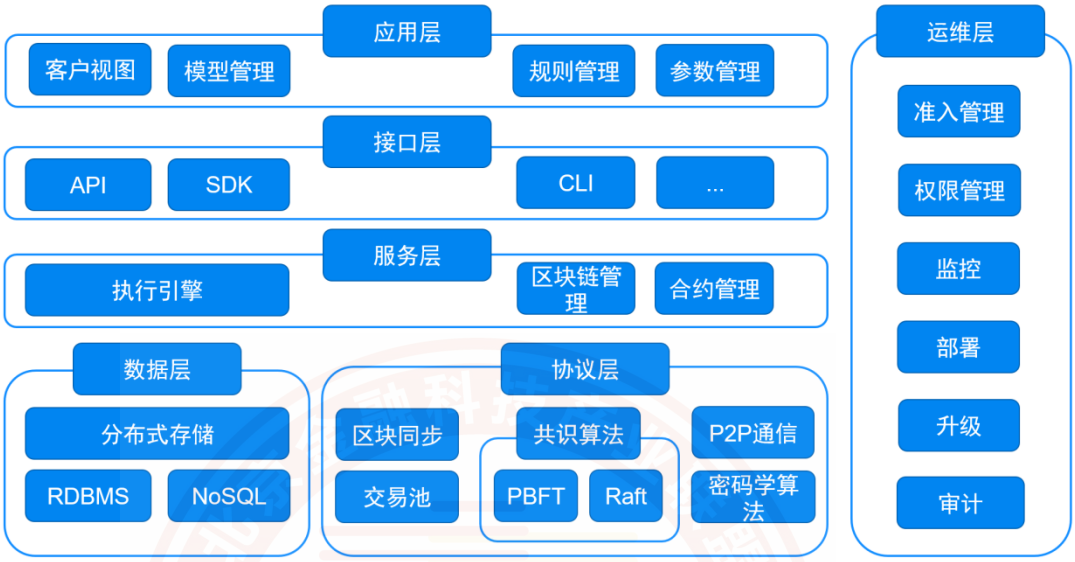

图 11. 技术架构图

4. 应用价值

金融机构所有客户的身份信息和交易信息，分布式加密存储在联盟链网络的各区块中，从而实现各金融机构与监管机构的共同维护，打破数据孤岛，形成完整数据链。同时保证客户身份信息和交易信息的有效性，提升数据质量，强化数据安全。智能合约的应用，不仅可以设立共识机制，建立行业标准，约束联盟成员的行为，还可以实现自动监测，主动上报大额和可疑交易，降低反洗钱成本，强化事前、事中洗钱风险的监控和预警，提高金融机构的风险管理水平。

基于区块链技术，未来可以联合公检法、工商、海关、税务、

征信等部门构建更加全面的联盟链网络，实现联网核查，进一步提高反洗钱的工作效率。

（三）智能选址

1.案例背景

对于线下实体来说，成功的铺位选择是提升竞争优势的无形资产，不仅能带来可观的客流，增大品牌曝光率，还能大幅提升营业额。而随着数字经济时代的到来，市场环境瞬息万变，线下选址的试错成本越来越高，选址方法亟需变革。一方面，传统选址方法主要依据人工调研和以往经验，导致选址决策会受到人为因素的干扰，且调研数据维度少、时效性差、质量难以校验，无法保证选址的准确性与科学性；另一方面，传统选址方法投入成本高、时间周期长，即耗费的人力、物力、财力及时间成本较大，选址效率低，容易错失良机。

如今，随着区块链、大数据、AI 等技术的广泛应用，目前线下选址主要分为两类场景：一类是网点推荐，即没有目标选址点位，需要大数据智能推荐备选点位，以缩小待选范围，实现精准选址；第二类是定点评估，即已有备选区域，需要通过大数据评估备选区域周边情况，辅助最终决策。

2.解决方案

基于多方、多维度数据及区块链隐私计算技术，提供专业的

智能选址解决方案。采用基于区块链的多数据源智能选址服务，为某银行网点选址规划提供参考和建议，优化银行网点布局，提高网点市场竞争力。通过协调多方数据完成选址建模，并通过共识数据合约，全流程审计，实现数据安全合规与隐私可控，最终根据需求方输入数据得到选址结果。该方案中大数据助力快速精准选址，使得选址维度全面且科学，并采用行业领先的隐私计算模型算法，使得选址方法更安全、更精准。业务架构图如图 12 所示。

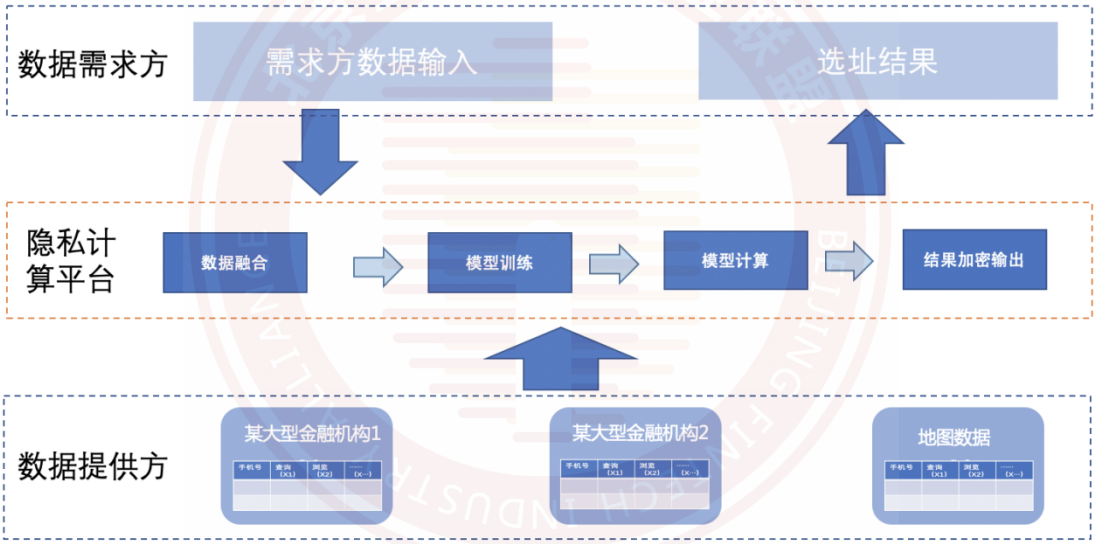

图 12. 业务架构图

3. 技术架构

方案采用了区块链、TEE 可信计算、机器学习等技术，利用多个参与方的相关数据，在保护数据隐私前提下协同计算。

首先多个参与方的训练数据和预测数据按照样本 ID 进行对

齐，之后各方将数据元信息上传到区块链，原始数据存储在本地。同时在银行部署 TEE 可信计算服务，用于敏感数据的解密和计算。调用链上数据信息发起训练或预测任务时，各参与方将原始数据加密传输到 TEE 环境中，在 TEE 内部进行解密和数据整合，并运行训练或预测算法进行计算，最终结果用任务发起者的公钥加密。技术架构图如 13 所示：

图 13. 技术架构图

4. 应用价值

本平台现已完成交付，提供包括人口相关、共生及竞争相关、周边设施相关 3 大类的 19 种选址评估维度，支持一键式灵活配置智能选址模型，提供网点多维度评价、智能化布局选点、流量经营等全面专业的选址方案，解决了可量化信息维度比较单薄的痛点，提升了区域环境认知及网点选址决策效率。与此同时，本方案解决了传统机器学习数据使用合规性、模型准确度、计算过

程可追溯等问题，通过区块链和可信计算等技术，实现多个数据方协同建模和预测，满足客户对数据隐私保护、数据贡献度衡量、计算全流程可审计等能力的需求，成功落地为银行网点选址提供了有力的技术支撑。

（四）白名单共享

1.案例背景

目前国内信贷征信数据分布于各银行、各小贷公司、各贷款平台等机构，由于机构众多、信息无法有效共享等众多原因，征信数据分布离散，没有共同建立信用屏障。传统方式通常是将信贷数据储存在一个中心节点上，这个中心节点完全由数据中心控制，数据中心可以随意地修改、删除这些数据。这就造成数据中心可能出于利益原因，做出出售假数据、篡改或者删除数据等恶意行为。区块链分布式账本、去中心化、不可篡改的特性，用来做征信数据的共享具有先天优势，能够解决各个节点数据线上互换的信任问题。

2.解决方案

基于多方、多维度数据及区块链隐私计算技术，提供专业的白名单共享解决方案。通过协调多家银行不同维度的数据在隐私计算环境中加解密后进行建模和训练，需求方银行再将数据输入到模型中得到最终结果。整个过程链上执行和记录，实现数据安

全合规与流程审计。实现各方数据不出本地即可完成白名单共享，满足业务需求，业务架构如图 14 所示。

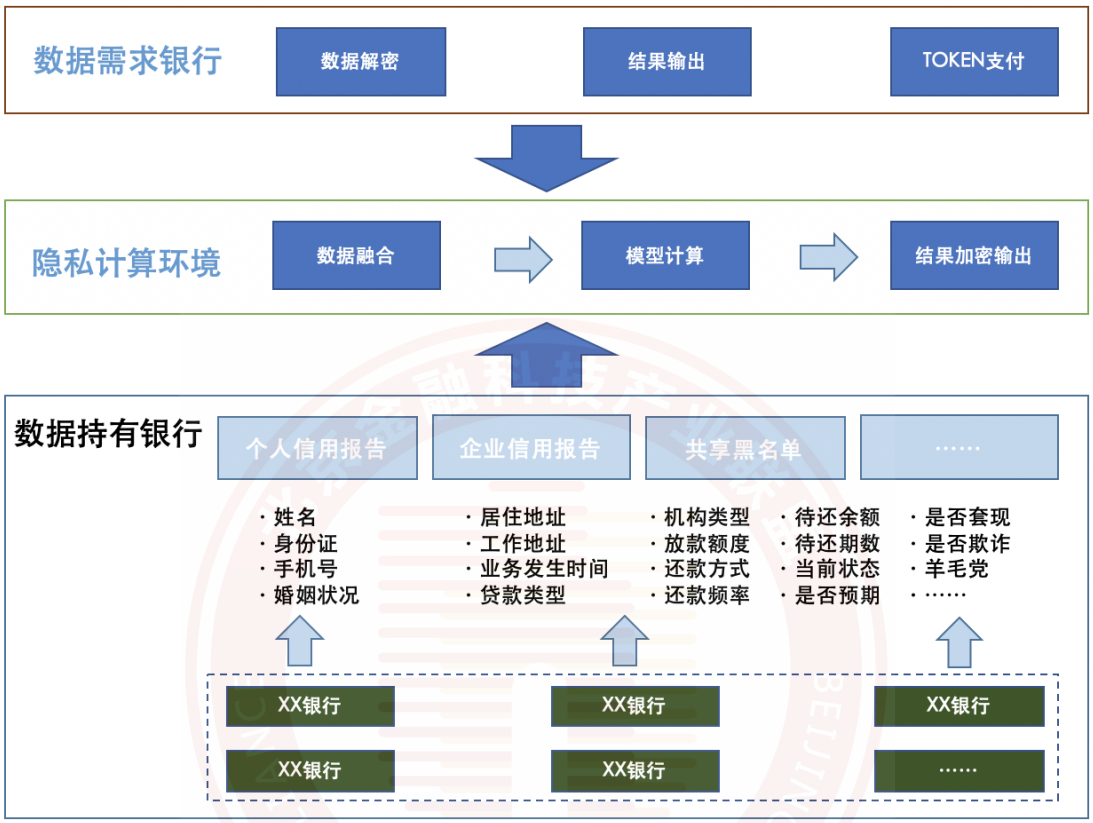

图 14. 业务架构图

3. 技术架构

金融十二行系统是多家银行机构共同构建的机构间风控共享白名单区块链网络。金融机构凭借各种区块链网络身份，通过自己的客户端系统登录网络并提交白名单信息，查看白名单信息。在重要信息提交的时候通过部署在多方的区块链共识网络进行交易多方协商，并将协商一致的交易上链存证，分发至不同机构

进行账本存储。同时，根据白名单贡献度进行链上 token 激励机制及数据资产化流通能力建设。各个机构在区块链网络和客户端之间构建中间网关，用于流量转发、证书管理、合约管理等重要技术实现，从而保证整体网络安全性的同时，实现系统性能的最大化。技术架构图如图 15 所示。

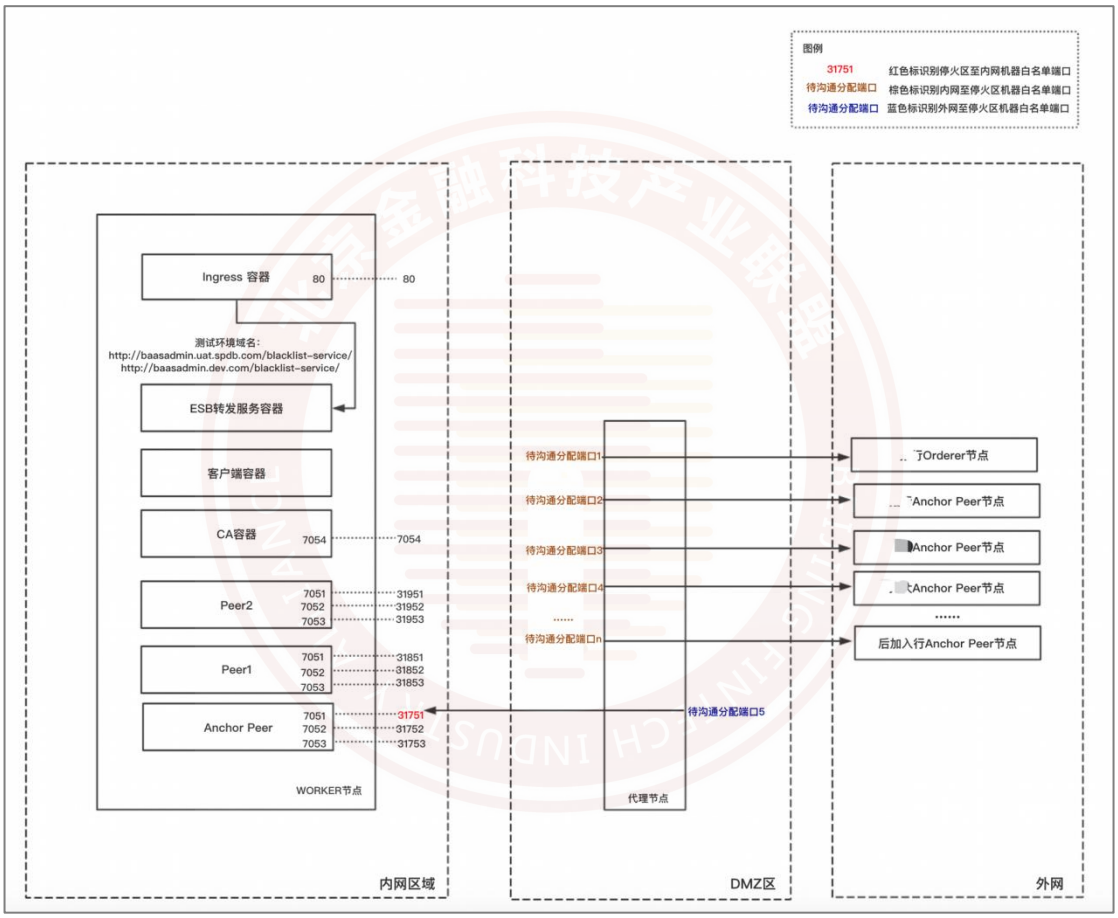

图 15. 技术架构图

4. 应用价值

自 2019 年 8 月该系统上线以来，截至 2021 年 1 月份为止，

十二行联盟网络区块高度超 19 万，交易数超 51 万。

基于隐私计算区块链融合的技术方案实现跨金融机构普惠金融场景下联合风控，联合建模，提升金融科技基础设施能力；全程保护各行内重要数据资产的同时，构建银行间白名单数据共享追溯激励机制，实现数据资产化输出。

后续，结合中国人民银行对网络平台与金融机构在征信信息方面的“断直连”要求，此案例涉及的相关方需要与持牌征信机构达成合作，以便后续合规运行。

六、 总结与展望

为了实现数据的合规共享需要从技术和管理两方面入手。隐私计算和联盟链的结合，从技术上部分解决了数据合规共享中存在的问题。在隐私保护数据共享的合规及政策方面，我们提出以下四方面的建议：

（一）遵循知情同意原则，维护个人信息安全

区块链与隐私计算的融合互补，拓宽了数据协同的应用边界，有效解决了计算过程和数据流通中的可信性、安全性、可监管性。在一些涉及个人信息处理的应用场景，仍面临违反“告知-同意”等法律法规的风险。金融应用中的数据要素所包含的信息，很大

一部分是个人信息。“不可见”只能算是遵循了最基本的“安全保障”原则（即防止非授权访问），如果数据主体对数据处理的目的或方式不知情或未同意，即便技术上实现了“不可见”或“匿名化”，其实也是不符合相关法律法规要求的，仍旧属于“违法行为”或“违规行为”。概括来说，利用个人信息进行隐私保护计算，至少需要满足如下几点原则：一是目的明确原则；二是最小必要原则；三是公开告知原则；四是个人同意原则。

所以，对于自然人的行动轨迹、消费记录、支付记录、借贷记录、公用事业开支等个人信息，如果希望利用其进行隐私计算，单纯做到明文信息“不可见”，其实并不能满足合规要求，更重要的是需要履行“告知义务”并且获得其本人的同意和授权。当然，在反洗钱、反恐融资、反欺诈等履行法定职责、维护公共利益等特殊法定场景下，处理相关个人信息则不必事先告知或征得本人同意。

（二）落实断直连等要求，推动征信信息共享

数字经济的迅速发展使得互联网等行业积累了大量个人信息，这些信息在人工智能、大数据等技术的加成下，在征信领域应用及其广泛，为判断企业和个人的信用状况提供了有效的支撑。此前，金融机构与互联网公司往往采用数据直连的模式进行合作。互联网向金融机构直连输送的数据中包含大量个人隐私数据，在未对数据类型按金融行业标准进行细分的情况下，就进行共享使

用，往往造成个人数据滥用，导致个人隐私的泄露。

2021 年 7 月，中国人民银行征信管理局向网络平台机构下发了征信信息“断直连”的意见反馈。该反馈要求网络平台在与金融机构开展引流、助贷、联合贷等业务场景合作中，不得直接向金融机构提供个人信息，即实现平台个人信息与金融机构的全面“断直连”。该要求是为了将个人隐私与征信数据概念区分开，以杜绝个人数据的滥用，从而对个人隐私进行保护。

“断直连”要求的下发，预示着网络平台与金融机构的数据合作模式将会被重塑。此后，金融机构想要获取个人信息必须通过与征信机构开展合作，使用征信机构提供的个人征信信息去开展信贷风控工作；网络平台需要通过征信机构将其所提供的数据合规化处理后，才能与金融机构开展相关数据合作。

（三）坚持良法善治道路，完善监管标准体系

建立健全围绕隐私计算区块链等新兴数据处理技术的行业监管体系，制定具有前瞻性、可操作性、针对性强的行业规定、规范、技术标准。

建立健全金融企业内部数据分类分级统一化标准及监管体系，包括制定行业通行分类分级标准；明确金融企业数据合规部门责任；建立实时监测数据违规使用预警系统；借助联盟链技术引入安全风险评估、审计、预警机制等。

结合应用实践和合规原则，对通过隐私计算、区块链等系

统自动化处理个人信息所涉及的“告知-同意”方式、内容及技术服务商责任等方面出台地方性法规并建立响应及时的监管体系。包括，明确对重要数据（个人信息、商业秘密）在隐私计算、区块链应用场景下的规定、监管部门及企业合规负责人制度。

（四）加快市场主体培育，推进场景应用落地

相比于个人信息处理，当涉及对企业信息进行处理时，则不需要满足“知情-同意”的原则，因为隐私信息保护规则不适用于企业。事实上，全球大部分国家的立法实践，也通常是选择不将企业纳入隐私权所保护的主体当中。从这个意义上说，金融应用中的数据要素流通，更宜于从对公用户、企业用户的相关金融信息着手运用隐私保护计算等金融科技展开试点。

鼓励并推进隐私计算区块链在企业数据、公共数据、个人信息匿名化处理后数据的广泛应用，推进政府数据开放共享，提升弱合规监管数据资源的高质量利用。包括积极建立统一数据交易平台，对数据交易过程中确权、定价、交易方式、交付形式、协议签署等制定标准化监管规定并明确平台管理的合规负责人制度等。

鼓励隐私计算与区块链融合的合规应用场景研发及实践工作，寻求行业典型应用场景落地的标杆案例并普及通用场景下新技术应用。包括积极推进行业试点合作单位名单建设及维

护，建立联合实验室用于研发及产品试用，给与试点单位在可控风险范围内的可试错政策支持，以避免因试点合作过程中对新型技术的自动化应用而导致违规风险的问题；给参与试点成果研发和应用落地的金融企业、技术企业提供一站式窗口服务、知识产权成果转化、政府或行业奖励、国家投资基金入股等孵化政策支持。政策引导和支持对于技术发展及场景落地也起到至关重要的作用。宽松的政策往往能刺激技术的快速发展。技术领先的国家往往会出台相对宽松的政策激励本土技术发展，以求继续领先。如果制定过于严苛的监管条例和法律法规，会极大冲击本土市场主体的合作意愿，继而降低技术发展诉求，影响本土市场的经济竞争力和技术竞争力。监管机构需要在政策引导支持和监管规范中寻求合理的平衡点，可以与业界、学术界共同联合制定合理的监管规范，以保证隐私保护和技术创新合理、健康地发展。