中关村区块链产业联盟
ALLIANCE FOR BLOCKCHAIN INDUSTRY, Z-PARK

区块链+隐私计算技术与应用研究报告

（2023 年）

中关村区块链产业联盟
2023年11月

版权声明

本白皮书、研究报告版权属于中关村区块链产业联盟，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：中关村区块链产业联盟”。违反上述声明者，本单位将追究其相关法律责任。

编制说明

组 织 单 位:

中关村区块链产业联盟

牵头编制单位:

中国信息通信研究院、北京航空航天大学、北京邮电大学、中国联合网络通信集团有限公司

参与编制单位:（排名不分先后）

北京科技大学

四川大学

北京交通大学

上海摩联信息技术有限公司

华控清交信息科技（北京）有限公司

蚂蚁科技集团股份有限公司

光之树（北京）科技有限公司

编写组主要成员:（排名不分先后）

刘阳、池程、马宝罗、尹铃元、张钰雯、关振宇、陈红松、许刚、任爽、边松、何坤、刘峥、丁慧、冯希顺、武姗姗、刘江华

前 言

区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，全球主要国家都在加快布局区块链技术发展。以习近平同志为核心的党中央高度重视区块链发展，多次强调要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

随着以“数字新基建、数据新要素、虚拟新经济”为核心特征的数字经济发展的全面来临，全球各国和产业界都高度重视区块链基础设施推动数字经济发展的重要动能，欧盟区块链服务基础设施 EBSI、印度国家区块链框架 NBF 等国家级重大工程先后启动建设。区块链是我国为持续推进产业数字化转型，利用区块链自主创新能力而谋划布局的数字经济“新型基础设施”，以代表产业数字化转型的工业互联网为主要应用场景，以网络标识这一数字化关键资源为突破口，推动区块链的应用发展，发挥实现新基建的引擎作用。

为了进一步凝聚产业共识，推动区块链基础设施规模化发展，启动了区块链系列报告编制工作，希望能够有助于产业界和学术界凝聚共识，更好地发挥区块链作为基础设施的作用，为技术和产业变革提供创新动力。本报告聚焦“区块链+隐私计算”方向，通过理清“区块链+隐私计算”概念，分析“区块链+隐私计算”核心挑战和发展路径，将有助于推动区块链基础设施与隐私计算融合化部署，优化区块链基础设施性能，推动区块链基础设施规模化落地。

目 录

图 目 录

一、区块链+隐私计算整体概述

隐私计算是面向隐私信息全生命周期保护的计算理论和方法，具体是指在处理视频、音频、图像、图形、文字、数值、泛在网络行为信息流等信息时，对所涉及的隐私信息进行描述、度量、评价和融合等操作，形成一套符号化、公式化且具有量化评价标准的隐私计算理论、算法及应用技术，支持多系统融合的隐私信息保护。在互联网经济时代，数据已成为新的生产要素，大数据时代需要更丰富、更多样、更安全的技术处理手段，传统的数据安全解决方案已不再适于日益增长的数据流通安全需求和合规要求，如何确保数据安全有序流通使用、实现数据价值最大化，是数字经济发展过程的亟需解决的难题。

隐私计算是以安全多方计算、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，在保证原始数据隐私安全的同时，完成对数据的计算和分析，实现数据的“可用不可见”。隐私计算保障了数据计算过程中的隐私保护问题，但如果参与隐私计算的节点存在主观作恶的意图，就可以利用中间结果进行攻击。当多方节点共同参与隐私计算时，数据确权问题也会成为隐私计算过程中遇到的挑战。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。

区块链具备数据可溯源、难以篡改、智能合约自动执行等技术特点，可以提供数据全生存周期的全闭环管理。实现上链前数据真实性交叉验证，上链后数据难以篡改和可追溯；还可以通过共识机

制在参与方之间建立信任基础，实现点对点的价值传递；还通过协同机制、激励机制的设置与共识，促进数据开放共享与价值协作。但与此同时，区块链也面临一些挑战，比如如何保护链上数据隐私等问题。透明性是区块链的特性之一。交易数据经过验证节点验证状态和有效性达成共识后上链，上链的账本数据是所有参与节点都可见的，不能完全满足数据的隐私保护。合作机构或组织出于自己数据安全的考虑，可能会放弃加入区块链，从而限制了区块链的发展。要想解决链上数据的安全问题，需要引入其他的隐私保护机制。

数据流通模式迭代演变，呼唤新型架构隐私计算网络。当前，数据流通使用前沿的隐私计算技术，但隐私计算尚未形成统一的国际/国家标准，各方多采用各自实现的隐私计算算法，对其安全性、可靠性尚未形成共识；在基于隐私算的数据流通过程中，缺少对于隐私计算算法安全性、有效性和数据流通合规性的共识、存证、溯源等手段。

区块链与隐私计算结合，是解决数据共享难题、构建可信运营环境、实现数据高价值流通的有效技术手段。在原始数据无需归集与共享的情况下，可实现多节点间的协同计算和数据隐私保护。同时，能够解决大数据模式下存在的数据过度采集、数据隐私保护，以及数据储存单点泄露等问题。区块链确保计算过程和数据可信，隐私计算实现数据可用而不可见，两者相互结合，相辅相成，实现更广泛的数据协同。

二、区块链+隐私计算重点问题

（一）兼顾数据隐私保护和共享利用

区块链+隐私计算技术有助于促进数据共享，实现数据价值的充分挖掘和利用。区块链凭借公开透明性和不可篡改性，提供了数据共享的良好平台。隐私计算技术实现了对敏感数据的有效保护，打消了共享方数据泄露顾虑。如果只是简单采取对共享的敏感数据加密存储在区块链上这种方式，数据的隐私得以保护，然而数据的可用性被极大削弱，呈现出来的只是一些看不懂的数据。另一方面，在数据共享过程中，共享方身份是否真实、共享数据来源是否可靠等问题都会带来隐私数据泄露和数据可用性降低等风险。因此如何有效融合区块链和隐私计算技术，在保护数据隐私与安全的同时，实现数据可信共享和有效利用成为亟待解决的问题。

（二）兼顾交易隐私保护和可用性

区块链凭借去中心化、低交易成本的特点，提供了便捷高效的资产交易平台。交易数据公开存储在区块链上，尽管能提高交易的透明度和可信度，但也带来了隐私泄露的风险。虽然在区块链中，用地址来表示交易双方来起到匿名的作用，链上的信息虽然是匿名的，但是通过链上信息绑定的链下信息，以及对相关交易进行聚类和分析，可以追溯到真实世界的交易双方，使得匿名性荡然无存，因此迫切需要对用户交易信息实施有效的隐私保护，以维护用户的经济利益不受损失。在区块链中，交易从产生到销毁的整个生命周期中都面临隐私泄露风险，任何一个环节出现漏洞都可能导致交易

隐私保护失效。采用单一的隐私保护技术往往难以保障交易隐私信息不被泄露，如何建立全面的交易隐私保护机制面临着挑战。另外，保护用户交易隐私不能以牺牲交易可用性为代价，其他用户在不知道交易双方真实身份、交易金额等隐私信息的情况下，也要能够验证交易的有效性和金额的正确性，以保证交易正常执行。

（三）兼顾用户身份隐私保护和身份认证

数字身份是构造数字世界信任体系的关键要素，区块链+隐私计算正在发展成为数字身份的关键技术。一方面区块链凭借去中心化、分布式存储、公开可验证、不可篡改等特点为解决传统身份认证中可信度差和共享差问题提供了新思路，另一方面隐私计算技术能够实现用户身份隐私保护，保障用户敏感身份信息不被泄露。但如何更好地融合两者以构建安全高效的身份认证机制还存在很多挑战，例如如何在实现用户数字身份有效认证的同时进行全面隐私保护，如何根据用户的实际需求进行身份隐私保护，如何兼顾用户身份隐私保护和监管审计都有待进一步研究。

三、区块链+隐私计算关键技术

（一）区块链+隐私计算整体架构

区块链+隐私计算采用两层网络体系架构，如图 1 所示。区块链实现参与方身份、权限的分布式管理，数据输入、数据计算、数据输出全过程存证和追溯；隐私计算实现数据的协同计算、数据价值的流动。

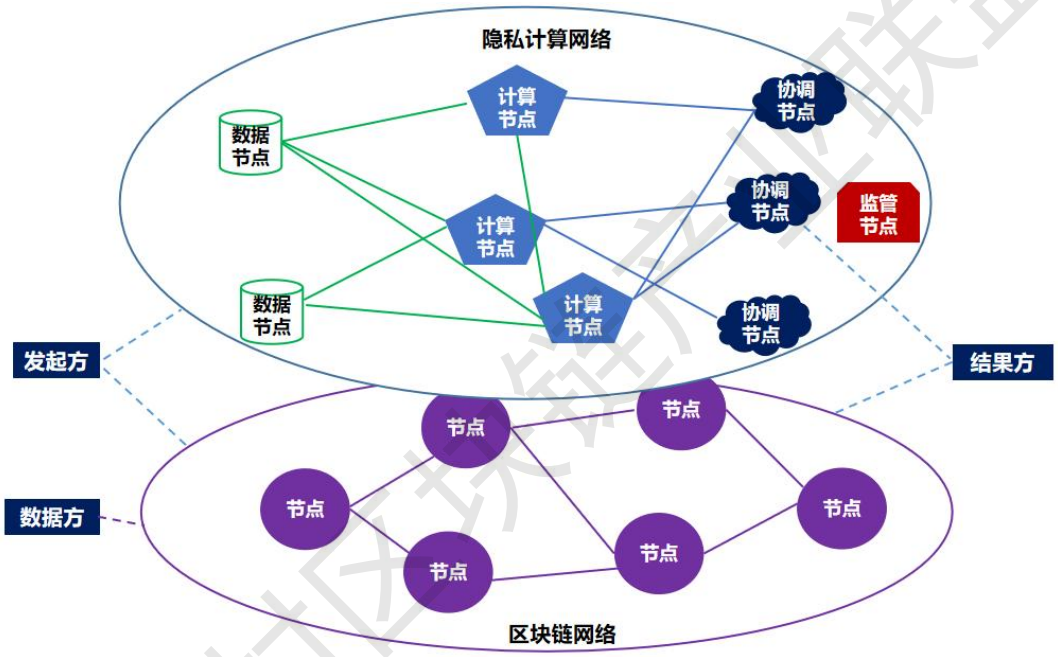

图 1 区块链隐私计算整体框架

基于区块链的数据流通基础设施生态体系中，参与方角色主要包括：

数据方：原始数据所有者，愿意分享数据的使用权参与隐私计算，并获取相应的数据价值收益。

计算节点：计算能力提供方，集成隐私计算引擎，对外提供高性能的隐私计算运算服务，并获取相应的隐私计算服务收益。

协调节点：在具体隐私计算协议需要的情况下，参与计算过程的协调工作，同时，协调方也承担隐私计算网络中计算任务的管理、监控等功能。

发起方：根据业务需要，启动隐私计算任务，调度数据方的数据和计算方的计算能力。

结果方：获取隐私计算任务结果。

监管节点：审计、监管生态体系运作的合规性，支持全程数据可追溯。

（二）数据隐私保护

区块链与隐私计算的结合，打造数据时代的信任机制与隐私保护。区块链具有“去中心化”、“分布式数据存储”、“可追溯性”、“防篡改性”、“公开透明”等优势特点，为解决多方协作和多方信任问题提供重要手段。通过共识机制为各参与方建立可信任的数据管理环境，防范和避免各类数据造假、篡改、遗失等数据管理问题，实现点对点的数据互通和价值传递。通过智能合约实现链上数据真实性验证和审计。通过协同机制、激励机制的设置与共识，促进数据的高效共享与应用。区块链“信息数据共享和透明”的特点，为数据的隐私安全带来了挑战，如何确保链上数据的隐私保护问题，直接影响着数据安全流通共享的效率。

隐私计算是一套包含密码学、人工智能、安全硬件等众多领域交叉融合的跨学科技术体系，隐私计算以保护数据全生命周期隐私安全为基础，实现对数据处于加密状态或非透明状态下的计算和分

析，在保证各方原始数据安全隐私性的同时，完成对多方数据的融合计算，实现多方数据的“可用不可见”。从而达到促进数据要素流通融合、有效提取数据要素价值的目标。然而，数据的真实性、数据来源、数据确权及流转过程是否安全和合规是隐私计算技术面临的难点。同时，隐私计算也无法解决跨系统信息交换的隐私保护，由于多方数据质量参差不齐，隐私计算主要针对单一信息系统和管理域的信息机密性进行保护，不同管理域间密钥管理机制、访问控制策略、数据安全保护能力存在差异，短板效应决定了隐私保护技术不能从根本上解决跨信息系统、跨管理域信息交换中的隐私保护问题。

区块链与隐私计算与结合，不仅很好的解决区块链面临的数据隐私保护问题，实现数据的安全流通，还能为数据的真实性、数据确权等合规问题提供可行解决方案，实现数据共享全流程可记录、可验证、可追溯、可审计。

（三）数据安全共享

基于区块链和隐私计算的数据安全共享技术使得不同区块链之间互相协作、可信共享数据，并且保证数据共享过程中不会泄露原始敏感数据。区块链上信息公开可见的特点，在促进数据共享的同时也带来了隐私泄露的问题。如果只是简单地采取敏感数据加密存储在链上的方式来保护共享数据隐私，呈现出来的只是一些看不懂的数据，削弱了数据的可用性。另外，由于数据共享环境的复杂性和敌手攻击行为的多样性，如何保证共享数据的真实性和可靠性面

临着挑战。

基于区块链和隐私计算的数据安全共享技术在保护区块链上隐私数据安全的同时，实现对数据的共享和有效利用。一方面，使得不同机构互相协作、共享数据，有助于打破数据壁垒和信息孤岛，充分利用数据价值。另一方面，保证了共享过程中不会泄露原始数据，可以有效地化解保护数据隐私与安全和数据共享与流通之间的矛盾，有助于打消参与机构数据泄露顾虑，引导其转变经营理念、提高数据融合积极性，助力疏通数据融合应用通道，激发市场守正创新活力和能力，更好地发挥数据纽带作用。并且基于区块链和隐私计算的数据安全共享技术还能提供安全性校验。通过区块链共识机制，建立起信任基础。通过区块链的授权机制和身份管理，实现数据共享方身份的真实性验证，在互不可信的共享者之间建立起一个安全可信的合作机制。通过智能合约实现数据真实性验证，保证可信数据共享。

目前基于区块链和隐私计算的数据安全共享技术可分为两大类，一是数据提供者将需要共享的隐私数据进行加密处理后存储在区块链上，只有满足一定的条件才能够正确解密出原始数据，实现对数据的安全共享和利用。例如，在基于对称加密技术的数据安全共享方案中，只有拥有指定密钥的用户才能解密得到共享数据。在基于秘密共享技术的数据安全共享方案中，只有足够多合法成员才能共同协商出解密密钥，实现组、群内的数据共享和利用。

二是数据共享方不需要先解密出其它共享方的原始数据，而是

直接对共享数据的密文进行各种计算操作，计算过程中不会泄露原始数据。以基于多方安全计算的数据安全共享方案为例，数据共享方将共享数据加密存储在区块链上，利用多方安全计算技术对数据密文进行计算，整个计算过程中无须解密还原出数据明文。在整个过程中，区块链作为一个消息广播媒介，将加密后的共享数据以及共享方需要互相传播的消息记录在链上，可以有效地减少通信代价，提高数据共享的效率。另外区块链对参与计算的数据和计算过程进行记录存证，可以有效追溯恶意输入，从而进行问责处罚。

（四）数据安全交易

基于区块链和隐私计算的安全交易技术主要关注区块链交易的安全性和匿名性。常规的区块链交易，交易的详细信息对网络中任何一方都可见。相反，通过安全交易技术，其他人只知道发生了有效的交易，而不知道交易的详细信息。交易双方的地址、交易金额等敏感细节可以隐藏起来，并且可以避免诸如“抢先”之类的问题。安全交易技术是一种更加安全的信息验证或者身份验证机制，安全性和隐私性就是安全交易技术的价值所在。目前，安全交易技术在区块链上得到广泛应用，包括保护交易匿名性、身份隐私、链下数据存储完整性等。依据交易的生命周期划分，可以分为交易分布、交易共识、交易存储和交易应用四个阶段的安全交易技术。

交易发布阶段的安全交易技术目的是为了在区块链用户发布交易之前尽量去除交易中的敏感隐私信息，相关技术包括动静态数据掩码、差分隐私和匿名化技术等。

交易共识阶段的安全交易技术目的是为了从交易被全网广播到通过共识机制写入区块链并最终确认这段时间，实施有效的交易隐私信息隐藏，主要需要防止恶意参与者非法监听交易数据。相关技术包括节点身份准入机制、匿名通信机制和通道隔离技术等，如 Hyperledger Fabric 利用数字证书对接入节点进行身份认证和权限限制，并结合多通道技术限制节点对交易的访问权限。

交易存储阶段的安全交易技术主要目的是为了防止攻击者通过对区块链上存储的交易数据进行观察分析，推测出用户地址、交易金额等隐私数据。交易存储阶段的安全交易技术通常利用密码学技术来隐藏存储在区块链上的交易敏感信息，例如 Zcash 利用非交互零知识证明技术在不影响交易有效性验证的条件下，实现了对交易双方地址和金额的隐藏，达世币利用混币机制隐藏交易双方地址。

交易应用阶段的安全交易技术主要目的是为了对智能合约和区块链应用所能收集和使用的交易信息进行规范，防止智能合约漏洞所导致的交易隐私信息泄露，以及区块链应用对交易信息非法的收集和利用。相关技术包括智能合约代码审计、智能合约漏洞分析、数据合规审计等。

（五）数字身份认证

基于区块链和隐私计算的安全数字身份认证技术旨在支持用户数字身份认证，同时对用户身份中敏感信息进行隐藏保护。数字身份是用户真实世界中的身份在数字信息系统中的映射，数字身份认证机制提供了认证用户数字身份真实性的方法，对于数据确权、保

证数据来源可信、审计监管等均有重要意义。传统的数字身份认证机制主要包括基于公钥基础设施的身份认证服务和基于 Kerberos 的身份认证服务，利用可信第三方来进行用户真实身份验证以及数字身份凭证颁发。用户得到可信第三方生成的一对公私钥，利用公钥作为数字身份标识，私钥签名实现数字身份认证。但是这种身份认证方式不可避免地存在第三方不可信、单点故障、身份数据泄露等风险。区块链凭借去中心化、不可篡改、公开可验证等特点提供了更加安全的身份认证机制，能够有效解决传统数字身份认证中存在的诸多问题。

当前基于区块链的数字身份认证机制可以分为两类：去中心化身份认证机制和自主身份认证机制。在去中心化身份认证机制中，与传统数字身份认证机制相同的是也需要可信第三方对用户的身份声明进行验证并产生签名，形成用户的身份凭证，帮助其他用户正确验证该用户身份。不同的是，用户身份凭证不再被中心化机构存储在其数据库中，而是存储在区块链的分布式账本中，有效缓解了中心化存储所带来的单点失效、盗用、篡改等问题。在自主身份认证机制中，用户数字身份由用户自己生成保存，无需任何第三方参与，从根本上提高了用户身份安全。

基于区块链和隐私计算的安全身份认证机制在不影响用户身份认证前提下，增加用户身份敏感信息隐藏保护功能，通常做法是采用非对称加密算法对用户的敏感身份信息进行加密保护，而不是直接存在区块链上。具体的，在去中心化身份认证机制中，用户的身

份凭证中通常包含一些不愿意公开的私人信息问题，常用的安全身份认证机制是可信第三方在验证了用户的真实身份后，将用户的敏感身份信息加密后放在凭证中，并将凭证存储在区块链中，既保证用户敏感身份信息不被泄露，又不影响用户数字身份的使用和认证。在必要的时候，还可以解密出用户的真实身份，实现追溯问责。对于自主身份认证机制，常用的安全身份认证机制是用户在生成的凭证中选择性的公开自己某些真实身份信息，利用非对称加密机制将自己不愿意公开的敏感身份信息进行加密隐藏，并将处理后的身份凭证存储在区块链上，提供了更加细粒度的身份隐私保护。

四、区块链+隐私计算应用实践

(一)基于安全多方计算的反诈骗黑名单共享

1.需求分析

在互联网、大数据及人工智能等新兴技术的驱动下，我国金融业积极开拓创新产品和服务，行业数字化转型不断升级，金融活动日趋复杂。与此同时，不法分子依托新兴技术手段，通过金融渠道进行如赌博、诈骗等犯罪活动，金融欺诈呈现出组织化、移动化、隐蔽化、场景化等特征，并已形成灰黑产业链，对居民资金安全以及金融机构的业务安全造成严重威胁。有调查显示，当前我国常见金融欺诈行为包含金融信贷欺诈、互联网业务欺诈和信用卡欺诈等，且逐步发展至移动端。2019 年，移动端欺诈攻击同期增长近三倍，金融恶意软件的欺诈攻击增长 56%。

虽然金融机构能够通过其自身沉淀的黑名单信息实现事前筛查并阻挡有欺诈记录的客户，但其并无法了解客户在其它机构的过往行为。然而，金融机构间往往出于资源竞争、数据安全及合法合规的顾虑而拒绝共享黑名单数据及相关解释逻辑信息，导致各机构对其客户金融行为的了解仅局限于自身渠道，无法覆盖客户全面的行为信息。特别是《个人金融信息保护技术规范》要求金融机构原则上不应共享、转让其收集的个人金融信息，确需共享、转让的，应充分重视信息安全风险。面对欺诈活动逐渐形成配合严密的产业链条的形势，金融机构普遍面临数据壁垒问题，行业整体欺诈侦测能力难以提升。

2.技术方案

为破解数据壁垒，实现各方数据安全合规融合应用，商业银行、农村信用社、小贷公司等金融机构作为数据提供方，应用安全多方计算技术打造基于隐私保护的黑名单共享平台，实现各方黑名单信息及相关逻辑标准的共享。具体地，各数据提供方的黑名单数据通过数据节点（DS）以密文形式输入安全多方计算平台，由计算节点（ES）执行联合统计；随后计算结果通过 DS 以密文形式输出至查询机构，由查询机构解密并使用。在此方案下，金融机构能够协同分析黑名单数据，事前拦截有历史欺诈行为的个体，并对可疑线索进行持续监控，谨慎防范欺诈风险。

在上述黑名单隐匿查询过程中，涉及数据传输行为、计算合约及结果输出的事后审计存证功能可由区块链技术实现。具体地，查询机构发起黑名单隐匿查询请求后，各数据提供方在同意后与查询机构达成计算合约，并将计算合约传输上链。随后，各数据提供方按照合约将自身黑名单数据输入至平台，同时将该输入行为上链，用于事后核查各方数据输入真伪情况以及数据计算是否遵照计算合约。最后，平台基于各方黑名单数据进行计算得到查询结果发送至查询机构，同时将本次查询任务的计算结果传输上链存证，用于事后审计。方案技术架构如图 2 所示。

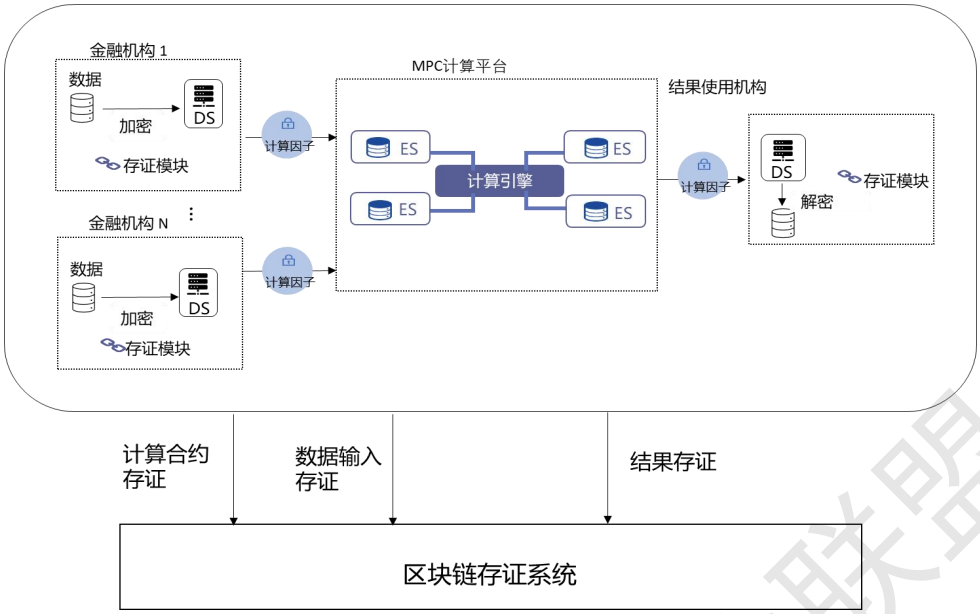

图 2 基于安全多方计算的反诈骗黑名单共享方案技术架构

案例利用安全多方计算技术化解金融行业数据孤岛现象，帮助金融机构实现黑名单信息安全共享，协同甄别金融诈骗行为。区块链技术对计算合约、数据输入和结果输出过程进行存证，方便监管方事后审查计算合约是否应用安全多方计算技术保护各方数据明文信息，同时审核数据输入、计算和输出过程是否遵循计算合约。

(二)依托数据安全融合计算实现场景化金融服务

1.需求分析

本地生活服务与金融服务数据合规共享难题。为了满足日益增长的金融需求，越来越多的企业开始逐步探索和推广生活场景化的金融应用。一方面，本地生活服务 APP 为用户提供一站式、全生命周期的运营管理，可以更高效实时地将各种权益（如信用卡补贴）推送给目标用户。另一方面，金融服务机构提供广度和深度覆盖银行网点、品牌效应等，可助力应用 APP 拓展更深入金融服务场景和

更广的覆盖范围。通过消费场景和金融服务场景的有机结合，可促进国内居民的消费，拉动经济内循环。

然而，在数据安全及合法合规日趋严格的背景下，特别是《个人信息保护法》出台，互联网应用提供商、金融机构之间进行数据共享、转让面临更大的信息安全和个人信息保护风险。

2.技术方案

本案例将用户在本地生活服务 APP 的数据与银行端的金融数据进行合法合规融合计算，并依托蚂蚁链区块链隐私计算融合的全链路数据生命周期管理能力，实现本地生活场景中的金融服务应用。

通过在隐私计算平台上融合授权后的本地生活用户数据及银行数据，实现在保护数据安全的前提下的多方协同计算与数据全生命周期的监控。通过隐私计算，可以帮助银行更好识别这些用户的消费习惯，同时本地生活服务应用也能基于融合计算的结果更好转化流量，实现正向循环。

本地生活应用中用户授权后的数据、结合银行用户授权相关数据数量级大，数据格式差异大。在进行联营合作时，需要将各方的数据进行融合计算，并保证各方企业数据的安全隐私、合规可审计，计算高效响应业务实时性需求。方案技术架构如图 3 所示。

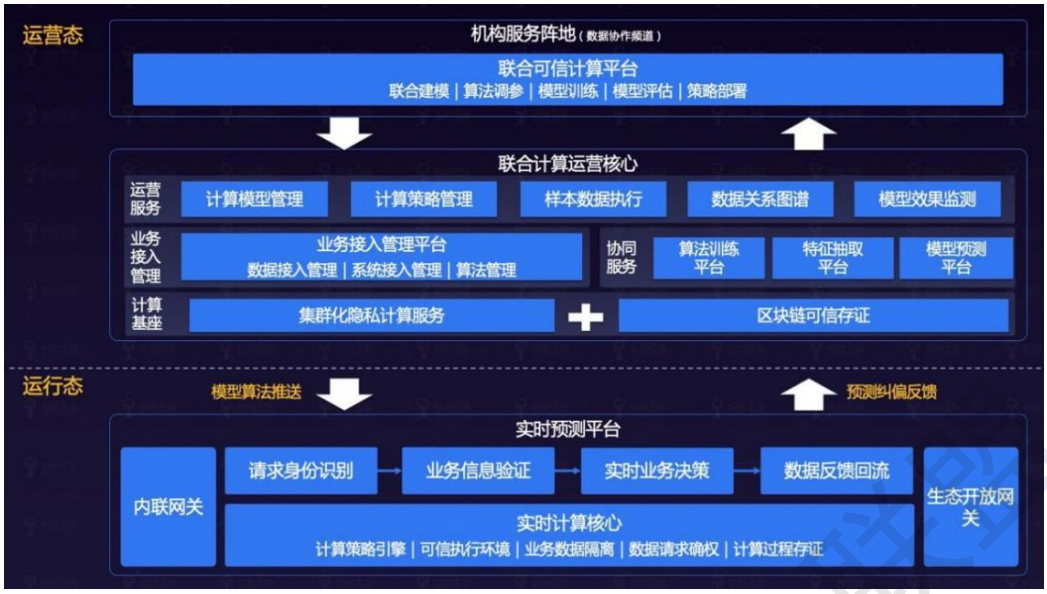

图 3 基于隐私计算的服务数据合规共享方案技术架构

针对这些问题，本方案从以下要点展开:

1. 扩展底层计算资源。首先是通过扩充底层资源，并支持更多硬件集群类型，进一步提高计算能力;

2. 优化调度算法。根据任务计算消耗资源类型，大小，有效的调度计算任务在多个安全计算集群选择最优的集群进行计算，实现资源的有效利用，同时使高优先级的计算任务被更早的安排计算;

3. 计算任务流程可定制化。数据隐私服务将提供更多基础的安全计算算子，业务可以根据自己业务的情况，通过任务编排工具，将这些基础算子按照自己业务的需要组成一个计算任务流。

4. 结合区块链公开、公正、可追溯的能力，实现对计算全过程的追溯。

多方数据联合计算场景中，通过隐私计算实现联合建模和大数据分析释放数据价值。“信任”是隐私计算的关键基础，区块链技

术可提供信任基础设施。隐私计算结合区块链技术形成完备的技术方案，实现数据可信、安全、隐私的参与计算，并实现可追踪、可审计，从根本上解决“数据孤岛”、数据合规共享等问题。

(三)基于隐私计算的政务数据开放共享

1.需求分析

政务数据开放共享隐私安全。数据作为新型的生产要素，市场化利用，核心问题是数据的安全、合规隐私、数据的权属规则问题。数据共享及价值挖掘需要提升多机构协同的效率，解决隐私保护、数据可信等问题，保障数据开放过程中数据的安全、合规以及各参与方的权益。在培育发展数据要素市场的过程中，要在《数据安全法》《个人隐私保护法》的法律法规保障下，建立健全数据管理制度，保障数据在多个机构之间流转、协同使用等开放共享场景下的安全性、合规性与协作效率。在制度保障和规则建立后，还必须利用区块链、隐私计算等领先的信息化技术，建设符合数据要素市场化流通的系统，保障数据协作全流程合法合规、权属清晰、隐私安全。

2.技术方案

蚂蚁链“区块链+隐私计算”技术融合的解决方案，结合了多种隐私计算和区块链的优势，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。

对于政务数据共享场景，本方案在各县市政府相关部门部署区块链数据隐私协作平台，实现市县数据的可信接入、分类分级管理以及多方协作应用的落地。具体包含：（1）平台部署，在每个数据源管理方部署数据可信接入服务，实现数据目录的注册；在大数据局数据运营管理方部署协作管控平台，实现对所有接入数据的门户展示、流程管理；（2）数据接入，部署完成后，各个参与的机构完成将本地待开放、共享的数据的目录注册以权限定义，初始化数据的类型、使用审批流程的设置；（3）开发及部署协作应用，结合各县市数据场景业务需求，使用协作平台在接入的各类数据的基础上，完成机构协作应用的开发和运行，打通机构间数据协作的链路，形成多方原始数据到数据应用服务的链路。方案技术架构如图 4 所示。

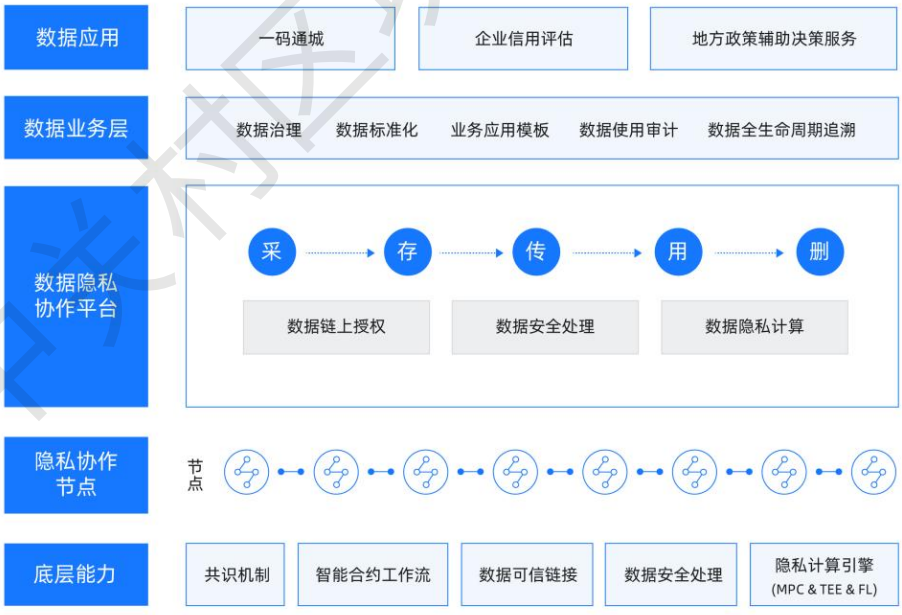

图 4 基于隐私计算的政务数据开放共享方案技术架构

蚂蚁链数据隐私协作平台将区块链、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。具体地，在大规模数据开放场景中，单一的隐私计算能力不足以解决不同的管控需求，该技术方案，将不同数据进行分类分级管理，并智能化地通过链上智能合约（数据协作工作流）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。

案例通过区块链隐私计算技术，将原本无法流转开放的数据安全合规使用，实现了政务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，满足政府政务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，有效保证了数据安全的前提下最大化释放数据价值。

（四）基于隐私计算+区块链的数运贷

1.需求分析

数据资产凭证以数字化凭证作为载体，承载数据要素，它采用新一代区块链技术，更易读、更智能、能跨链；它不仅是数据要素的载体，亦是全生产要素数据的载体。数据资产载体可以解决数据确权问题，使数据资产初步具备了进入市场流通的条件。空白凭证作为数据主管部门的监管信任源点，通过发行和存证可以强化数据流通监管。凭证作为政府认可的可信数据载体，具备可验证、可溯源等特点，可以自由通行于各信任载体，并受到主管部门的监管与

保护，进一步实现跨域互信互认、互联互通。

在某省政数局的监管下，提出公共数据资产凭证化的工作思路，由国内头部物流企业大数据平台研发中心完成对数运贷项目的实施。

数运贷在合规前提下，以快速推进数据要素资产化作为战略目标，基于本体数据要素市场化配置的发展要求，申请引入该省政数局主导的数据资产凭证体系，推进与省政数局下属的数据资产凭证运营机构开展数据资产凭证的合规环节运营合作。

2.技术方案

省政务服务数据管理局监制空白数据资产凭证，为数运贷业务的开展建立信任源点。凭证运营中心作为凭证流转的运营主体，向政数局提出申领和签发空白凭证的请求。物流企业根据与商业银行的数据合作协议向凭证运营中心申领数据资产凭证，商业银行接收数据资产凭证，依据隐私计算结果进行联合风控完成放贷。并根据监管要求对凭证进行及时存证。根据监管要求，凭证运营中心及时将数据资产凭证进行存证，并对交易双方进行费用结算。方案技术架构如图 5 所示。具体场景流程:

(1) 企业申请贷款：企业向银行提出贷款申请，通过涉企移动政务服务平台向凭证运营中心提交数据授权;

(2) 银行申购数据资产凭证：银行接收企业贷款申请并审核贷款材料，依贷款申请和授权回执向物流企业申购企业数据;

(3) 物流企业申领凭证：物流企业接收银行的申购申请，并向凭证运营中心申请凭证制作，用以签发实体数据资产凭证;

(4) 凭证运营中心申领凭证：凭证运营中心向政数局申领空白凭证；

(5) 政数局签发空白凭证：政数局向凭证运营中心签发空白凭证；

(6) 物流企业提供计算结果：物流企业接收空白数据凭证，向凭证运营中心提供数据协议报价，并将隐私计算结果写入数据资产凭证；

(7) 凭证中心开具凭证：凭证中心向商业银行发出凭证协议报价，并开具实体数据资产凭证，数据资产凭证同步向政数局进行存证；

(8) 凭证运营中心与商业银行完成运营费用结算；

(9) 凭证运营中心与物流企业进行数据费用结算；

(10) 商业银行根据联合风控模型结果对企业进行评估和放贷。

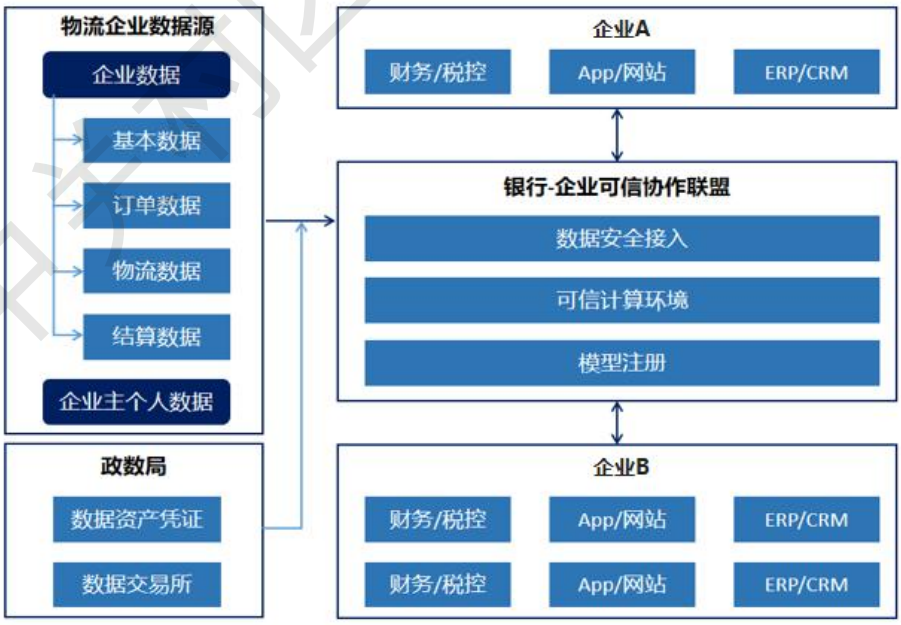

图 5 基于隐私计算+区块链的数运贷方案技术架构

案例通过利用可信计算环境，实现源端数据安全计算，及时可信的利用企业多种经营数据进行计算分析，回传所需指标和模型计算结果，为贷前模型提供更多可用的特征变量，为贷中行为分析/预警、还款管理等提供数据，为贷后预警、交叉销售提供数据依据。并通过使用数据资产凭证，发行合规数据产品，并通过数据交易所完成银企两端数据融合，提升风控管理能力。

五、“区块链+隐私计算”总结与展望

(一)强化核心技术突破，实现跨平台互通

企业面对与不同的数据提供机构合作时，需要部署不同平台，存在着严重的系统建设和运营成本浪费，因此“互联互通”成为了数据流通应用上一直面临的挑战。但是在数据流通过程中，参与机构不可避免存在隐私泄露的顾虑，为了解决数据跨平台互通中的隐私保护的问题，需要加快推进隐私保护核心技术攻关，推动技术成熟度提升，为数据流通过程中的隐私安全保驾护航。此外，还需要推进数据互联互通标准的研究制定，为隐私保护技术提供发展指南，推动数据价值的安全流通。

(二)深化技术协同创新，推动数据可信流通

隐私计算的各种技术在安全性、效率和准确性上各有其不同，具有各自的优缺点，尚未有一项技术可以完美解决隐私保护所面临的全部问题，联邦学习、MPC 和 TEE 等技术的内部结合有助于取长补短，共同发挥更大作用。此外，要想真正发挥隐私计算的技术价值，推动数据可信流通，还需与外部技术不断融合，例如隐私计算与区块链的融合，支持数据流通过程可回溯、可验证、可审计；隐私计算与云计算融合，支持云端数据存储、处理的同时加强安全与隐私控制。

(三)推进隐私计算及区块链人才培养

当前，对区块链和隐私计算的整体认知仍然较浅，尤其是隐私计算专业人才极度匮乏，技术应用落地方案不完善、门槛高、难度

大。面对供不应求的人才市场，后续应完善相关人才培养和教育规划政策的制定，充分发挥科研院所、联盟协会、企业等技术优势，加快推进人才培养，有效连接“产学研用”各方，推进校企合作，明确人才培养标准和课程、拓宽培养渠道，完善和创新人才培养机制。吸引人才还需要依靠良好的产业发展，以产业应用和实体经济发展为导向，带动人才培养。

（四）推动隐私计算+区块链应用落地

隐私计算在多数据流通融合中保护隐私安全效果显著，目前已在政务、金融、医疗、交通、安防等多个行业中均存在广泛的应用场景。区块链的公开可验证性引发了数据使用和隐私保护的矛盾，隐私计算为解决这一矛盾提供了很好的途径，但目前隐私计算与区块链融合主要集中在理论层面，实际应用案例还比较少，后续需要加快探索隐私计算+区块链应用场景和落地应用，加大产业建设力度，推进领军企业建设和示范性应用，为下一步规模化应用推广打好基础。

中关村区块链产业联盟

地址：北京市海淀区学院路 51 号首享科技大厦 2 层

邮编：100083

微信公众号：中关村区块链产业联盟