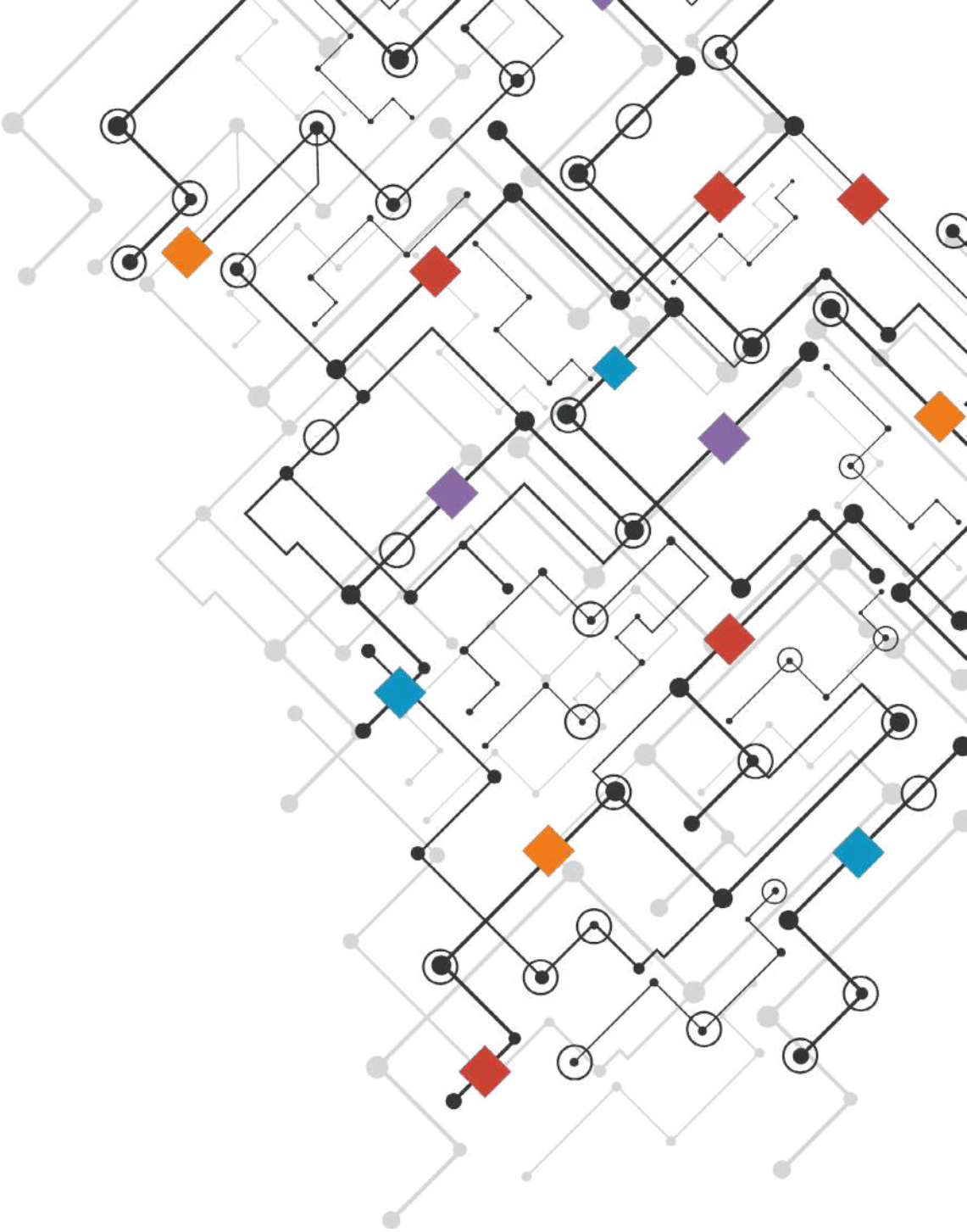
金融壹账通
ONECONNECT



区块链法律合规白皮书

编写单位：深圳壹账通智能科技有限公司

2019-4-16

编委会主任：陈心颖
编委会副主任：叶望春　陈　蓉　程　啸
编写组组长：门雪松　窦文伟　雷志凌　钱　洋
唐明思　王　硕　王　鹏　陆一帆　熊定中
编写组成员：周政宇　王梦寒　冯承勇　覃耀文　童慎微
汤　雯　司　政　严婷婷　张春艳　阮神裕　向子瞭
校　　对：周　燕

目 录

序

科技革命和产业变革深刻影响和改变着人类发展和世界格局，18 世纪中叶以来，人类历史上先后发生了三次工业革命：以蒸汽机为代表的第一次工业革命开创了蒸汽时代、以电力大规模应用为代表的第二次工业革命开创了电力时代、以计算机技术为代表的第三次工业革命开创了信息时代，每一次的技术革命都对社会的发展产生了巨大且不可替代的重要作用。进入 21 世纪以来，全球科技创新空前密集活跃，以人工智能、区块链、云计算、大数据、物联网为代表的新一代信息技术迅猛发展，并加速应用于各领域的深度融合，新产业、新业态、新模式不断涌现，新一轮科技革命和产业变革正深刻的改变着人类的生产和生活方式。

在基于技术带动全球产业变革的新工业革命浪潮中，区块链作为一项推动“信息互联网”向“价值互联网”变迁的颠覆性技术，有望成为全球技术创新和模式创新的桥梁和纽带。区块链技术创新持续加速，核心技术成熟度快速提升，人类借助区块链技术正在打造一个完全有别于当下互联网的全新时代。目前，区块链正在席卷各行业，世界多国已将区块链技术列入国家战略发展范畴，世界 500 强企业也开始全面布局区块链，借助区块链技术重新定义用户关系、商业价值、产业规模、生态模式等，区块链不仅是一场技术革新互联网风暴，而是一场颠覆全球各产业链新兴经济与传统经济，金融行业、市场格局的大变化。

区块链技术具备重构金融业务基础架构的潜力，分布式存储、共识机制、加密算法、智能合约等区块链核心技术，能够显著减少交易信息的不对称，降低数据管理、风险控制的成本，构建信任机制的新形态。保险、银行、证券、资产管理等金融领域都存有强烈的内在需求，通过区块链技术驱动业务升级。

中国平安作为全牌照的金融集团，成立三十年来，始终坚持创新、砥砺前行。随着“金融 + 科技”战略的确立和实施，中国平安正转型成为全球领先的金融集团和科技集团，在人工智能、区块链、大数据、云计算、金融科技、医疗科技等方面均取得重大突破，区块链技术作为核心技术之一，也在金融生态建设中得到广泛应用。金融壹账通作为平安集团“金融 + 科技”双驱动战略的重要载体，致力于区块链基础研究、核心技术研发以及科技成果转化，现已成为区块链技术研究、行业应用的先行者和引领者。其推出的壹账链 BaaS 平台和 FiMAX 底层框架，具有三大优势：一是拥有领先的隐私保护系统和完善的信息安全保护方案，解决机构关心的数据安全问题，通过独创的密码匿踪技术能有效保护链上信息不被泄露；二是具备高性能的底层框架，解决业务关注的效率问题，单链在国密 + 零知识环境下仍可达到万级别吞吐量；三是系统具有更强的完整性和稳定性，满足项目落地的系统需求，在丰富的产品基础上总结的经验，能够提前一步将系统做的更稳定、更完善。

这些优势，帮助金融壹账通在与世界顶级技术公司的激烈竞争中获得胜出，建设上线了香港金管局的香港贸易融资平台、天津口岸区块链试点验证项目、福田汽车“福金 ALL-Link”供应链金融平台等众多前沿项目，为新型金融生态注入了无限想象空间。金融壹账通的区块链技术成果已广泛的应用于金融、房产、汽车、医疗、智慧城市五大生态圈十四个应用场景，未来仍将持续打造开放的区块链平台，从应用于实际业务场景，走向服务于整个金融生态圈、为政府部门和机构赋能。

区域链技术在快速发展应用的同时，也可能冲击人们业已构成的相关法律认知，甚至与已有法律秩序形成冲突。科技需要在法律的轨道上发展，建立健全相关法律法规和政策体系，完善对区块链技术的法律政策规制，提升区块链技术应用的安全评估和管控能力，建设更加高效、均衡、公平的经济和社会秩序，充分发挥区块链等新技术的正面作用，防范和控制利用区域链实施的欺诈、传销、非法集资、非法经营等违规违法乱象，也成为当前亟待研究和解决的问题。

“服务国家、服务社会、服务大众”是中国平安时刻铭记于心的使命和理念。履行社会责任，协同推动区块链健康发展，平安义不容辞。金融壹账通基于世界领先的区块链技术研究和近多个前沿的项目实践，系统梳理了现有的区块链技术及应用的法律制度体系及操作规则，编制了《区块链法律合规白皮书》，对区块链技术带来新问题进行了分析研究，为区块链技术能在更加广阔的领域发展和创新应用提供法律支持。同时，白皮书对数据权属，特别是政务数据、企业数据方面的研究和分析，有助于解决数据孤岛现象，为跨部门协同、精准

快速服务的实现提供法律支持；对链上数据的法律属性、链上数据交互合规、金融领域应用的合规监管等方面的研究和分析，对于理性看待区块链等前沿科技的技术优势，妥善应对潜在风险，支持和保障区块链产业新业务新模式的有序发展，具有重要的参考意义，是非常前瞻性的成果。

“集众智、聚合力、谋大势”，中国平安愿与社会各界共同携手努力，深化科技合作，催生创新动能，用更多更好科技创新成果，协同驱动智能商业的形成，服务社会经济发展。

平安集团副总经理兼首席稽核执行官 叶素兰

二〇一九年四月

前言

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新综合应用，是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种分布式基础架构与计算范式[1]。

区块链技术带来的机遇与挑战已经引起了国家、各行各业的广泛关注。《“十三五”国家信息化规划》将区块链纳入新技术范畴并做前沿布局。标志着从中央政府层面开始推动区块链技术的研发和应用的发展。2018 年以来，全国又有 30 余个省市两级政府颁布了 40 多项政策措施，支持区块链应用，带动地方区块链产业发展。中央和地方各级政府的重视，已经为区块链产业的发展提供了良好的政策环境[2]。无论是传统的金融行业、IT 巨头，还是初创公司或自媒体都参与到了这场科技浪潮中来。以区块链技术为基础，在贸易、通讯、大数据、人工智能及金融科技等多方面正在发生或将要发生一场巨大的变革，各大机构和平台围绕物流和供应链、跨境贸易、信用体系建设和反欺诈、资产管理等业务纷纷布局。

区块链技术应用作为一个蓝海领域，存在未知的风险尚未被完全暴露，因此在进行技术应用的同时，需要做好风险防控工作。区块链的应用项目也是良莠不齐，存在浓厚的投机氛围，虚假炒作，以科技创新为名行非法集资和金融诈骗之实的现象层出不穷。

中国政府已经将区块链纳入监管，相关配套法律、法规、规则及政策文件正在逐步丰富和完善。整体来看，否认比特币、以太币等各色虚拟货币及代币融资的合法性，对各类数字货币交易场所和代币融资平台予以关停退出。到了 2018 年，全国的代币融资（ICO）和比特币等虚拟货币交易场所因涉嫌非法集资、非法证券活动，基本全部实现了退出[3]。国家互联网信息办公室（以下网信办）颁布了《区块链信息服务管理规定》，正式将通过区块链系统或者技术向公众提供信息服务的行为，纳入了互联网信息安全监管范畴。对利用区块链技术进行信息传播的行为进行监督管理。

2018 年 5 月 28 日，习近平总书记在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话中明确提出：“进入 21 世纪以来，全球科技创新进入空前密集活跃的时期，新一轮科技革命和产业变革正在重构全球创新版图、重塑全球经济结构。以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”。区块链技术和应用的发展进入了新的阶段。

为了区块链产业的长远健康发展，有必要在做好技术突破和业务创新的同时，做好风险的防控，商业上的创新应用与监管合规的有效结合是必须考虑的重点问题。区块链项目涉及宏观的法律制度以及微观的人员、安全和操作规则都需要同步建立并配套执行。

本白皮书就区块链项目落地所涉及的合规事项进行初步梳理总结，对区块链的数据权属、区块链数据的法律效力等前沿问题研究探索，并以最新发布的《区块链信息服务管理规定》为核心就区块链项目的网络安全合规进行初步探讨，供各界区块链产业从业者参考。力图为区块链产业的合规稳健发展提供支持。

1. 引自《中国区块链技术和应用发展白皮书（2016》第 5 页。
2. 引自《中国区块链技术和应用发展研究报告（2018）》第 3 页。
3. 引自人民银行条法司副司长龚雁在 2018 年防范和处置非法集资法律政策宣传座谈会上的讲话。

一．中国区块链法律法规政策体系及监管框架

(一) 区块链法律法规政策体系

区块链在中国兴起的时候，政府部门较早的时间就给予了关注。2013 年，政府部门已经关注到了区块链代币的风险并开展了相关治理整顿工作。2016 年 10 月，工业和信息化部（以下工信部）指导下，中国区块链技术和产业发展论坛发布了《中国区块链技术和应用发展白皮书》，这是首次政府指导下的区块链技术文件，自此工信部开始积极推动区块链核心技术和标准的建设工作，标志着区块链技术整体进入了政府治理视野[4]。

现在已经初步形成了对区块链进行规制的法律法规体系，包括了法律、行政法规、部门规章、其他规范性文件及相关政策文件。主要包括有《网络安全法》、《刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定（2019 修订）》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国计算机信息系统安全保护条例》、《互联网信息服务管理办法》、《最高人民法院关于互联网法院审理案件若干问题的规定》、《区块链信息服务管理规定》等。

总体来看，中国区块链的法律法规政策体系的内容，可以分为两大部分：一是鼓励技术探索，规范技术应用；二是强化对区块链网络的信息安全管理。

鼓励技术探索，规范技术应用主要表现在三个方面：一是将区块链技术纳入新技术范畴并做前沿布局，鼓励和支持区块链技术研究和应用的探索；二是认可区块链技术在信息存储和证明领域的应用；三是严格禁止代币发行融资等涉嫌违反法规和监管的业务开展。

1. 鼓励区块链技术探索和运用

国务院已经将区块链技术的研发纳入了国家信息化规划，在 2016 年 12 月 15 日，国务院印发了《“十三五”国家信息化规划》（以下规划），布置了“重大任务和重点工程”，提出“加强量子通信、未来网络、类脑计算、人工智能、全息显示、虚拟现实、大数据认知分析、新型非易失性存储、无人驾驶交通工具、区块链、基因编辑等新技术基础研发和前沿布局，构筑新赛场先发主导优势。”同时还对区块链技术应用发布了指导意见，提出了要在信用体系、供应链、工业互联网等领域加大区块链的应用研究与探索，主要有：（1）要在区块链、大数据、人工智能等交叉融合领域，构建若干产业创新中心和创新网络，促进区块链技术与人工智能的融合，建立新型社会信用体系，最大限度降低人际交往成本和风险；（2）加强供应链信用和监管服务体系建设，研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制，加强对信用评级、信用记录、风险预警、违法失信行为等信息的披露和共享。创新供应链监管机制，整合供应链各环节涉及的市场准入、海关、质检等政策，加强供应链风险管控，促进供应链健康稳定发展。

各中央部委也积极的支持和推动探索区块链技术在供应链、物流、工业网互联网、信用体系建设、信贷风险管理领域的应用。北京、上海、贵州、山东、浙江、重庆等地，陆续出台了支持区块链技术发展的文件，部分地区将区块链发展列入了当地的金融与发展的“十三五规划”中。

4. 引自苏宇《区块链治理之现状与思考，探索多维价值的复杂平衡》 中国法律评论 2018 年第 6 期。

2. 认可区块链技术在信息存储和证明领域的应用

由于区块链具有难以篡改、删除的特点，在确认诉争的电子数据已经保存至区块链后，法院颁布了司法解释，认可区块链技术作为一种保持内容完整性的方法具有可靠性。

2018 年 9 月最高人民法院公布的《最高人民法院关于互联网法院审理案件若干问题的规定》，其中对电子数据的真实性审查就提出了明确的标准，根据该规定第十一条规定：当事人提交的电子数据，如通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院即应当确认。

在具体的审判实践中，采信区块链数据作为证据的案件逐渐增多。

在杭州互联网法院在华泰一媒文化传媒公司诉深圳市道同科技发展有限公司侵害作品信息网络传播权一案，北京东城区法院在中文在线数字出版集团股份有限公司诉北京京东叁佰陆拾度电子商务有限公司侵犯作品信息网络传播权纠纷案，北京互联网法院在北京微播视界科技有限公司与百度在线网络技术（北京）有限公司、百度网讯科技有限公司侵害作品信息网络传播权纠纷案，北京知识产权法院在北京大公网科技有限公司与深圳市美丽视界文化传播有限公司侵害作品信息网络传播权纠纷案中，均采信了区块链取证作为证据。

同时，杭州互联网法院和北京互联网法院分别推进建设司法区块链，用于著作权保护、合同、金融纠纷等领域的电子证据存证，推进电子数据的生产、存储、传播和使用实现全流程可信。

3. 严格禁止区块链技术的违规应用

区块链技术本身中立，但是技术的运用应该遵守相应的业务规则。

从现行监管要求来看，严格禁止以区块链技术开展代币融资活动，否认代币的货币属性，禁止数据货币的交易。2017 年 9 月央行等七委 (中国人民银行、中央网信办、工业和信息化部、工商总局、银监会、证监会、保监会）发布的《关于防范代币发行融资风险的公告》指出，比特币、以太币等所谓虚拟货币，本质上是一种未经批准非法公开融资的行为，代币发行融资与交易存在多重风险，包括虚假资产风险、经营失败风险、投资炒作风险等，投资者须自行承担投资风险。要求即日停止各类代币发行融资活动，已完成代币发行融资的组织和个人应当做出清退等安排。到了 2017 年 11 月底，全国所有已发现的平台均停止 ICO 发行及虚拟货币交易，85 家 ICO 平台均已停止发行和交易，81 家已完成清退工作，余 4 家失联平台已移交相关责任部门处理；88 家比特币交易平台均已停止交易 [5]。人民银行发文要求金融和支付机构禁止开展代币融资和数字货币交易相关业务。

司法机关加大了对通过区块链技术进行违法犯罪活动的打击力度。从 2016 年起，公安机关破获多起以区块链为名的集资诈骗案件。2019 年 2 月 20 日公安部副部长孟庆丰在全国公安机关打击非法集资犯罪专项行动和“猎狐 2019”专项行动视频会上表示：公安机关要把专项行动主攻方向瞄准借助互联网实施的非法集资案件、互联网金融领域的非法集资案件、打着“虚拟货币”等幌子进行网络传销的案件。

4. 加强区块链网络信息安全监管

区块链作为一种全新的信息存储、传播和管理机制，去中心、自治化的特点给现有的网络和数据安全监管政策带来新的挑战 [6]。监管机构逐渐强化监管力度，从政策制定、技术应对等多方面强化区块链网络信息安全。

---

5. 引自《互联网金融风险专项整治工作简报（第 53 期）》。

6. 引自《区块链安全白皮书 - 技术应用篇（2018 年）》第 5 页。

2019 年 1 月 10 日，网信办发布《区块链信息服务管理规定》。该规定明确了网信办作为区块链信息服务的监管执法主体，加强区块链信息服务管理。要求区块链信息服务提供者履行备案手续，建立健全信息安全管理制度和技术保障措施，制定并公开管理规则和平台公约，落实真实身份信息认证制度。服务提供者和服务使用者不得利用区块链信息服务从事法律、行政法规禁止的活动或者制作、复制、发布、传播法律、行政法规禁止的信息内容，对违反法律、行政法规和服务协议的区块链信息服务提供者和使用者，应当依法依约采取处置措施；构成犯罪的，依法追究刑事责任。

(二) 区块链监管框架

区块链目前是复合监管体系，中央网信办、公安部、工信部、人民银行和银保监等根据现有的政府职能分工，分别在相应的主管领域内履行对区块链的监管职责。

5. 网信办

网信办是根据国务院授权，负责全国互联网信息内容的管理工作，并负责监督管理执法。网信办根据国务院的授权，对区块链上信息内容进行监管。出台了《区块链信息服务管理规定》，核心是要防范、处置区块链链上的有害信息。明确了区块链信息安全责任的主体包括区块链信息服务提供者和使用者。并要求在上线新产品、新应用、新功能时，要进行安全评估；区块链信息服务提供者应当对区块链信息服务进行备案，备案系统已经上线。同时要求区块链信息服务提供者应当落实信息内容安全管理责任，对于法律、行政法规禁止的信息内容，具备对其发布、记录、存储、传播的即时和应急处置能力。

6. 公安部

《中华人民共和国人民警察法》第六条规定，公安机关的人民警察负责监督管理计算机信息系统的安全保护工作。《中华人民共和国计算机信息系统安全保护条例》第六条规定，公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

公安机关作为负责监督管理计算机信息系统的安全保护工作的行政机关，主管全国计算机信息系统安全保护工作。在职责范围内，对区块链项目的网络实名制的落实、网络安全管理制度和操作规范的落实、等级保护和关键信息基础设施保护、用户信息和网络日志的留存、计算机病毒和网络攻击或入侵的防范技术措施、禁止发布传输的信息的应急处置措施、内容安全和应用安全管理、个人信息保护、网络产品和服务安全管理等实施情况监督检查，对危害行为进行规制、对涉嫌违法犯罪的行为进行查处。

7. 工信部

工信部承担着统筹规划互联网，监督管理电信和信息服务市场，承担通信网络安全及信息安全管理的责任，推动着区块链技术标准的研究和应用推广。2016 年 10 月 18 日，发布了《中国区块链技术和应用发展白皮书 (2016)》，其中提出了，我国区块链技术发展路线图和标准化路线图等相关建议。2017 年 5 月，在工信部信息化和软件服务业司 (以下信软司) 指导下，首个在政府指导下的国内区块链基础标准——《区块链和分布式账本技术参考架构》标准被正式公布； 2018 年 1 月，工信部发布《区块链数据格式规范》，为区块链行业应用提供统一的数据标准，对国内区块链标准建设具有重要意义。

8. 人民银行和银保监会等金融监管机构

人民银行、银保监会、证监会、互联网金融风险专项整治工作领导小组等金融监管部门负责区块链在具体金融业务场景下的监管。积极开展了区块链技术在金融业务领域应用研究的同时，对具体业务应用有着严格的监管要求。

按照分类监管的原则，根据具体业务的特征，由相应的主体进行监管。如 2018 年人民银行要求支付机构不得为数字货币交易提供支付服务。同时由于区块链技术应用的复杂性，防止监管套利行为的发生，对于一些复杂的问题由人民银行、银保监、证监会、工信部、网信办等多个部门联合发文予以规制，包括否认代币的货币属性，严格禁止开展代币发行融资活动等。

互联网金融风险专项整治工作领导小组（以下互金整治小组）承担着总体推进互联网金融整治工作的职责。区块链技术在金融业务领域的应用，还应遵守互金整治小组的监管要求。

二．区块链技术下的数据权属及数据合规

区块链项目的正常运营，离不开众多主体的建设参与，既可能有行政机关、事业单位，也会有工商企业、银行、保险等各类主体。在数据层面上，各联盟参与主体上传数据，区块链能实现在多方共识的基础上保持数据一致，从而形成交叉验证机制的数据基础，可以在充分保障数据存储与传输的安全性、私密性与可扩展性的前提下，有效查验数据，防止数据被篡改，实现业务流程上的优化、模式创新和新业态培育[7]。但是，区块链上的数据归属于哪一区块链参与主体、各主体对于区块上的各类数据享有何种权利等，需要予以厘清。

有必要在联盟链建设之初就明确数据的权属和使用问题，避免各主体、各层级围绕数据产生矛盾。特别是在网络安全法已经实施，个人信息保护意识和措施不断强化，银行等金融机构已面临更加严格的信息合规监管的情况下，有必要就区块链联盟的数据权属做出研究梳理，构建一套合法、合理，符合监管要求的数据权属安排，促进区块链技术应用的顺利落地和展开。

区块链联盟链项目，主要参与主体为行政机关、企业及其他组织，本白皮书主要就此类组织的数据权属展开分析。

（三）数据新型财产权利的权属分析

9. 数据的民事权利客体属性

数据能否构成民法上的权利客体，理论界存在较大的争议。

否认数据成为权利客体的，主要理由是：一方面数据不构成民法上的客体，数据缺乏民事客体须有确定性或者特定性的基本要求，无法被民事主体所独自和控制。数据缺乏民事客体所要求的独立性，无法控制基于复制、或者网络流通等行为的分享；数据也不构成民法中的“无形物”，不具有类似知识产权所具有的信息垄断性的内在特征。另一方面是数据的非财产性。数据本身不具有独立的经济价值，依赖于载体、代码和其他要素才能发挥作用，不能单独产生经济利益；数据本身不是财产价值的直接来源，价值之源在于数据的控制和自我保护[8]。

支持数据权利的观点，主要认为：第一方面，数据是民法上的客体。数据具有确定性，数据的独占性可以通过法律实现，通过对数据的收集和处理数据的控制者通过法律以规定其义务的方式赋予数据主体对其自身相关数据拥有控制性的权利；数据能够独立存在，能够与其表现的电子形式媒介在观念和制度上进行分离，并具有独立的利益指向。数据是以其所含内容来界定权利义务关系，不是以作为存储在网络的电子形式来加以讨论，数据本身具有信息垄断性的内在特征；第二方面，数据具有财产权属性。数据具有经济价值，数据权利可以转移，实践层面，数据已经作为商品进行交易具有交换价值；第三方面，数据具有人格权属性[9]。

本白皮书认为，数据应当作为民事权利的客体，主要理由是：首先，数据能否作为民事权利客体，关键不在于数据自身的特性，而是法律是否有必要将其作为权利客体，基于特定的需求和价值判断，法律可以赋予民事主体对数据某种垄断性的专属权利而制造稀缺性；其次，数据作为权利的客体，使自然人有权控制个人数据，防止个人数据被泄露和非法利用所引发的问题；还能有效避免人民在日常生活中为获得网络服务、满足对数据产品的使用需求而付出额外成本。最后，数据作为权利客体，有可以促进数据的流动与利用，从而实现社会福利的最大化[10]。

7. 引自《中国区块链技术和应用发展报告》第 23 页。

8. 参见梅夏英：“数据的法律属性及其民法定位”，载《中国社会科学》2016 年第 9 期，第 164-184 页。

9. 参见李爱君：“数据权利属性与法律特征”，载《东方法学》2018 年第 3 期，第 74 页。

10. 参见程啸：“论大数据时代的个人数据权利”，载《中国社会科学》2018 年第 3 期，第 121 页。

10. 传统中心式网络下数据控制者的数据权利

数据控制者对其所合法收集和存储的数据享有何种权益，法律应当如何保护，目前在我国现行法中尚无明确规定，理论界亦未达成共识。

一种观点认为，对数据控制者的数据权利最严密和有效的保护，是承认数据控制者通过合法收集、存储的数据属于新型财产权利，甚至通过排他性权利或绝对权的方式加以保护。例如，程啸教授认为，根据我国《中华人民共和国民法总则》第 127 条规定："法律对数据、网络虚拟财产的保护有规定的，依照其规定"的体系设置，立法者在紧接着人格权、物权、债权和知识产权之后规定，对数据的保护，实际上等于认同了数据的权利是一种新型的财产权利。[11] 龙卫球教授认为数据控制者对于其数据收集和加工产品享有一种"数据资产权"，该权利近似于所有权，是法律对数据控制者的数据资产化经营利益的一种绝对化赋权，既是对其经营效果的一种利益归属确认，更是通过提供便利和安全的保障而鼓励数据资产化交易的一种制度基础。这种赋权是基于劳动正当论而产生的，因此对于数据控制者而言，具有激励其以合法的方式进行加工创造，以此推进数据产业发展的效果。[12] 在美国，也不乏这种观点的主张者，他们认为将数据控制者的数据权利认定为绝对权的好处在于可以明确数据权属，有利于促进数据交易，保障数据市场的秩序。[13] 在欧盟，有观点将数据控制者所收集的数据资产当作数据库特殊权利加以保护。这个观点早在 1996 年的欧盟《关于数据库法律保护的指令》[14] 中就已被提出，即对于不符合独创性标准因而无法受到著作权法保护的数据库，只要数据库制作人在内容收集、核准和提供等方面上有实质性投入（substantial investment），数据库制作人就可以享有特殊权利的保护（sui generis right）。[15] 实践中，欧盟企业不时利用数据库特殊权利来保护数据集合。[16] 不过，欧盟对于数据库特殊权利的适用范围和标准本身仍有争议，尤其何种数量与质量的投入构成"实质性投入"仍然没有共识。[17] 而且由于我国尚未明文规定数据库特殊权利及其保护方式，因此这种观点仅具有理论上的意义。

另一种比较有力的观点认为应当通过反不正当竞争法对数据控制者的权益加以保护。例如，在新浪公司与淘友技术公司、淘友科技公司侵害数据的纠纷案件中，被告淘友公司的脉脉软件抓取、使用了原告新浪公司的新浪微博用户职业信息、教育信息，并通过技术手段获取、使用了原告新浪公司的新浪微博用户对应关系。在该案件中，新浪公司以淘友公司的行为构成不正当竞争行为为由提起诉讼，北京知识产权法院判决认为：淘友技术公司、淘友科技公司违反《开发者协议》，未经用户同意且未经微梦公司授权，获取新浪微博用户的相关信息并展示在脉脉应用的人脉详情中，侵害了微梦公司的商业资源，不正当地获取竞争优势，这种竞争行为已经超出法律所保护的正当竞争行为，构成《反不正当竞争法》意义上的不正当竞争行为，属于一种民事侵权行为。[18] 同样，在美国和欧盟均有观点主张采用商业秘密的方式来保护企业数据。在欧盟，有观点认为 TRIPs 和欧盟《商业秘密保护指令》[19] 所规定的商业秘密，作为对思想与信息的保护制度，可以扩张适用于个人数据，因为商业秘密不仅包括技术知识，还包括如顾客与供应商的信息等商业数据。因此，没有必要将企业所收集和加工的个人数据作为绝对权加以保护，而只要针对他人的特定违法行为进行规制即可，即不法获取、使用与披露数据控制者的数据集合的，应当承担相应的民事赔偿责任。[20] 在美国，也有观点认为数据控制者所收集和加工的数据可以通过《统一商业秘密法》（Uniform Trade

11. 参见程啸："论大数据时代的个人数据权利"，载《中国社会科学》2018 年第 3 期，第 121 页。

12. 龙卫球："数据新型财产权构建及其体系研究"，载《政法论坛》2017 年第 4 期，第 75-76 页。

13.See Andreas Wiebe, Protection of Industrial Data – A New Property Right for the Digital Economy? 12 Journal of Intellectual Property Law & Practice, at 62-71 (2017).

14.Directive No. 96/9/EC on the Legal Protection of Databases.

15.See Jens L. Gaster, The New EU Directive Concerning the Legal Protection of Databases, 20 Fordham Int'l L. J. at 1129-1142 (1997).

16. 参见龙卫球："再论企业数据保护的财产权化路径"，载《东方法学》2018 年第 3 期，第 54、55 页。

17.Estelle Derclaye, Databases Sui Generis Right: Should We Adopt the Spin-Off Theory? 26 European Intellectual Property Review, at 402-413 (2004).

18. 参见"北京淘友天下技术有限公司、北京淘友天下科技发展有限公司与北京微梦创科网络技术有限公司不正当竞争纠纷案"，北京知识产权法院（2016）京 73 民终 588 号民事判决书。

19.Directive(EU) 2016/943 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure.

20.Barbara Anna Radoń, Trade Secrets Protection for "Big Data": Personal Data as Trade Secrets in the European Union, Munich Intellectual Property Law Center Master Thesis (2015/16).

Secrets Act）加以保护。[21] 然而，通过《反不正当竞争法》保护数据控制者对数据的权利，实际上等于将数据控制者的数据权利降格为一种受法律保护的纯粹经济利益，只能在其遭受特定方式侵害的时候获得救济，其保护的强度和密度显然不足。这种保护方法既不利于数据的流动和分享，也无法充分地鼓励数据控制者更多地收集、存储、转让和使用数据。[22]

本白皮书采取第一种观点，即将数据控制者所收集、存储和加工的数据资产作为一种新型财产权利加以保护。财产权的类型与内容，总是随着社会发展而处于流动与变化之中，并没有什么经济利益“一定属于”或者“一定不属于”财产权的客体。法律是否将特定利益作为一种财产权加以保护，取决于立法者想用财产权这一法律工具达成何种法政策目标。“在人们眼中，财产权是什么，取决于人们想用财产权做什么——换言之，人们所欲达成之目的决定了财产权的类型、形式与内容。”[23] 基于目的论的思想，数据控制者对其收集、存储和加工的数据资产是否享有新型财产权利，主要取决于法律政策目标是鼓励数据产业的发展，还是限制数据产业；至于数据权利在多大程度上符合传统民法权利客体的要求，则属于立法与司法技术的范畴。正如程啸教授与龙卫球教授所指出的，赋予数据控制者以新型财产权利的地位，有利于激励数据控制者以合法、支付对价的方式收集数据，有利于推动数据产业的发展。

11. 数据控制者对数据资产取得新型财产权利的正当性基础

数据控制者之所以可以取得数据权利，是因为数据控制者通过合法的、支付对价的收集与存储行为，原始取得了以其所收集和存储的数据为客体的新型财产权利。程啸教授认为，数据控制者对合法收集的个人数据享有应当受到法律保护的权利，并且该权利既不依赖于被收集者的授权，也不依赖于其他在先权利或许可，而是基于以下原因原始取得的权利：首先，就个人数据而言，数据控制者依据法律规定，在公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意收集个人数据的行为是合法的事实行为。其次，数据控制者本身收集、存储个人数据的行为需要付出相应的成本，而且他们向被合法收集个人数据的被收集者支付了合理的对价，符合公平原则，理应产生相应的民事权利。[24] 龙卫球教授也认为数据控制者取得数据资产权的前提条件是其通过自己合法的、具有价值创造意义的收集、存储和加工而产生数据集合。[25]

数据控制者所收集、存储和加工的数据集合须满足一定的条件，才能作为数据新型财产权利的客体，数据控制者才能取得相应的权利。第一，数据集合须作匿名化处理。数据控制者对数据享有的权利，不得对作为数据来源的网络用户隐私等民事权利造成侵害或者带来危险，因此数据控制者首先须在技术上对其所收集的数据集合进行匿名化处理，其才能对数据集合享有新型财产权利。[26] 第二，数据控制者对数据资产所享有的权利，受到目的限制原则的控制。详言之，数据控制者所享有的数据权利的权能，自始就受到数据控制者与网络用户之间所达成的数据收集协议所约定的数据使用目的的约束，数据控制者对数据的利用，不得与约定的目的相违背。[27]

12. 小结：取得数据权利的数据控制者的中心地位

既有研究对数据控制者所收集、存储和加工的数据资产所享有的权利或利益的研究，均以一个基本法律关系为预设：即存在一个中心式的数据控制者，它可能是大型互联网企业，也可能是行政机关，它在提供网络服务的同时，也不断地收集着网络用户的个人数据。尽管

21. 不过，现有的研究仅对特定数据控制者的数据保护提出采取商业秘密的方案，而这些数据控制者所收集的信息如农业数据或者体育联盟数据，和大数据时代通过收集消费者的个人数据所形成的企业数据有所不同。参见 Ellixson, Ashley & Griffin, Terry, Farm Data: Ownership and Protections (September 16, 2016). Available at SSRN: https://ssrn.com/abstract=2839811 or http://dx.doi.org/10.2139/ssrn.2839811，最后一次访问 2018 年 7 月 19 日；also see Lara Grow & Nathaniel Grow, Protecting Big Data in the Big Leagues: Trade Secrets in Professional Sports, 74 Washington and Lee Law Review, (2017).

22. 程啸：“论大数据时代的个人数据权利”，载《中国社会科学》2018 年第 3 期，第 121 页。

23.Stuart Banner, American Property: A History of How, Why, and What We Own, Harvard University Press, 2011. at 289.

24. 程啸：“论大数据时代的个人数据权利”，载《中国社会科学》2018 年第 3 期，第 117-118 页。

25. 龙卫球：“数据新型财产权构建及其体系研究”，载《政法论坛》2017 年第 4 期，第 75 页。

26. 见王融：“关于大数据交易核心法律问题——数据所有权的探讨”，载《大数据》2015 年第 2 期，第 4 页。

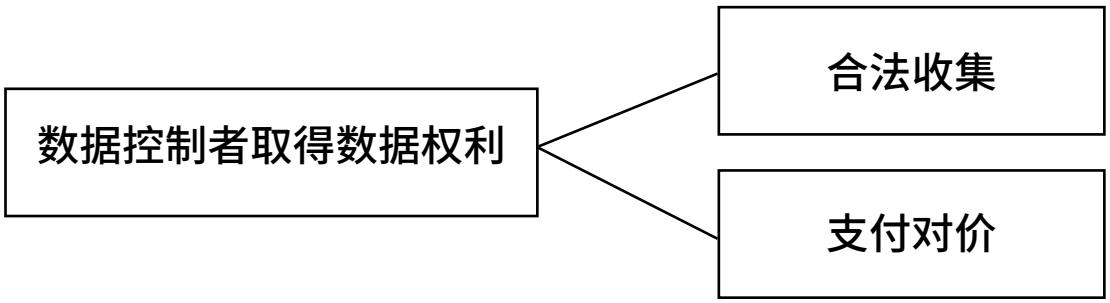
27. 参见梁泽宇：“个人信息保护中目的限制原则的解释与适用”，载《比较法研究》2018 年第 5 期，第 17 页。

数据控制者对其所收集、存储和加工的数据资产享有何种权利或者利益还存在争议，但无论将该种权利认定为新型财产权利，还是认定为商业秘密抑或其他纯粹经济利益加以保护，均以数据控制者是该种权利或利益的享有者为前提进行讨论的。数据控制者取得数据集合的过程也是一种单向度的数据流动过程，即个人数据从网络用户流向数据控制者。

作为网络用户，其对自己使用网络服务时所形成的数据不具有控制的能力。因此 GDPR 等数据规范才授予用户以访问权、更正权、删除权以及反对权等权利，这些权利依其权利内容，在性质上属于请求权，即数据主体有权请求数据控制者告知其个人数据是否被处理以及处理的内容为何；数据主体有权请求数据控制者更正或删除其所收集的某些个人数据等等。[28] 这种权利义务构造，正是以数据控制者作为中心而规定的。

总而言之，传统理论对数据控制者所享有的数据权利及其正当性基础的讨论，均是以中心式数据控制者的存在为前提条件的，这不同于本白皮书接下来将要讨论的去中心式区块数据的场景。

图 1：中心式数据控制者取得数据权利的正当性基础



(四) 区块链数据权属的一般规则

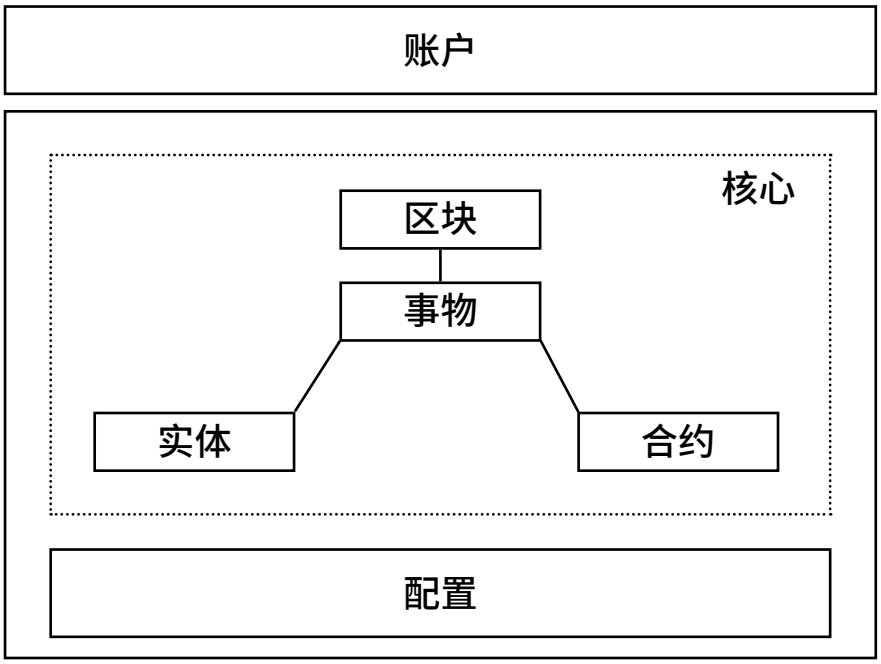
区块链是一种公共数据库，它记录了网际间所有的交易信息，随时更新，让每个参与主体可以通过合法的手段从中读取信息，写入信息。这就带来一个问题，参与主体对于区块链上的数据享有何种权益？既有的中心式数据控制者对数据享有新型财产权利的理论，在区块链技术下是否仍然发挥作用？

13. 区块链上的数据类型

区块链是通过透明和可信的规则，构建不可伪造、不可篡改和可追溯的块链式数据结构。2018 年 2 月，在工业和信息化部信息化和软件服务业司指导、工业和信息化部中国电子技术标准化研究院主办的“中国区块链技术和产业发展论坛第二届开发大会”上，主办方正式发布了《区块链·数据格式规范》（即中国区块链技术和产业发展论坛标准）。该标准将区块链技术数据对象结构划分为区块、事务、实体、合约、账户、配置六类。区块链核心的数据对象包括区块、事务、实体和合约。每一区块数据对象中包含一个或多个事务数据对象，每个事务对象包括属性类的实体数据对象，还包括事务的业务逻辑，即合约数据对象。在区块链核心数据对象之外，包括配置数据对象，提供区块链系统正常运行过程中所需的配置信息。配置数据对象和区块链核心数据对象共同构建了区块链运行所需的基础数据基础。而账户数据对象表示区块链业务的实际发起者和相关方对应的数据结构。

28.Matthias Berberich & Malgorzata Steiner, Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers, 2 Eur. Data Prot. L. Rev. 422 (2016), at 424.

图 2：数据视图相关的实体间关系



并以此为基础，将区块链数据分为以下六类：

以数据对象的类别为依据，将区块链上的数据可以分为六类，即账户数据、区块数据、事务数据、实体数据、合约数据、配置数据。其中，账户数据是指描述区块链事务的实际发起者和相关方的数据。区块中记录的事务信息均被关联到相关的账户之上，每个区块链服务客户拥有一个或多个账户来使用区块链服务。区块数据是指区块链网络的底层链式数据，用来把一段给定时间内发生的事务处理结果持久化为成块链式数据结构。事务数据是指描述区块链系统上承载的具体业务动作的数据，既包括交易类型事务，也包括非交易类型事务。实体数据是指描述事务的静态属性的数据，通常包括发起方地址、接收方地址、交易发生额、交易费用、存储数据和实体数据备注。合约数据是指描述事务的动态处理逻辑的数据。合约又称智能合约，是一套以计算机代码形式定义的承诺，以及合约参与方可执行承诺的协议。配置数据是指区块链系统正常运行过程中所需的配置信息。[29]

（五）区块链数据的权属分析

区块链参与主体将事务数据、实体数据或合约数据“上传”至区块链的技术，本质上是通过特定的哈希算法和 Merkle 树数据结构，将一段时间内接收到的交易数据和代码以及其他任意数据封装到一个带有时间戳的数据区块中，并链接到当前最长的主区块链上，形成最新的区块。[30]

29. 中国区块链技术和产业发展论坛：《区块链·数据格式规范》。

30. 袁勇等：“区块链技术发展现状与展望”，载《自动化学报》2016 年第 4 期，第 484 页。

14. 区块链参与主体对区块链上非自己上传的数据不享有新型财产权

本白皮书认为，基于区块链的技术特征，任何节点或区块链参与主体对于整体的区块数据均不享有如同中心式的数据控制者对其合法收集、支付对价的数据集合相同或相似的新型财产权利。具体理由阐述如下：

第一，从数据主体而言，区块链应用场景下不存在一个中心式的数据控制者收集和存储数据。由于区块链系统的节点一般具有分布式、自治性、开放可自由进出等特性，因而，一般采用对等式网络（Peer-to-Peer network，P2P 网络）来组织分散的参与数据验证和记账的节点。P2P 网络中的每个节点均地位对等且以扁平式拓扑结构相互连通和交互，不存在任何中心化的特殊节点和层级结构，每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能。因此，在整个过程中，均不会涉及中心化的第三方，也不会在一个中心化服务器中存储任何数据。[31]

具体而言，区块链参与主体将数据上传至区块链的技术特征包括以下两个环节：第一，任一区块数据生成之后，将由生成该数据的节点广播到全网其他所有的节点来加以验证。第二，P2P 网络中的每个节点都时刻监听区块链网络中广播的数据和新区块，节点接收到邻近节点发来的数据后，将首先验证该数据的有效性：如果数据有效，则按照接受顺序为新数据建立存储池以暂存尚未记入区块的有效数据，同时继续相邻近节点转发；如果数据无效，则立即废弃该数据，从而保证无效数据不会在区块链网络继续传播。[32]

因此，从区块链的数据层与网络层设计机理可见，区块链是典型的分布式大数据技术。全网数据同时存储于去中心化系统的所有节点上，即使部分节点失效，只要仍存在一个正常运行的节点，区块链主链数据就可完全恢复而不会影响后续区块数据的记录和更新。这种高度分散化的区块链存储模式与传统意义上的大数据存储模式的区别在于：前者是完全“去中心化”的存储模式，后者则是基于中心化结构基础上的数据备份模式。[33] 换言之，基于区块链技术的数据上传与共享技术，并没有将数据存储在任何一个中心机构的服务器上，而是所有的区块链参与主体均同时存储了区块链上的所有数据。

第二，从数据产生过程而言，任一区块数据生成之后的广播与其他节点的监听、接收和验证数据有效性的过程，不同于数据控制者“收集”数据的过程。数据控制者对于数据的“收集”其实包含以下一系列的技术过程：首先，数据控制者通过传感器收取、射频识别（RFID）、数据检索分类工具以及移动设备的应用软件等，对网络用户的数据进行采集。其次，数据控制者将各种各样的、结构复杂的数据转换为单一的或便于处理的结构；并且，在数据处理的过程中设计一些数据过滤器，通过聚类或关联分析的规则方法进行数据清洗；然后才将这些整理好的数据进行集成和存储。数据处理与集成是非常重要的一步，如果单纯随意地放置数据，很容易产生数据访问性的困难，导致采集的数据无法利用。[34] 换言之，“数据收集”并不只是简单随意地采集和存储数据，而是在采集之后，通过一定的技术手段对数据进行初步加工，形成有利用可能性的数据集合。

在区块链技术下，某一节点对于其接收的数据进行验证并且暂存在区块链的行为不具有数据控制者进行数据收集的技术特征。[35] 一方面，各个节点对数据进行接收和验证的行为，只是采取一定的技术手段，对生成的区块数据的合法性进行验证，例如采取工作量证明，即各个节点消耗自身算力尝试不同的随机数，进行指定哈希计算，并不断重复该过程直至找到合理的随机数，随后生成区块信息，记录交易数据。[36] 这个过程并不涉及对数据进行初步的处理和清洗，只是将原始交易数据记入区块链而已。另一方面，最终记入区块链的交易数据，并非存储在某一个节点的服务器上，而是同步地在各个节点上均出现相同的数据。这也不同于数据控制者主动或被动进行数据搜集并储存在自己服务器上的行为模式。

---

31. 参见 [加] 唐塔普斯科特、亚历克斯·塔普斯科特著，《区块链革命》，凯尔、孙铭、周沁园译，中信出版集团 2016 年版，第 33 页。
32. 袁勇等：“区块链技术发展现状与展望”，载《自动化学报》2016 年第 4 期，第 486 页。
33. 袁勇等：“区块链技术发展现状与展望”，载《自动化学报》2016 年第 4 期，第 486-487 页。
34. 刘智慧、张泉灵：“大数据技术研究综述”，载《浙江大学学报》（工学版）2014 年第 6 期，第 962 页。
35.Nakamoto S.： Bitcoin: a peer-to-peer electronic cash system, available: https://bitcoin.org/bitcoin.pdf, 2009.
36. 长铗、韩锋等著：《区块链：从数字货币到信用社会》，中信出版集团 2016 年版，第 62 页。

因此，如果说数据控制者对于其所合法收集的数据享有新型财产权利，是因为数据控制者在收集数据的过程中付出劳动，如同“民事主体合法建造房屋而自该房屋建造完毕之时取得房屋的所有权”，[37] 那么区块链各个节点对区块数据的接收和验证，并没有对数据本身产生任何加工活动，而只是单纯的按照既定的自动规则进行验证和同步。在技术上更为重要的是，此种验证和同步是区块链技术的本质特征，按照中心式数据控制模式下的应用场景来理解，它更像是一种网络存储技术。显然，任何人都不会认为仅仅提供网络存储服务的平台对用户上传的数据拥有任何权利。从这个角度理解，就更能更清晰的看出，区块链参与主体实则对于区块数据并不享有如同数据控制者相同的数据权利。当然，各个节点对区块数据进行接收和验证的过程确实是一个消耗电力与算力的工作，但是区块链的底层技术结构已经为该工作支付了对价，如比特币区块链技术就赋予那些率先完成区块创建的人能够得到一定数量的比特币，把价值作为激励，促使参与主体有动力保证比特币平台的长期成功，购入顶尖装备来挖矿，并更高效地花费能量从而维护账本。[38]

第三，任何节点在监听、接收和验证数据有效性的过程，均不存在对产生区块数据的节点支付对价的行为。根据公平原则的要求，数据控制者之所以可以取得其所收集的数据的财产权利，是因为其向产生数据的网络用户支付了对价，这些对价即可能是直接的经济回报，也可能是免费或者低价使用的各种数据产品和软件服务。但是，区块链技术中对区块数据进行监听、接收和验证数据的一方，并没有义务向广播区块数据的节点支付对价。恰恰相反，由于接收节点对数据进行验证的过程需要花费电力和算力，因此区块链的底层技术结构向接收节点奖励一定的价值作为激励措施。这与数据控制者向网络用户支付对价的权利义务结构存在天壤之别。

综上所述，本白皮书认为，除非当事人之间存在明确的约定或者法律有相应的规定，否则基于区块链本身的技术特征，任何节点或区块链上的参与主体对于区块链上记载的且并非自己上传的数据，都不享有任何财产权益。

15. 区块链联盟链可以对数据权属做特别约定

尽管区块链的技术特征并没有授予任何节点对区块数据享有数据权益，但是，在联盟链中，联盟参与主体可以通过特别约定，确定数据权利的归属。

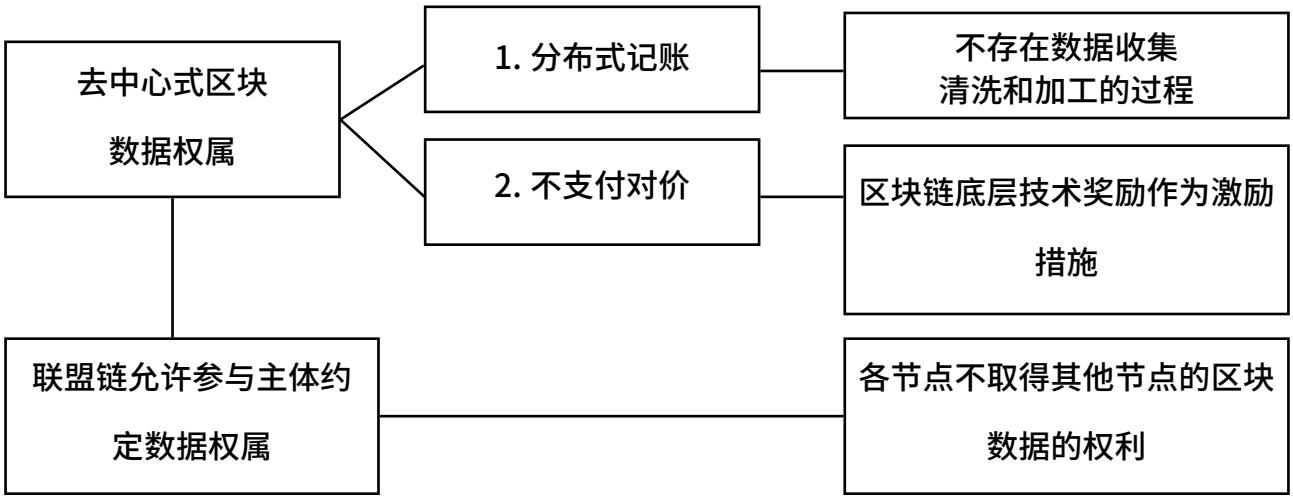
首先，联盟参与主体对于自己上传至区块链上的数据享有新型财产权利。因为，这些数据可能是联盟参与主体自己收集、存储和加工的数据资产，也有可能是联盟参与主体制作的有关资料。总之，这些数据资产均是联盟参与主体根据中心式的数据收集活动所获得的，因此联盟参与主体对这些数据资产享有新型财产权利。联盟参与主体可以将这些数据上传至区块链，也可以和其他联盟参与主体达成合意，确定这些数据资产的权属。不过，从反面而言，各个联盟参与主体也仅对自己上传至区块链上的数据享有权属权利，只能授权他人知悉和利用自己享有权利的数据。

其次，联盟链的技术特征允许联盟参与主体之间就数据权属进行特别约定[39]。所谓联盟链（Consortium Blockchain），是指参与区块链的节点是事先选择好的，节点间通常有良好的网络连接等合作关系，区块链上的数据可以是公开的也可以是内部的。因此，联盟链是部分意义上分布式、“部分去中心化”的区块链。联盟链允许预先约定各个节点对区块链的访问权限，例如，可以允许每个节点可读取，或者只受限于共识验证参与者，或走混合型路线，如区块的根哈希及应用程序接口对外公开，允许外界用来进行区块链数据和区块链状态信息的查询等。不过，联盟参与主体对数据权属的特别约定应当满足法律规定，即不得侵害他人商业秘密或个人隐私（商业秘密为主）。

37. 程啸：“论大数据时代的个人数据权利”，载《中国社会科学》2018 年第 3 期，第 118 页。
38. 参见 [加] 唐塔普斯科特、亚历克斯·塔普斯科特著，《区块链革命》，凯尔、孙铭、周沁园译，中信出版集团 2016 年版，第 35 页。
39. 参见长铗、韩锋等：“区块链：从数字货币到信用社会”，中信出版集团 2016 年版，第 52 页；另参见袁勇等：“区块链技术发展现状与展望”，载《自动化学报》2016 年第 4 期，第 490 页。

基于联盟链的这一技术特点，各个节点可以在创建基础区块链时就区块数据的权属问题在《跨境贸易区块链联盟章程》中进行约定：一方面，在内容上可以约定某个节点对区块数据享有收集、存储和利用的权利，或某些节点对区块数据只具有访问和查询的权限，但不得利用这些数据资产；另一方面，该章程的具体内容应当通过书面形式进行订立。

图 3：去中心式区块数据的数据权属



(六) 政务信息资源的权属分析

随着电子政务建设的不断完善，行政机关在履行职责过程中越来越大量地收集和获取的个人数据，也形成了具有财产价值的数据集合。行政法上将行政机关在依法履行行政职能中所收集的数据集合称为“政务信息资源”。《国务院关于印发政务信息资源共享管理暂行办法的通知》规定，政务信息资源是指政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或者通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。随着政务信息资源在政府部门之间的广泛流动和大量交换，这些数据集合的权属亟待明确。

实践中，有一些地方性法规将政务信息资源的权属界定为国家所有。如 2015 年 2 月 15 日福建省政府通过的《福建省电子政务建设和应用管理办法》第 9 条[40]、2015 年 8 月 28 日汕头市政府通过的《汕头经济特区电子政务建设管理办法》第 27 条第 2 款[41] 规定了政务信息资源属于国家所有，由电子政务实施单位的同级人民政府电子政务管理部门负责综合管理。有的学者对此表示赞同，认为将政务信息资源界定为国家所有，意味着政务信息资源属于公共资源，公众可以接近或使用政务信息资源，避免政府部门独占该数据资产。[42] 本白皮书赞同这一观点。

40.《福建省电子政务建设和应用管理办法》第 9 条：应用单位在履行职责过程中产生的信息资源，以及通过特许经营、购买服务等方式开展电子政务建设和应用所产生的信息资源属于国家所有，由同级人民政府电子政务管理部门负责综合管理。

41.《汕头经济特区电子政务建设管理办法》第 27 条第 2 款：电子政务实施单位在履行职责过程中产生的信息资源，以及通过特许经营、购买服务等方式开展电子政务建设和应用所产生的信息资源属于国家所有，由市电子政务主管部门负责综合管理。

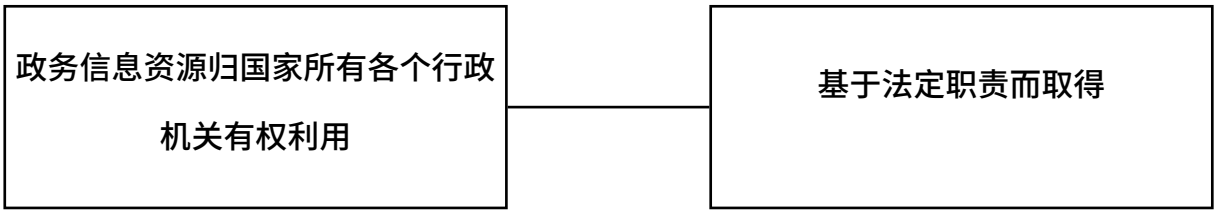
42. 参见曾娜：“政务信息资源的权属界定研究”，载《时代法学》2018 年第 4 期，第 32-33 页。

值得注意的是，国家取得政务信息资源的所有权与企业等数据控制者对其所收集、存储的数据资产取得新型财产权利的原因有所不同。一方面，企业等数据控制者收集个人数据的正当性基础在于获得自然人的同意；而行政机关收集政务信息的正当性基础在于行政机关履行法定职责以及行政相对人的法定义务。另一方面，数据控制者获得数据财产权利的原因是数据控制者经过合法收集、存储和加工数据，并且支付了合理对价这些事实行为；但行政机关取得数据权利的原因是由于公共政策的考虑，将政务信息资源界定为国家所有，并且各个行政机关有权利用，有助于行政机关履行其法定职责，也有利于促进政府各个部门之间的数据共享。

因此，行政机关对于政务信息资源的新型财产权利并不取决于行政机关是通过何种方式来收集、加工和存储相关政务信息资源的。即便是行政机关委托数据企业进行收集的政务信息，虽然数据企业是真正进行数据采集、数据清洗和加工的主体，但只要该信息属于行政机关履行职责过程中应当获取的信息，数据企业所收集的政务信息资源也应当归属于国家所有。即便行政机关是采用区块链技术的方式获取政务信息资源，国家也取得该政务信息资源的所有权，这并不因为区块链技术中不存在一个中心式的数据控制者而有所不同。

综上所述，行政机关在履行法定职责的过程中，依照法律规定直接或者通过第三方服务所获取和制作的各类政务信息资源，应当属于国家所有，各个行政机关对此享有依法存储、利用和共享的权力。

图 4：政务信息资源的数据权属



(七) 联盟链技术背景下区块链数据权属的一般规则

基于上述分析，在联盟链的技术背景下，确定区块链中数据的权属应当遵循以下规则：

规则一：在没有特别约定或者法律另有规定的情况下，基于区块链的技术特征，任何节点或区块链参与主体对于区块链上记载的、非自己上传的数据均不享有任何财产权益。

规则二：联盟链允许各参与主体对区块数据的权属与利用方式进行特别约定，但各个参与主体仅能对自己所有的数据进行特别约定，且该约定不能违反法律行政法规的强制性规定。

规则三：行政机关在履行法定职责的过程中，依照法律规定直接或者通过第三方服务所获取和制作的各类政务信息资源，应当属于国家所有，各个行政机关对此享有依法存储、利用和共享的权力。

(八) 区块链技术下数据交互合规

区块链技术对业务流程的优化提升，主要体现在业务场景中，各参与主体数据同步至区块链上，通过区块链技术的数据交互（授权）、自动交叉验证、共识机制和智能合约，来打通各业务阶段，实现各环节的优化。区块链各参与主体间的数据交互的合法性，尤其是涉及政务、金融领域的应用时，政府机关、金融机构和其他主体间的数据交互合法性显得尤为重要。本白皮书在此简要提示链上主体间的数据交互风险及合规建议。

根据区块链上各主体间数据交互的流程和方式，以下将从区块链各参与主体数据上传云计算存储、数据授权、信息自动通知（状态通知）、交叉验证及重复融资检测几个方面进行简要的风险和合规提示。

16. 数据上传云计算存储

首先，区块链参与主体需要将自己所掌握的相应数据上传至区块链中。如果区块链的节点部署在第三方云平台平安云上，区块链各参与主体的数据皆上传存储在云服务器中，获取数据后，保存到本地存储中；调用云计算的接口发送信息入链。参与主体对外接入局域网和云计算上的智能服务通过数据加密加签传输的方式保证安全。

区块链的参与主体在自己的二级节点上对数据进行加密，并将数据的密文保存在区块链上。区块链的其他参与者只能读取数据的密文，未被授权的参与主体无法对密文数据进行解密，确保了数据的隐私性。同时，区块链参与主体可以通过授权的方式，允许其他参与主体可以查看某条加密数据或某条数据中的某些字段信息。授权操作通过系统中的安全通信通道，数据提供方将待授权数据的解密密钥发送给数据接收方。数据接收方可以从链上读取到数据的密文信息，并使用接收到的解密密钥对数据执行解密操作，得到明文数据。

在上述数据交互过程中，云计算仅是作为提供数据存储和交互服务的平台，区块链参与主体上传的数据为密文数据，云计算的运营方或其他任何第三方在未经该主体授权的情况下无法获取明文数据。在此云计算作为数据传输的中转站，是优化了原有的数据交互方式（例如纸质通知），但并未改变原有的数据提供方和数据接收方，在数据提供方上传的数据不涉及国家秘密等有强制存储要求的数据类型的情况下，以云计算作为区块链的节点部署平台并存储上链的密文数据本身并不违反法律相关规定。

17. 数据授权

在数据交互过程中，密文数据经授权后将成为明文数据在数据提供方和数据接收方间流转，对此，在数据授权阶段，相关主体需注意商业秘密保护及个人信息保护方面的法律风险：

（1）商业秘密保护。各参与主体需要首先评估授权的字段是否会涉及自身的商业秘密。其次，需关注授权的字段是否包含他人的商业秘密，他人是否（通过数据标示或协议约定等方式）允许自己转授权。信息接收方也需核查授权方是否有权授权接收方查看此条明文数据。

（2）个人信息保护。对于涉及个人信息的情况，如物流领域的应用中，若需将收件人的身份、地址、电话等个人信息提供给第三方时，需特别注意符合个人信息保护相关法律法规的要求。

鉴于《中华人民共和国网络安全法》《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》于 2017 年 6 月 1 日施行，配合之前已有的部分相关个人信息保护的法律法规，我国已形成了一套体系化的，从民事、行政及刑事全方位覆盖的个人信息保护制度，个人和单位都需遵守，如有违反则需承担相应法律责任。如《中华人民共和国民法总则》第一百一十一条规定，“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”《中华人民共和国消费者权益保护法》第二十九条亦规定，“经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。经营者及其工作人员对收

集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。”《中华人民共和国电子商务法》第二十三条规定：“电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。”第二十五条规定：“有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全，并对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。”

因此各主体需特别注意在收集、授权和转授权等过程中数据交互的合规，以免遭受商业损失甚至承担刑事责任。

18. 各类授权方式的风险提示

具体到本试点项目的授权形式的相关风险，除上述概要风险外，在此针对各种授权方式的风险简要提示如下：

（1）逐条数据或逐个字段的手动授权

根据项目需求说明书，手动授权是为最基础的数据访问授权形式。每个链上参与方均可指定某条加密数据或某条数据中的某些字段向链上特定的其他参与方进行授权。完成授权后，被授权方将对这些特定数据始终保留解密权限。

对此，建议设置授权方可撤销或更改授权，以便在错误授权的情况下，使被授权方无法再行解密，减少授权方损失。

（2）基于时间区间的数据自动授权

根据项目需求说明书，每个链上参与方均可指定时间区间将自身的业务数据授权给相关业务方，可包含过去的时间段也可包含未来的时间段。对于过去的时间段，即认为是将该时间段内已经发生了的业务进行批量授权；如果包含了未来的时间段，则在时间区间范围内新发生的业务会自动授权给被授权方。授权时，由数据所有人配置授权的具体字段。授权时间可以根据业务需求自行定义，建议与业务合作时限相匹配。业务合作关系终结时，数据所有人可手动提前解除授权关系。

此种情况下，需特别注意授权数据是否可能包含第三方的商业秘密和 / 或个人信息，授权方是否有转授权的权限。

（3）基于业务关联性的数据自动授权

在实际业务中，业务之间存在着派生的关系，如销售业务会派生出货运业务，由于派生业务通常是对原生业务的一项服务，所以系统中可将派生业务设定为对原生业务所有人自动授权（可配置授权哪些字段）。此类授权不针对特定参与主体，如物流企业可同时服务于多家贸易企业，贸易企业对每一单物流信息的授权将自动基于运输业务与订单之间的关联关系向原生业务的所有人进行匹配。此类授权，没有时间限制。

对此，同样需特别注意授权范围，以及转授权是否已获许可的问题。

三．区块链数据的法律效力

在区块链技术下，进行各项业务的主要依据是经各个主体上传并交叉验证后的数据，因此区块链上数据的法律效力十分重要。在政府行政事务领域，行政机关可以通过区块链技术交叉验证行政相对人提供信息的准确性，并作出具体的行政行为，而行政相对人有权对行政行为提起复议，甚至提起行政诉讼。在金融领域，各业务主体通过区块链技术上传、验证数据，并开展具体的业务。因此，确保区块链上数据的法律效力是通过区块链技术开展业务的基础。

（九）立法认可区块链数据作为电子证据的有效性

有关电子数据的证据效力，在我国经历了一段从无到有，从概念化到落实具体操作程序的发展阶段。最高人民法院曾于 2002 年发布了《最高人民法院关于行政诉讼证据若干问题的规定》，其中第六十四条规定：以有形载体固定或者显示的电子数据交换、电子邮件以及其他数据资料，其制作情况和真实性经对方当事人确认，或者以公证等其他有效方式予以证明的，与原件具有同等的证明效力，但尚未作为法定的证据种类予以明确。

例如此前在证券行政案件的审理过程中，因证券交易和信息传递电子化、网络化、无线化等特点，电子交易信息、网络 IP 地址、通讯记录、电子邮件等电子数据证据在证券行政案件中至关重要，2011 年最高人民法院颁布了《关于审理证券行政处罚案件证据若干问题的座谈会纪要》，该纪要特别提出“由于电子数据证据具有载体多样，复制简单、容易被删改和伪造等特点，对电子数据证据的证据形式要求和审核认定应较其他证据方法更为严格。”电子数据只有在符合一定要求的情况下才能作为证据提交。

而 2014 年修改《中华人民共和国行政诉讼法》，在第三十三条有关证据种类的规定中加入了电子数据这一类别，从法律层面认可，电子数据若经法院审查属实，能作为认定案件事实的根据。

2015 年修改的《电子签名法》第八条规定，查数据电文作为证据的真实性，应当考虑以下因素：（1）生成、储存或者传递数据电文方法的可靠性；（2）保持内容完整性方法的可靠性；（3）用以鉴别发件人方法的可靠性；（4）其他相关因素的规定。

而区块链作为一种去中心化的电子数据留存技术手段，具有开放性、分布式、不可逆性等特点，通过区块链技术留存的数据仍是电子数据，是属于法定的数据种类，可以在行政审判过程中作为证据材料提交并使用。

（十）司法解释明确区块链数据作为电子证据的有效性

技术层面上，区块链的分布式 IT 架构具有去中心、透明开放、状态一致、强依赖密码学的特征；在这些特征基础上，数据层面上，区块链能实现在多方共识的基础上保持数据一致，防止数据被篡改，并可对基于数据的应用全过程进行溯源 [43]。基于这一技术特征，区块链技术非常适合应用在电子证据的保存和真实性审查中。

当前对电子数据真实性的审查判断主要依靠公证程序，且基本为形式审查，程序复杂繁琐，证明力不强。互联网法院案件在线审理和大量证据在线的特征，客观上要求打破通过公证程序认定真实性的单一途径，通过技术手段和相关配套机制对电子数据真实性作实质性认定 [44]。

43. 引自《中国区块链技术和应用发展研究报告（2018）》第 23 页。

44. 参加胡仕浩、何帆、李承运《关于互联网法院审理案件若干问题的规定》的理解与适用》，《人民司法（应用）》2018 年 28 期第 24 页。

2018 年 9 月最高人民法院公布的《最高人民法院关于互联网法院审理案件若干问题的规定》，其中对电子数据的真实性审查就提出明确的标准，根据该规定第十一条规定：当事人对电子数据真实性提出异议的，互联网法院应当结合质证情况，审查判断电子数据生成、收集、存储、传输过程的真实性，并着重审查以下内容：

（1）电子数据生成、收集、存储、传输所依赖的计算机系统等硬件、软件环境是否安全、可靠；

（2）电子数据的生成主体和时间是否明确，表现内容是否清晰、客观、准确；

（3）电子数据的存储、保管介质是否明确，保管方式和手段是否妥当；

（4）电子数据提取和固定的主体、工具和方式是否可靠，提取过程是否可以重现；

（5）电子数据的内容是否存在增加、删除、修改及不完整等情形；

（6）电子数据是否可以通过特定形式得到验证。

当事人提交的电子数据，如通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院即应当确认，进一步明确认可区块链可作为电子数据收集的技术方式。

（十一）审判实践对区块链数据作为有效证据的认可

司法审判实践中，在《最高人民法院关于互联网法院审理案件若干问题的规定》颁布之前，互联网法院已经开始认可区块链技术在保存电子证据方面的真实性和可靠性。

2018 年 6 月杭州互联网法院在华泰一媒文化传媒有限公司（以下华泰一媒）诉深圳市道同科技发展有限公司（通道科技）侵害作品信息网络传播权的案件，是中国法院首次对采用区块链技术存证的电子数据的法律效力予以确认。该案中：原告华泰一媒将通道科技刊载了侵权文章的网页进行了截图，并对该网页的源代码进行获取，并将操作日志、记录调用时间等内容打包压缩后，计算了哈希值上传到了 FACTOM 区块链和比特币区块链进行了电子数据保存。

杭州互联网法院根据华泰一媒提交的账号、密码登陆保全网下载侵权保全文件包，其中包含的网页显示第一女性时尚网（Ladyfirst.com.cn）中发布了被诉侵权文章，经查看，正文内容与涉案文章基本一致。其中网页源码操作显示源码为 www.ladyfirst.com.cn，经查询，该网址备案主体为道同公司。将上述侵权保全文件包进行哈希值计算，并根据千麦司法鉴定中心提供的 FACTOM 区块链和比特币区块链的查询方法和步骤进行查询可知，该哈希值存在于上述区块链中，且上传时间与文件包形成时间存在合理性，根据区块链机制可知该涉案电子证据已上传至区块链进行保存且未被修改。[45]

杭州互联网法院的法官认为，在实践审判中应以技术中立、技术说明、个案审查为原则，对该种电子证据存储方式的法律效力予以综合认定，既不能因为区块链等技术本身属于当前新型复杂技术手段而排斥或者提高其认定标准，也不能因该技术具有难以篡改、删除的特点而降低认定标准，应根据电子数据的相关法律规定综合判断其证据效力。由于区块链具有难以篡改、删除的特点，在确认诉争的电子数据已经保存至区块链后，作为一种保持内容完整性的方法具有可靠性。

45. 引自卢忆纯 《区块链电子存证的法律效力认定》作者系杭州互联网法院。

2018 年 10 月，北京东城区法院在中文在线数字出版集团股份有限公司诉北京京东叁佰陆拾度电子商务有限公司侵犯作品信息网络传播权纠纷案中，就区块链在保持电子数据完整性、方法可靠性的审查方面，认为：通过第三方存证平台完成取证后，该平台自动生成了一个唯一对应且进行加密的数字指纹（哈希值），然后生成载有哈希值、区块链保全 ID、取证时间等信息的数据保全证书，从而保证了电子数据的完整性。

2019 年 1 月 24 日，北京互联网法院在北京微播视界科技有限公司与百度在线网络技术（北京）有限公司、被告百度网讯科技有限公司侵害作品信息网络传播权纠纷一案中，原告提供了 ICP 备案信息查询、抖音网站首页截图、抖音手机软件（Android 系统和 iOS 系统）开发者信息截图、谢某出具的授权书、（2018）京东方内民证字第 10028 号公证书、（2018）粤广南粤第 8614 号公证书、伙拍小视频手机软件（Android 系统和 iOS 系统）开发者信息截图及相应的区块链取证证书，“全国党媒平台纪念 5.12 互动活动总参与量超 6 亿”网页截图及区块链取证证书作为证据，法院予以采信。

（十二）互联网法院司法区块链建设推进电子证据全流程可信

除了在具体案件中采信区块链数据作为电子证据之外，杭州互联网法院和北京互联网法院分别推进建设司法区块链，用于著作权保护、合同、金融纠纷等领域的电子证据存证，推进电子数据的生产、存储、传播和使用实现全流程可信。

杭州互联网法院建设的司法区块链，由三层构成：一是区块链程序，用户可以直接通过程序将操作行为全流程的记录于区块链，如在线提交电子合同、维权过程、服务流程明细等电子证据；二是区块链的全链路能力层，主要是提供了实名认证、电子签名、时间戳、数据存证及区块链全流程的可信服务；三是司法联盟层，即使用区块链技术将公证处、CA ／ RA 机构、司法鉴定中心以及法院连接在一起的联盟链，每个单位成为链上节点。

四 . 区块链信息合规监管

信息安全是区块链运行的基础，是上链主体真实身份确认，数据一致性验证等核心功能正常实现，区块链系统稳定运行的保障。区块链去中心化的特点，还带来了商业秘密和隐私保护方面的新问题。需要对区块链系统的信息安全进行专门的讨论。

(十三) 区块链信息安全监管要求

我国《网络安全法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《全国人民代表大会常务委员会关于维护互联网安全的决定》等法律法规都对信息安全做出了明确的要求，区块链作为新一代的网络信息技术，区块链产品和服务运营者应该遵守现有的网络信息安全要求。

19. 区块链网络运行安全保障义务及合规建议

《网络安全法》第十条要求：建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

由于区块链技术整体仍处于不断演变，逐步成熟的阶段中，还缺乏强制性的国家标准，少量基础性的标准处于研制阶段。全国信息安全标准化技术委员会正在推进区块链安全标准化的工作，成立了信息安全评估小组，信息安全管理工作组、大数据安全特别工作组等，开展多项研究工作，包括区块链应用安全管理基本控制措施、风险模型，区块链安全的一致架构设计，区块链开发平台网络与数据安全技术研究等。

虽然区块链安全国家标准还在研究中，但是作为区块链安全技术核心的算法领域，包括数字摘要算法，数字签名算法，加密算法等[46]，我国已经有了完备的制度和技术标准。根据 2018 年《国务院关于机构设置的通知》，国家密码局负责依法履行密码行政管理职能，对密码工作部门实施业务领导，负责网络与信息系统中密码保障体系的规划和管理。目前已经建立完备的密码算法管理体系，包括有行政规章，规范性文件，10 余项标准规范等，SM2、SM3 等算法已经在区块链领域成为主流算法。

从符合监管要求的角度，本白皮书建议在中国大陆的区块链系统或者服务，应优先采用符合中国国家密码局制度和标准的算法。

20. 网络信息内容安全保障义务及合规建议

区块链去中心化、防篡改特性，给网络信息内容安全监管带来了新的挑战。区块链有两个技术特点：一是多点共识，需要大部分节点通过共识机制进行数据一致性验证，链上 51% 的节点一致同意才能写入数据区块；二是前后两个区块都是通过单向哈希形式链接在一起的，改掉了其中的任何内容，哈希值就会发生变化，链就会断开，无法形成区块链上的共识。这两项技术特点保证了区块链上信息不可篡改。因此，一旦暴力、色情 、恐怖等有害信息被写入区块链中，不但可利用其同步机制快速扩散，也难以进行修改、删除。

内容安全监管一直是网络信息安全监管的重点。《网络安全法》要求：网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

46. 引自《中国区块链技术和应用发展研究报告（2018）》第 10 页。

网信办、公安部均在各自职权范围内对违反网络信息内容安全的行为进行重点整治，区块链信息服务的提供者应采取有效的措施，对上链信息的内容安全进行严格管控。

就防控有害信息上链，本白皮书建议：

（1）落实实名制的要求，基于 PKI/CA 准入机制和实名注册接入机制。

（2）建立信息安全管理制度：通过制度、用户服务协议，明确区块链服务提供方和使用方的权利和义务，落实信息安全责任。

（3）建立日志留存制度：平台通过记录平台用户登录退出时间、登录 IP 及端口、重要的操作，完成了对用户重要操作的记录，且日志保存时间要求 6 个月以上。

（4）建立有害信息防护措施：一是通过应用层网页敏感词过滤功能，一旦检测到敏感词，不让提交到后台系统；二是在智能合约层进行敏感词过滤，智能合约在处理数据时一旦发现有敏感词，既上链失败。三是在底层共识算法中进行敏感词过滤，节点在 commit 时发现敏感词后，即共识失败，不会加入到区块链数据链路中； 四是通过 openAPI 等，与政府或第三方的不良信息管理平台对接，实时更新不良信息关键词不间断的对敏感词库进行维护，保证对违法有害信息的防范控制做到及时有效。

（5）完善区块链共识机制。结合数字签名的 BFT 机制，在区块链共识层增加不良信息关键词拦截功能，并实时接受管理节点的关键词更新管理，实时拦截不良信息上链。

（6）实现智能合约的升级管理机制，达到突发事件发生后的不良信息应急响应拦截机制。

（7）建立溯源调查等技术措施。一是通过封号、关停服务等措施，一旦发现有违法行为，立即停止该账号的所有行为、关停相关服务。并通过截图、留存日志等方式保存记录，并向有关主管部门报告。二是使用区块链监督节点、日志留存等措施，为区块链服务提供方依法落实信息网络安全责任提供相应的技术支撑和能力。

（十四）区块链金融信息安全监管要求及合规建议

各对等节点的组网技术，是区块链的核心。通过构建数据共享协议，每个节点有相同的网络权利，实现数据在所有用户侧的同步记录和存数，[47] 与传统中心式数据库在一个或几个中心集中存储数据的方式不同，在区块链系统中，所有用户侧均有可能存放完整的数据。[48]

金融业务因涉及到敏感的个人信息和商业秘密，事关企业、个人的资金安全，信息安全要求更为明确、严格。人民银行、银监会、证监会、保监会等联合发布的《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》要求，金融机构应当按照安全、准确、完整、保密的原则，妥善保存客户身份资料和交易记录，金融机构应采取必要管理措施和技术措施，防止客户身份资料和交易记录的缺失、损毁，防止泄漏客户身份信息和交易信息。

就如何弥合区块链的去中心化和分布式存储的技术特点，与金融机构严格的信息保密责任之间矛盾，促使金融机构合法、合规利用区块链技术进行业务拓展方面，本白皮书建议：

参与区块链的金融机构应采用加密技术进行信息上链：通过零知识协议的隐私安全中间件系统，对上链数据进行加密，区块链各参与

47. 引自《中国区块链技术和应用发展白皮书（2016）》第 6 页。

48. 引自《区块链安全白皮书 - 技术应用篇（2018）》第 37 页。

主体可以在无法对密文解密的前提下对第三方交易密文进行交叉验证。

这样从技术上，可以解决业务上链和信息保密并行的要求。理由是：从技术角度看，数据与信息不同。根据国际标准化组织在信息技术标准中的定义，数据是信息的一种体现形式，该种体现形式是通过编码沟通，通过特定的设备或装置读取出来。而信息则是特定语境下具有特定含义之客体，如事实、事件、东西、过程或思想、理念的知识。[49] 将信息和数据在技术的不同层面的区分之后，金融机构将上链数据加密计算，未经授权的参与者无从读取数据所体现的信息，即含有内容的知识，则数据上链并不构成违反信息保密的要求。

(十五)《区块链信息服务管理规定》理解与适用

21.《区块链信息服务管理规定》的主要内容

2019 年 1 月 10 日，网信办发布的《区块链信息服务管理规定》（以下规定）正式实施，配套的区块链备案登记系统于 1 月 28 日正式上线。规定围绕着上链信息内容安全，明确了监管对象、确定了信息安全责任的主体，规定了信息安全责任主体的义务，建立了区块链服务的安全评估和备案机制，并规定了相关罚则。

规定第二条规定：在中华人民共和国境内从事区块链信息服务，应当遵守本规定。法律、行政法规另有规定的，遵照其规定。本规定所称区块链信息服务，是指基于区块链技术或者系统，通过互联网站、应用程序等形式，向社会公众提供信息服务。可以从四个方面理解监管规定的区块链信息服务：

首先是使用区块链技术。虽然规定中对什么是区块链技术没有明确的定义，但是相关的行业和团体标准已经建立 , 可以参照判断是否采用了区块链技术。这方面可以参照的标准包括：《中国区块链技术和应用发展白皮书（2016）》中提出的区块链标准体系框架，将区块链标准分为基础、业务和应用、过程和方法、可信和互操作、信息安全 5 类，并初步明确了 21 个标准化重点方向。2017 年，该标准体系框架写入了《软件和信息技术服务业“十三五”技术标准体系建设方案》。工信部信息化和软件服务业司指导下的中国区块链技术和产业发展论坛发布的《区块链参考架构》《区块链数据格式规范》。中国国家标准 / 行业标准的《信息技术区块链和分布式账本技术参考架构》已经立项。未来将是判断是否采用区块链技术的重要依据。同时，国际标准化组织已经成立了区块链和分布式记账技术委员会（ISO/TC307）, 正在进行区块链基础工作、安全、隐私和身份、智能合约机应用、治理、区块链和分布式记账技术与 IT 安全技术等的标准化研究工作。

其次是通过网站或者 APP 提供服务。即通过网站或者移动互联网程序的方式提供服务。

再次是向社会公众提供服务。区块链根据应用场景和权限体系的不同，可以划分为公有链、联盟链和私有链。其中：

公有链是指任何人都能参与的区块链，无需授权、任何人都可以自由加入或者离开，查询、发送信息、参与记账。联盟链是指多个机构共同管理维护的区块链，参与区块链的节点是事先选定的。联盟链也只对联盟内部成员开放全部或部分功能，链上信息的读取、写入以及记账规则都按照联盟共识来设定。公有链和联盟链的参与者范围都超出了一个组织内部的范畴，具有社会公众的属性。

私有链是指区块链记账权限仅在一个人或者一个机构手里，并且参与记账的权限由机构内部制定，读取权限可以开放也可以任意程度地限制。如果仅限于公司或者组织内部使用，则不具有社会公众的属性，应不属于规定的监管范围。若将强读取权限开放给公司或者组织之外的机构或者个人，则具有社会公众属性，应按照规定要求进行监管。

最后是提供的服务是信息服务。根据 2011 年修订的《互联网信息服务管理办法》第二条的规定，互联网信息服务，是指通过互联网

49. 参见纪海龙 《数据的私法定位与保护》 法学研究 2018 年第 6 期第 72-91 页。

向上网用户提供信息的服务活动。

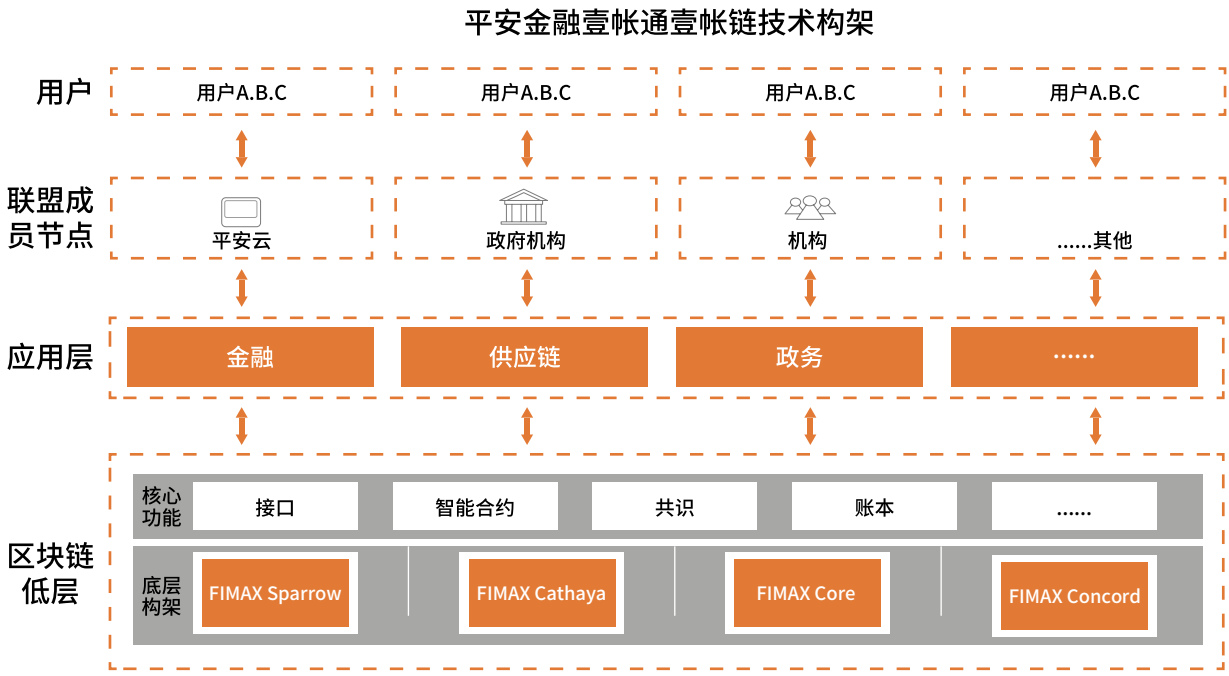
22. 区块链信息服务提供者

《区块链信息服务管理规定》第二条规定：本规定所称区块链信息服务提供者，是指向社会公众提供区块链信息服务的主体或者节点，以及为区块链信息服务的主体提供技术支持的机构或者组织。

区块链信息服务提供者，分为两大类：一类是区块链信息服务内容提供者，即提供了区块链信息服务的主体或者节点；第二类是区块链信息服务技术提供者，即为区块链信息服务提供系统开发部署、运维等技术提供者。

理解区块链信息服务提供者的含义，需从区块链的技术架构入手。区块链在具体实现上各有不同，整体架构存在共性。本白皮书以平安金融壹账通的壹账链架构（详见图 5）为基础进行说明。壹账链已经正式应用在跨境贸易、供应链、资产管理、海关通关等多个业务场景中。整体架构份四个层次，分别为区块链底层、应用层、联盟成员节点和用户。

图 5：平安金融壹账通壹账链技术架构



（1）区块链信息服务内容提供者

在区块链联盟链一般会由多个主体参与，联合构建。需要成员管理、权限管理、共识节点管理等。目前常见的联盟构建形式有三种：

①联合治理形式：由联盟成员推举专人组建联合治理委员会，联合治理委员会负责管理联盟链；

②领导型成员治理形式：由联盟中占领导地位的一个或几个成员对联盟链进行管理，其他联盟成员作为参与方加入到该许可链中；

③法定机构治理形式：由法定机构或其他监管机构创建组织来管理和维护许可链的运行。[50]

以上三种模式中都可以看出，区块链联盟的情况下，可能会存在着多个主体都提供区块链相关信息服务。

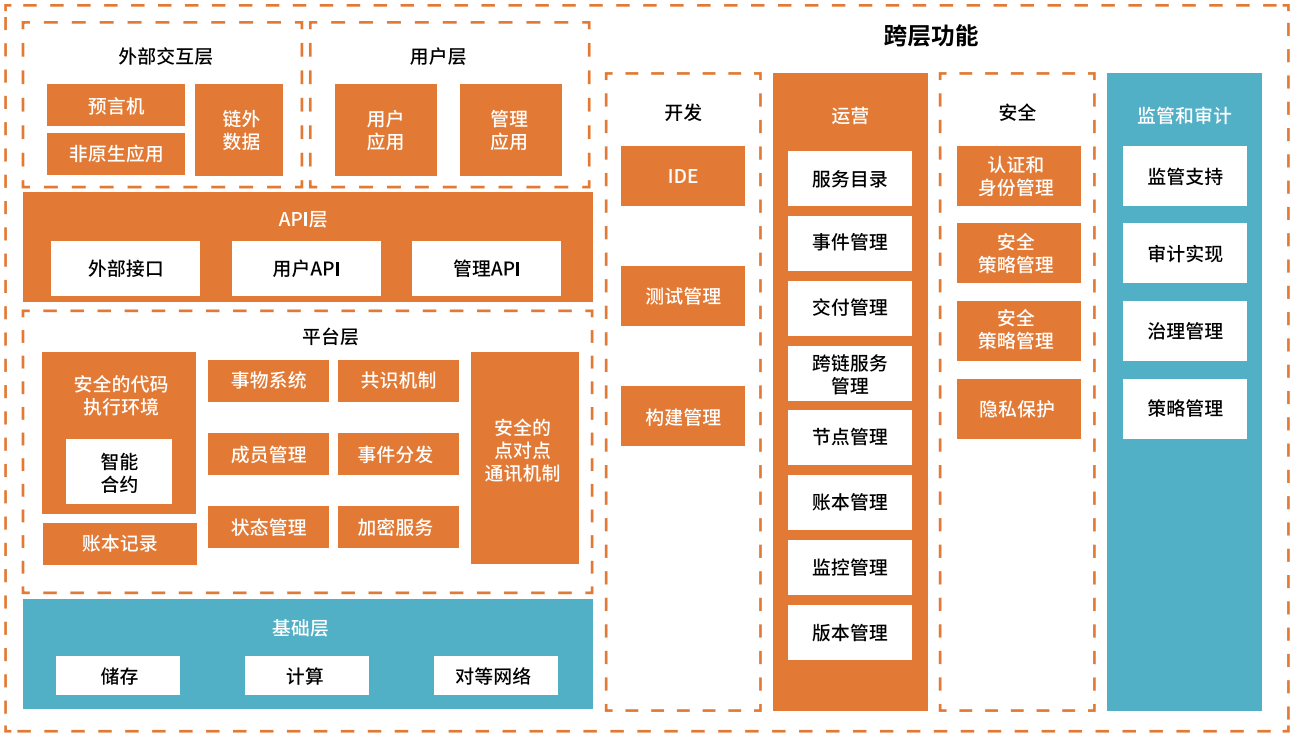
联合治理形式下，联合治理委员会如果是登记成为法人实体的，则该法人实体作为区块链服务提供者；如果没有实体的，则联合治理委员会的成员都有可能构成区块链服务的提供者。领导型成员治理模式下，占据领导地位的一个或者几个成员都是区块链信息服务提供者。法定机构治理模式下，由法定机构或者监管机构创建的组织是区块链信息服务的提供者。

加入联盟链的成员，根据参与的形式不同有所区别。如果通过部署节点的方式加入区块链联盟链，根据规定的要求，也是区块链信息服务的提供者。

（2）区块链信息服务技术提供者

提供区块链系统的开发、部署、运维服务的是区块链技术服务的提供者，主要工作包括有：基础层的存储、计算、对等网络的配置和开发；平台层的智能合约、事务系统、共识机制、成员管理、事件分发、状态管理、加密服务、安全的点对点通信机制部署开发等；外部交互层包中的预言机、非原生应用、链外数据交互；用户层的用户应用和管理应用的开发。详细的系统建设工作可参见由《中国区块链发展和应用白皮书（2018）》所提出的区块链系统功能架构图。

图 6：区块链系统功能架构



50. 引自《中国区块链技术应用和发展研究报告（2018）》第 34 页。

23. 区块链信息服务提供者的义务

围绕着保障区块链上的网络信息安全，《区块链信息服务管理规定》对区块链信息服务提供者提出了多项合规义务，主要可以归纳为四类：一是信息安全制度建设；二是信息安全技术要求；三是完善客户管理；四是合规经营义务。

（1）信息安全制度建设

规定要求区块链信息服务提供者要从管理制度和平台规则两个方面，完善信息安全制度的建设，具体包括：

规定第五条要求：区块链信息服务提供者应当落实信息内容安全管理责任，建立健全用户注册、信息审核、应急处置、安全防护等管理制度。

规定第七条要求：区块链信息服务提供者应当制定并公开管理规则和平台公约，与区块链信息服务使用者签订服务协议，明确双方权利义务，要求其承诺遵守法律规定和平台公约。

（2）信息安全技术要求

技术要求包括两个方面：一是违法信息处置技术符合国家标准；二是区块链系统符合国家网络安全标准。

违法信息处置符合国家技术标准方面，规定第六条要求：区块链信息服务提供者应当具备与其服务相适应的技术条件，对于法律、行政法规禁止的信息内容，应当具备对其发布、记录、存储、传播的即时和应急处置能力，技术方案应当符合国家相关标准规范。以下几项措施，作为区块链信息服务提供者落实技术要求的参考：

- 在区块链的底层、应用层、用户端进行有限信息的防控；
- 建立敏感词库，覆盖底层共识算法、智能合约层和应用层；
- 一旦发现有违法行为，能够停止该账号的所有行为、关停相关服务。
  并通过截图、留存日志等方式保存记录，向有关主管部门报告

区块链系统负荷国家计算机网络安全标准方面，规定第十五条要求：区块链信息服务提供者提供的区块链信息服务存在信息安全隐患的，应当进行整改，符合法律、行政法规等相关规定和国家相关标准规范后方可继续提供信息服务。以下几项措施，供区块链信息服务提供者作为落实安全管理标准的参考：

- 分布式账本技术，各节点互为备份，保证数据安全；
- 每个节点部署至少两台服务器，做到双活备份；
- 加密传输，数据验签，保证数据的准确性、一致性、完整性；
- 传输方式可以是专线、VPN 或者互联网；
- 可以做到一文一密，授权才能访问；

● 数据全加密，同时区块链技术保证不可篡改；

● 安全硬件、环境隔离、网络监控、安全检测；

● 具备相应级别的信息系统安全等级保护。

（3）完善用户管理

用户管理包括两个方面：一是落实用户实名制要求；二是对违规用户的应急处置。

区块链信息服务提供者应落实用户实名制的要求。规定第八条要求：区块链信息服务提供者应当按照《中华人民共和国网络安全法》的规定，对区块链信息服务使用者进行基于组织机构代码、身份证件号码或者移动电话号码等方式的真实身份信息认证。用户不进行真实身份信息认证的，区块链信息服务提供者不得为其提供相关服务。

区块链信息服务提供者应完善对违规用户的管理措施，规定第十六条要求：区块链信息服务提供者应当对违反法律、行政法规规定和服务协议的区块链信息服务使用者，依法依约采取警示、限制功能、关闭账号等处置措施，对违法信息内容及时采取相应的处理措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

（4）合规经营义务

区块链信息服务提供者的合规经营义务，主要集中在落实信息内容的安全管理，具体有：

● 区块链信息服务提供者和使用者不得利用区块链信息服务从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动，不得利用区块链信息服务制作、复制、发布、传播法律、行政法规禁止的信息内容。

● 区块链信息服务提供者开发上线新产品、新应用、新功能的，应当按照有关规定报国家和省、自治区、直辖市互联网信息办公室进行安全评估。

● 区块链信息服务提供者应当在提供服务之日起十个工作日内通过国家互联网信息办公室区块链信息服务备案管理系统填报服务提供者的名称、服务类别、服务形式、应用领域、服务器地址等信息，履行备案手续。区块链信息服务提供者变更服务项目、平台网址等事项的，应当在变更之日起五个工作日内办理变更手续。区块链信息服务提供者终止服务的，应当在终止服务三十个工作日前办理注销手续，并作出妥善安排。

● 区块链信息服务提供者应当记录区块链信息服务使用者发布内容和日志等信息，记录备份应当保存不少于六个月，并在相关执法部门依法查询时予以提供。

● 区块链信息服务提供者应当配合网信部门依法实施的监督检查，并提供必要的技术支持和协助。

● 区块链信息服务提供者应当接受社会监督，设置便捷的投诉举报入口，及时处理公众投诉举报。

24. 区块链信息服务备案

《区块链信息服务管理规定》要求区块链信息服务提供者进行服务备案，时间是在提供服务之日起十个工作日内，通过区块链信息服

务备案管理系统（https://bcbeian.ifcert.cn）进行。完成备案的，区块链信息服务提供者应当在其对外提供服务的互联网站、应用程序等平台的显著位置标明其备案编号（示例：粤网信备 xxxxxxxxx 号）。区块链信息备案包括两大部分，主体信息备案和服务信息备案。主体信息备案时指提供区块链信息服务的法人。服务信息备案时区块链信息服务者提供的服务项目。一个提供区块链信息服务的法人可以备案多个服务项目。例如，在网信办 3 月 30 日发布的首批境内区块链服务备案通过的名单中，中国平安共有 5 个项目通过备案，其中金融壹账通作为区块链信息服务提供者，通过了两个服务项目备案，壹账链和天津口岸区块链跨境贸易平台。

本白皮书总结了金融壹账通在办理备案过程中的经验，就几个重点事项分析如下，供办理时参考：

（1）需要备案的范围：根据《区块链信息服务管理规定》及电话咨询备案系统获得的意见：在中国境内，基于区块链技术的网站或应用程序，提供信息服务的应当进行备案。没有采用区块链技术的，不属于备案范围。具体可以参见本白皮书的前述的《区块链信息服务管理规定》的主要内容部分。

（2）服务内容：系统提供了三个备案选项，服务者可以根据自己提供的具体业务对应进行勾选，其中：

● 基础设施提供方：是提供硬件相关的矿机、云服务器、机房服务等；

● 应用运营方：利用区块链技术提供具体应用服务的，例如提供保全、区块链存证、防伪溯源、供应链等。

● 技术提供方：是提供区块链网络系统底层搭建及开发的。金融壹账通备案通过的壹账链 BAAS 平台就是典型的技术提供方备案。

（3）应用运营方：系统提供了三个选项，分别是钱包，区块链交易查询浏览器，和其他类应用，其中：

● 钱包：是区块链公有链中用于存储 TOKEN 的系统功能，涉及到发币，所以备案系统中特别予以列出。

● 区块链交易查询浏览器：浏览器用于查看区块记载的交易数据，每一个区块所记载的内容都可以从区块链浏览器窗口上进行查阅，是区块链系统的一个重要功能。若公有链的区块链浏览器用于查询、显示代币交易信息的，从代币交易管控和信息内容安全监管角度，对其做特定备案要求有一定必要性。

● 其他类应用：在钱包，区块链交易查询浏览器之外的服务，选择此项。联盟链系统也会涉及利用区块链浏览器，如果联盟链不涉及代币交易的，仅勾选其他类应用是可以的。

（4）添加主链：备案系统在“其他应用类信息”方面，提供了以太访、比特币、EOS 等主链，在此之外的，需要另行添加主链。联盟链备案的，可以添加底层系统框架的名称和相关信息。

五．区块链数据出境合规

(十六) 数据跨境交互的趋势

全球化的推进，区块链技术的跨境应用是必然之路。不可避免地面临境内主体与境外主体直接进行数据交互的情形：

一方面，若区块链联盟中的部分主体在境外，则其他国家和地区的机构和个人的信息将不可避免的被上传至区块链节点中，并通过系统的授权规则，在境内主体和境外主体之间直接交互明文数据。此种数据交互行为将受到我国和其他国家与地区的数据相关法律的规制。

从总体趋势上看，随着当今世界对数据价值的重视和各国面临的数据安全形势日趋严峻，各国各地区对数据流动的监管诉求日益上升，有关数据交互的管制，特别是有关个人信息的规范，已因欧盟和美国两大政治体的法律制定影响而逐渐被世界各国所关注，这将使得数据合规出境和入境成为项目未来合规运营的重要一环，在可预见的将来，区块链联盟中各主体在数据出境和入境方面可能将面临多重监管的压力。

另一方面，除区块链项目本身参与主体的国际化外，项目还有可能与其他国家或地区的区块链项目进行对接，特别是跨境贸易的业务场景中，将区块链技术应用在跨国运输、贸易、交易结算等场景时。届时项目的联盟规则如何与其他区块链项目的规则进行匹配适用，也将成为未来需面临的挑战。

(十七) 数据出境的基本要求

25. 数据出境法律政策概况

世界各国已经认识到数据是一国重要的基础性战略资源，日渐强调“数据主权”。2015 年 8 月 31 日，国务院印发的《促进大数据发展行动纲要》也指出，大数据已成为国家重要的基础性战略资源，正引领新一轮科技创新。充分利用我国的数据规模优势，实现数据规模、质量和应用水平同步提升，发掘和释放数据资源的潜在价值，有利于更好发挥数据资源的战略作用，增强网络空间数据主权保护能力，维护国家安全，有效提升国家竞争力。

从目前所知的已建立数据保护制度的国家和地区的法律规定来看，数据主权制度主要有三大趋势：一是对重要的数据跨境出口进行限制；二是数据本地化的要求，强化对数据的控制；三是延伸对数据的域外管辖权。[51]

国家或地区会对其境内所产生或收集的数据的“数据本地化”的要求，该要求与区块链去中心化的本质特征有所冲突。“数据本地化”的要求通常有几种表现类型 :

（1）仅要求在当地有数据备份，而并不对跨境提供作出过多限制；

（2）数据留存在当地，且对跨境提供有限制 ;

（3）要求特定类型的数据留存在境内 ;

（4）数据留存在境内的自有设施上。

51. 引自何波《数据主权法律政策与实践》，载于 CAICT 互联网法律研究中心微信公众号，2017 年 5 月 16 日。

因此区块链联盟各参与主体在参与长期项目并提交数据时，需要根据其所在国家或地区的法律来进行单项合规，设置配套的数据交互制度，否则可能导致法律层面、社会舆论甚至政治外交方面的负面后果。

以中国大陆目前的法律规范为例，有关数据出境，特别是公民个人信息和重要数据出境的要求，主要是在《中华人民共和国网络安全法》中明确约定。如该法第二十九条规定，国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。第三十五条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的公民个人信息和重要业务数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

网信办 2017 年公布的《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下“评估办法”）第二条也强调，网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

从以上规定来看，网络安全法下的数据存储本土化和出境安全评估义务主要适用于运营关键信息基础设施的企业，但是对于 “关键信息基础设施的运营者”如何界定，网络安全法及评估办法并未给出任何明确的定义、范围或解释。同时，评估办法第十六条规定，其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行，从而扩大了数据出境安全评估义务人的范围。

26. 中国的出境受限数据

中国的法律法规和监管文件，对特定种类的数据跨境交流作了限制性规定，在开展区块链项目应用时，应当予以特别注意，应及时跟进相关监管要求办理审批手续，或者采取有效措施，规避合规风险。跨境交流受限的数据主要有以下几类：

（1）国家秘密。根据《保守国家秘密法（2010 年修订》的要求，涉及国家安全和利益的事项，以及政党的秘密事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，属于国家秘密，具体包括①国家事务重大决策中的秘密事项；②国防建设和武装力量活动中的秘密事项；③外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项；④国民经济和社会发展中的秘密事项；⑤科学技术中的秘密事项；⑥维护国家安全活动和追查刑事犯罪中的秘密事项；⑦经国家保密行政管理部门确定的其他秘密事项。任何组织和个人不得邮寄、托运国家秘密载体出境，或者未经主管部门批准，携带、传递国家秘密载体出境。

（2） 个人金融信息。人民银行等金融监管机构严格禁止个人金融信息出境。2016 年 12 月，人民银行颁布了《金融消费者权益保护实施办法》，该办法第二十八、三十条条要求在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。

（3）人口健康信息。2014 年 5 月 5 日，国家卫生和计划生育委员会印发的《人口健康信息管理办法 (试行)》规定，不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

（4）人类遗传数据。1998 年 6 月 10 日，国务院办公厅转印发的科学技术部、卫生部联合制定的《人类遗传资源管理暂行办法》要求，重要人类遗传资源严格控制出口、出境和对外提供。已审核批准的国际合作项目中，列出人类遗传资源材料出口、出境计划的，需填写申报表，直接由中国人类遗传资源管理办公室办理出口、出境证明。因其他特殊情况，确需临时对外提供人类遗传资源材料的，须填写申报表，经地方主管部门或国务院有关部门审查同意后，报中国人类遗传资源管理办公室，经批准后核发出口、出境证明。

（5）国家档案。2017 年 3 月 1 日颁发的《档案法实施办法》规定，各级国家档案馆馆藏的一级档案严禁出境。各级国家档案馆馆藏的二级档案需要出境的，必须经国家档案局审查批准。各级国家档案馆馆藏的三级档案、各级国家档案馆馆藏的一、二、三级档案以外的

属于国家所有的档案和属于集体所有、个人所有以及其他不属于国家所有的对国家和社会具有保存价值的或者应当保密的档案及其复制件，各级国家档案馆以及机关、团体、企业事业单位、其他组织和个人需要携带、运输或者邮寄出境的，必须经省、自治区、直辖市人民政府档案行政管理部门审查批准，海关凭批准文件查验放行。

（6）征信信息。2013 年 1 月 21 日国务院印发的《征信业管理条例》要求，征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。

（7）石油作业数据。2013 年 7 月 18 日修订的《对外合作开采海洋石油资源条例》规定，为执行石油合同所取得的各项石油作业的数据、记录、样品、凭证和其他原始资料，其所有权属于中国海洋石油总公司。前款数据、记录、样品、凭证和其他原始资料的使用和转让、赠与、交换、出售、公开发表以及运出、传送出中华人民共和国，都必须按照国家有关规定执行。

（8）网约车平台采集的个人数据。2016 年 11 月 1 日，交通运输部、工业和信息化部、公安部、商务部等 7 部委联合发布的《网络预约出租汽车经营服务管理暂行办法》要求，网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流。

27. 区块链项目数据跨境交流合规指引

据此，从目前个人信息和重要数据跨境传输的立法趋势和监管态势来看，凡存在数据跨境传输行为的企业今后均有可能被囊括在安全评估的监管范围之内。因此对区块链项目的境内参与主体，建议持续关注国家关于数据出境的最新要求，未来尽早建立数据存储和跨境传输的内控政策以及出境安全的评估机制；对已建立相应政策和机制的企业，则建议根据评估办法的要求进行对照审查，调整修改。

首先，企业可结合评估办法第八条规定的评估重点内容，内部先行梳理出境数据的性质、数量、范围、敏感程度等，对拟出境数据必要性进行论证，并对拟出境数据的类型和传输对象进行分析。同时，对照评估指南对自身情况进行初步判定，提早进行准备以应对可能的数据出境评估要求。

其次，建设和完善信息保护和数据安全的软硬件设施，了解数据出境目的地的网络安全状况，确保与出境数据的境外接收方形成有效的联动机制。

最后，企业在发生跨境数据或信息传输前，与行业主管或监管部门进行有效的沟通，对可能的数据出境行为先行报备，了解清楚出境数据的评估属于自我评估还是报请评估，以减少数据传输的合规成本和风险。

（十八）金融数据出境合规指引

《网络安全法》第三十一条规定，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

可以看出，金融安全向来与国家安全息息相关，金融安全与网络安全也密不可分，金融行业的特殊性以及关键信息基础设施的重要性，构成了金融数据跨境流动必然受到更加严格的管制。

28. 金融数据出境政策概要

现有的法律法规、监管规章和政策文件，从网络安全、客户信息保密等角度，对金融机构的数据出境进行管制，主要的法律法规、监管规章和政策文件有：

（1）2006 年 10 月颁布的《反洗钱法》第五条规定：履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密；非依法律规定，不得向任何单位和个人提供。

（2）2016 年 11 月颁布的《网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

（3）2000 年 3 月 20 日，国务院颁布《个人存款账户实名制规定》第八条规定，金融机构及其工作人员负有为个人存款账户的情况保守秘密的责任。金融机构不得向任何单位或者个人提供有关个人存款账户的情况。法律另有规定的除外。

（4）2013 年 1 月 21 日，国务院颁布了《征信业管理条例》，第二十条要求信息使用者应当按照与个人信息主体约定的用途使用个人信息，不得用作约定以外的用途，不得未经个人信息主体同意向第三方提供。

（5）2003 年 4 月 10 日，人民银行印发了《人民币银行结算账户管理办法》，第九条规定银行应依法为存款人的银行结算账户信息保密。对单位银行结算账户的存款和有关资料，除国家法律、行政法规另有规定外，银行有权拒绝任何单位或个人查询。对个人银行结算账户的存款和有关资料，除国家法律另有规定外，银行有权拒绝任何单位或个人查询。

（6）2007 年 6 月 21 日，人民银行、银监会、证监会、保监会等联合颁布《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》，第三条要求金融机构应当按照安全、准确、完整、保密的原则，妥善保存客户身份资料和交易记录。

（7）2011 年 1 月，人民银行颁布了《关于银行业金融机构做好个人金融信息保护工作的通知》，第六条规定在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

（8）2011 年 5 月，人民银行上海分行颁布了《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》，第四条要求为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密。

（9）2014 年 6 月，人民银行办公厅颁布了《关于 2013 年个人金融信息保护专项检查情况的通报》，第二条要求外资银行内控制度建设较为完善，安全防范措施较为严密，制定了信息安全管理标准，对客户信息实施分级管理。但部分外资银行将数据中心设在境外、根据母国或总行监管合规要求跨境报送数据等行为，不符合监管部门的相关规定。

（10）2016 年 12 月，人民银行颁布了《金融消费者权益保护实施办法》，办法第二十八、三十条要求在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。境内金融机构为处理跨境业务且经当事人授权，向境外机构（含总公司、母公司或者分公司、子公司及其他为完成该业务所必需的关联机构）传输境内收集的相关个人金融信息的，应当符合法律、行政法规和相关监管部门的规定，并通过签订协议、现场核查等有效措施，要求境外机构为所获得的个人金融信息保密。

（11）2017 年 4 月 11 日，网信办颁布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，第二条要求网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

（12） 2018 年 5 月 21 日，银保监会颁布了《银行业金融机构数据治理指引》，第二十四条要求银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准。

29. 区块链项目金融数据出境合规指引

区块链技术在金融业务领域应用中，涉及到跨境数据交流的，除遵守人民银行、银保监会、证监会等金融监管机构的监管要求，还应遵守《网络安全法》体系下的监管要求。提供如下内容供参考：

（1）个人金融信息的范围

个人金融信息的内涵，根据中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知要求，个人金融信息是指银行业金融机构在开展业务时，或通过接入中国人民银行征信系统、支付系统以及其他系统、渠道获取、加工和保存的个人信息，包括有：①个人身份信息，包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等；②个人财产信息，包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；③个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等；④个人信用信息，包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息；⑤个人金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等；⑥衍生信息，包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；⑦在与个人建立业务关系过程中获取、保存的其他个人信息。

（2）个人金融信息出境合规要点

银行等金融机构为客户个人金融信息保密是金融行业运营的传统规范在网络时代的延续。《商业银行法》第二十九条规定，银行应遵守为存款人保密的原则。《反洗钱发》、《个人存款账户实名制规定》《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》等法律、法规和监管规定都要求金融机构应当按照安全、准确、完整、保密的原则，妥善保存个人金融信息。

从现行的监管要求看，原则上禁止银行业金融机构对本机构之外的其他机构或者个人提供个人金融信息。在以下法律法规或者监管规定的情形之下，可以对外提供：

1）法律法规要求提供的：例如在司法机关办理刑事案件时；

2）在为个人办理业务时必须提供时，且经过个人书面授权或同意的。

以上的保密要求延伸到了个人金融信息的跨境交流，并且有更加严格的要求。整体来看，现行的监管对个人金融信息的跨境交流原则上予以禁止，主要要求有：

1）在中国境内收集的个人金融信息，必须在中国境内进行储存、处理和分析；

2）银行业金融机构不得向境外提供境内个人金融信息。

2016 年 12 月 14 日，人民银行印发的《金融消费者权益保护实施办法》里为个人金融信息向境外提供开了口子。在同时满足以下情形时，境内金融机构可以向境外机构提供个人金融信息：

1）可提供信息的场景：处理跨境业务，例如跨境支付、外保内贷等；

2）当事人同意：经过当事人书面的授权同意，通过格式条款取得客户书面授权或同意的，应当在协议中明确该授权或同意所适用的向他人提供个人金融信息的范围和具体情形。同时，还应当在协议的醒目位置使用通俗易懂的语言明确提示该授权或同意的可能后果，并在客户签署协议时提醒其注意上述提示；

3）可输出个人信息的境外机构：必须是该境内金融机构在境外的关联机构，包括境内金融机构在境外的总公司、母公司或者分公司、子公司，或者办理该特定跨境业务必要的关联机构；

4）采取个人金融信息保密的措施：包括境内金融机构与境外机构签署保密协议，要求境外机构为所获取的境内个人金融信息保密，并通过现场检查等措施落实保密要求。

（3）总结：区块链项目个人金融信息出境合规指引

总结以上金融信息出境的合规要求，就区块链项目涉及到个人金融信息跨境交流的，本白皮书提出以下建议，供区块链项目参考：

- 项目开始前获取个人的书面授权同意，按照监管要求明确信息的范围和具体情形，并在醒目位置注明同意的可能后果；
- 做好区块链 系统中的信息读取授权，采用加密、零知识验证等技术措施，保障非必要、非关联机构不能读取个人金融信息的内容；
- 业务开始之初，联盟链各成员之间签署保密协议，严格遵守保密要求；
- 开展定期和不定期的现场检查，确保保密要求落实。