ICS
CCS 点击此处添加 CCS 号

团 体 标 准

T/ZAITS XXXX—2022

区块链信息服务合规自评估指引

Guidelines of Compliance for Blockchain Applications Self-Assessment

（征求意见稿）

2022 - XX - XX 发布　　2022 - XX - XX 实施

浙江省智能技术标准创新促进会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由浙江省智能技术标准创新促进会提出并归口。

本文件起草单位：蚂蚁科技集团股份有限公司、浙商银行股份有限公司、杭州云象网络技术有限公司。

本文件主要起草人：

区块链信息服务合规自评估指引

1 范围

本文件主要针对基于区块链技术设计和开发的产品或服务，描述了需求分析、产品设计、产品发布及部署等产品或服务全生命周期中合规风险自评估的核心要点、常见问题及应对方案、自评估流程等，为法务、合规等风险管理部门及人员提供实务操作指南和行业最佳方案建议。

注：由于目前在境内行业主要采取联盟链为主要技术路径，本标准仅从联盟链角度进行说明。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语
GB/T 35273-2020 信息安全技术 个人信息安全规范
JR/T 0171-2020 个人金融信息保护技术规范
JR/T 0193-2020 区块链技术金融应用 评估规则

3 术语和定义

GB/T 25069-2010、GB/T 35273-2020界定的以及下列术语和定义适用于本文件。

3.1
区块链信息服务 blockchain information service
基于区块链技术或者系统，通过互联网站、应用程序等形式，向社会公众提供的信息服务。

3.2
区块链信息服务提供者 blockchain information service provider
区块链业务服务提供者、区块链技术服务提供者。

3.3
区块链业务服务提供者 blockchain business service provider
向社会公众提供区块链信息服务的主体或者节点。

3.4
区块链技术服务提供者 blockchain technology service provider
为区块链业务服务提供者提供技术支持的机构或者组织。

3.5
区块链信息服务使用者 blockchain information service users
使用区块链信息服务的组织或者个人。

3.6
联盟链 consortium blockchain
对特定的组织团体开放的区块链，由某个群体内部指定多个预选节点为记账人，每个块的生成有所有的预选节点共同决定，其他接入节点可以参与交易，但不过问记账过程，其他节点可以通过该区块链开放的API进行限定查询。

3.7
上链 on chain
向区块链系统发起一次请求，将相关数据写入到区块链系统的操作行为。

3.8

加密代币 cryptocurrency

以数字化形式存在，采用区块链等特定加密技术发行的虚拟商品，包括比特币等去中心化数字货币、首次代币融资（ICO）形成的中心化数字货币，以及数字货币分叉等行为产生的代币等。

3.9

通证 token

区块链上可流通的加密数字权益证明。

3.10

区块链即服务 Blockchain as a Service

将区块链框架嵌入云计算平台，利用云服务基础设施的部署和管理优势，为开发者提供便捷、高性能的区块链生态环境和生态配套服务，支持开发者的业务拓展及运营支持的区块链开放平台。

4 缩略语

下列缩略语适用于本文件。

SDK：软件开发工具包（Software Development Kit）

PIA：个人信息安全影响评估（Personal Information Security Impact Assessment）

API：应用程序编程接口（Application Programming Interface)

ICO：首次代币发行（Initial Coin Offering）

BaaS：区块链即服务（Blockchain as a Service）

5 合规风险自评估原则

区块链技术合规风险自评估及管理，宜遵循以下原则：

a) 全生命周期覆盖原则；
区块链这一前沿技术在探索场景应用时，应自产品评审阶段至落地运营阶段始终贯彻合法合规原则，包括但不限于开发阶段的合规性与安全性评审及调整、根据监管合规要求的变化进行迭代调整、通过用户协议与平台规则等约束性法律文件约束各参与方均能承担合规责任等。

b) 制度化与流程化原则;
针对区块链技术的应用及开发，需要构建起制度化与流程化的合规管理体系，确保事前有评审、事中有监控、迭代经评估等，并结合供应链金融的行业特征，在业务中增设金融级核身、KYC、准入、登记确权等卡点。负责合规评审的部门及人员应当与业务及市场等部门及人员互相独立，保障合规制度与流程的独立性、公允性，所有进入市场化阶段的产品与应用都必须通过合规性评审考核。

c) 可追溯原则。
针对开发、业务与活动都应合理保存记录、日志等，实现业务可追溯，为企业内部合规管理与审计、外部监管核查与审计提供便利，为应急处置与报备提供基础，实现监管透明，保障合法合规开展经营。对于合规自评估风险点、考虑因素及评估结果业应及时整理，并建立与技术文档相关联的合规自评估文档，以便知识沉淀及监管备查。

6 合规风险审核要点

6.1 监管备案及许可

6.1.1 网信办区块链信息服务备案

基于区块链技术或者系统向社会公众提供服务的区块链信息服务者，应向中央网信办进行备案。需要完成备案主体注册信息和具体区块链服务信息，备案信息才视为有效提交。

6.1.1.1 对产品是否应进行单独备案进行评估

可考虑遵循以下判断路径（图1），其中核心是判断区块链信息服务是否向社会公众提供。“社会公众”可理解为不特定对象（包含自然人和非自然人），应结合应用场景需求进行分析。

例1： 如果仅为机构或组织内部档案管理提供区块链服务，且档案不基于区块链技术对社会公众开放或共享的，则可无需进行备案。

例2：如果是区块链技术服务提供方，即使当前服务仅面向有限客户（比如1-2家平台类组织），需要结合该客户是否面向社会公众提供服务，如果是也需进行备案。

例3：如果产品或服务属于测试孵化期，可在正式上线并向不特定对象提供服务时进行备案。

例4：如果是标准化BaaS服务平台技术提供方，以区块链技术服务方身份完成BaaS平台服务备案即可，无需就每一个签约客户或场景进行单独备案。但利用BaaS技术服务开展信息服务的区块链业务服务提供者应另行根据监管法规要求进行备案。

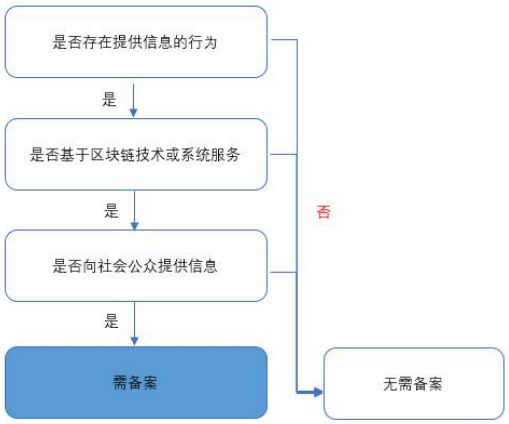

图 1　判断路径

6.1.1.2　判断备案主体身份

在区块链信息服务者包括两类，一是直接面向社会公众的信息服务提供主体；二是面向信息服务提供主体提供技术服务的机构，不直接面向社会公众提供服务。如果主体同时具备两类身份，则以信息服务提供主体身份完成备案。如果仅为技术服务提供机构，仅以技术服务提供主体完成备案（在备案系统中选择“技术服务提供方”）。反之，如果仅是信息服务提供主体，则以信息服务主体完成备案。

6.1.1.3　备案信息获取、提交及更新

为确保相关备案及时准确，主体内部备案工作负责人员应与业务方建立常态跟进和充分沟通机制，以确保其了解并确定需备案产品或服务。在明确需备案后，备案工作人员向业务方获取服务提供者名称、服务类别、服务形式、应用领域、服务器地址等备案信息，及时登录网信办备案管理系统提交备案。

在备案提交后，需定期登录查看备案结果及进度，如有备案未通过情况，尽快按照系统提示补齐信息（比如提交有效测试账号密码等），或致电网信办系统相关负责人员了解情况，争取尽快补交备案。在取得备案编号后，需第一时间通过业务部门，在对外提供服务的互联网站、应用程序等显著位置标明备案编号。如果服务发生变更（如平台网址变更），备案人员应在变更之日起五个工作日内在系统进行变更备案。如果业务方已停止服务，备案人员应在下线之日起三十天内在备案系统完成注销。

区块链信息服务提供者应对其内部备案工作负责人员进行必要培训，以确保相关人员准确理解和及时执行备案操作要求。

6.1.2　公安部入网备案

主体如办理入网手续时，应当在公安部履行相关备案手续。备案所需提交的材料包括：单位证件（如企业营业执照）、法人身份证正反面、法人手持身份证的照片；网站负责人的身份证正反面、手持身份证的照片及域名证书的彩色电子版。

一般而言，在完成备案后，审核人员会在3-5个工作日给予反馈（部分沿海城市地区可能更及时），反馈信息可能以短信形式或网站系统消息进行通知，也可能以直接致电进行通知（尤其是在备案不通过的情况下），建议保证系统提交的联系人为单位内部较稳定负责备案工作的相关工作人员。

在获取备案号后，需要工作人员及时联系业务方，将公安备案的标示及公安备案号放置到网站首页下方的中间位置。

6.2 内容安全管控

6.2.1 总体要求

区块链服务提供者应在内容风险管理方面制定有效的内容安全技术方案，具备对违禁信息的发布、记录、存储、传播环节记性即时和应急处置能力，确保在信息发布审核、事中管控、事后溯源三个环节落实主体责任，并应通过公司内部制度文件及定期培训等方式落实内容安全审核程序。

6.2.2 信息上链前的内容安全自查

由于区块链全链路端到端非对称加密传输技术特征，区块链信息服务提供者应通过多种方式保障上链信息从数据源头上在内容安全方面合法合规。

6.2.2.1 确认参与方身份的真实合法性

应通过设立管理节点等方式，严格把控联盟其他节点参与方身份，通过实名认证（组织机构代码、身份证号码或移动电话号码等）对参与方身份的真实性、合法性和区块链相关业务场景合理性进行充分确认，对非实名认证参与方应拒绝参与区块链数据读取和写入，并在合作协议以及终端用户服务协议中明确实名认证要求。

6.2.2.2 建设上链前屏蔽敏感信息能力

宜建设上链前屏蔽敏感信息的内容安全能力/模块（自研或使用外部第三方服务），作为信息上链前置必经流程。该内容安全技术能力/模块应实现对节点信息（如账户名称、头像、简介等注册信息）、待上链信息内容（如文本、视频、图片等）是否含有违法不良信息，在上链前进行自动/人工识别、审核过滤和信息登记，使有害信息无法写入、展示或在链上进行广播。

6.2.3 信息上链后的问题内容屏蔽及举报受理

6.2.3.1 违规识别

a) 保持违规识别模型的更新实时性和监测持续性。部分数据或信息有可能在数据上链时未违规，但随着监管要求的变化可能转为违规信息，需要进行及时处理。
b) 具备对链上内容展示前的风险识别能力。在数据上链后，考虑到上述非敏感内容转化为敏感内容的可能性，公司应具备采用安全技术或其他有效方式对区块链技术的应用和信息在展示前进行屏蔽的能力，覆盖黄赌毒、暴恐政、赌博等典型内容安全风险。例如可依靠敏感词和文本语意模型，对文本类信息进行策略管控；对视频类信息进行切帧通过图片算法、黑样本比对算法进行召回审核等。
c) 支持用户在发现违规内容后进行投诉举报。在面对终端自然人用户服务场景，应建立有效用户投诉渠道，将内容安全相关投诉及时进行处理。

6.2.3.2 违规处置

一经发现违禁信息，应立即采取或自动触发相应过滤屏蔽措施，使违禁恶意信息平台不可见，并向问题节点用户发出警示及立即整改通知，严重者应直接进行应急封号，并留存违法不良信息的审核日志信息。经警告后仍未按期整改的，应采取限制、中止、终止服务等处置措施。比如区块链溯源服务提供方，可直接冻结问题商品秘钥，使相关产品信息在链上无法展示。

6.2.3.3 记录留痕

应对所有日志（含上链主体证书唯一编号、写入哈希、写入时间、写入数据大小）进行不少于6个月的保存，有效实现链上信息可溯源调查。并在必要及适当的前提下，宜通过设立监督节点，配合有关监管部门通过区块链服务管理控制台区块链浏览器、API接口等多种方式对区块链交易信息进行监测、溯源及链上信息查询。

6.3 应用场景业务合规

6.3.1 防范业务涉及 ICO 等非法金融活动或交易

代币发行融资本质上是一种未经批准非法公开融资的行为，可能涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。区块链产品/服务中涉及同质化通证的，由于比特币效应，天然在业务上与代币发行等金融活动具备联结点，在合规评审中，需要在深入理解立法及监管要求及背景的前提下，掌握核心评审原则，有效区分市场已有合法操作与违法操作之间的界限，为业务提供产品/服务合规方案。

6.3.1.1 非法发售代币票券、数字代币

非法发售代币票券/数字代币不具有法偿性与强制性等货币属性，不具有与货币等同的法律地位，不应作为货币在市场上流通使用。在合规自评估中，可考虑从以下几点把握风险：

a) 代币是否具备“代替人民币在市场上流通”的虚拟货币特征。一般而言，应从以下三点要件进行评估：是否可以与人民币进行双向兑换；是否可超平台范围使用，或在平台内不同法人主体之间通用，或消费者之间可以相互转让；是否通过持有即可获得利息。以上要点作为虚拟货币的三条底线要求，可以为产品/服务合规风险判断提供基础性指导。各种 ICO 或变相 ICO 发行的代币，在价值尺度和流通性上都具备较明显的货币属性：首先，获得前提是需要支付相应的比特币、以太币等虚拟货币作为对价，由于比特币、以太币等虚拟货币与人民币之间可以直接双向兑换，代币与人民币之间亦存在间接双向兑换关系；其次，代币可支持市场持有主体之间的交易，也可以在境外虚拟货币交易所进行转让，具备流通性和作为支付工具（一般等价物）的能力。

b) 可将高风险代币共性作为合规风险自评估参考因素。比如是否有实体项目及对应价值的支撑，是否有实际的技术实现或落地，价值是否具有较大波动性或空间等。如果区块链产品/服务缺乏实际服务项目支撑或合理技术落地方案，仅以价值波动性作为产品/服务主要卖点，将面临更大合规风险挑战。

c) 可结合产品/服务实际场景进行合规风险综合判断。比如以区块链技术提供红包/优惠券数字营销服务的，在满足以下前提情况下，不宜认为构成代币票券：首先，在部分场景下可以用法币进行兑换或购买红包/优惠券，但无法与法币进行双向兑换；其次，仅能在平台内 C2B（消费者与企业之间）场景使用，不支持 B2B（企业之间）或 C2C（消费者之间）流转；再次，不可通过持有代金券获取利息；最后，发放场景一般为消费拉新促活或提升产品/服务复购率，发放时无需被发放对象支付货币性对价，票面金额由商家在核销时出资。如满足以上几点特征，英认为该类数字营销类产品性质与虚拟货币有本质差异。

6.3.1.2 非法发行证券

结合境内外主流金融市场对“证券”的定义，能代表特定财产权益，可均分且可转让或者交易的凭证或者投资性合同，都可能被认定为证券。证券发行在我国是持牌金融业务，未经有权机关批准，擅自公开发行证券的行为将构成违规。由于证券具有较宽的定义涵盖范围，合规评审要点包括：

a) 是否向不特定对象或累计向超过二百人以上发行；

b) 是否具备募资性，即持有者是否以金钱或其他财产性投资作为获取代币的对价；

c) 持有者是否合理期待通过第三方的努力获得投资回报。

如果相关业务涉及通证并锚定资产，将资产份额化后通过小程序、网站等方式向不特定社会公众发售，购买者预期获得投资性收益的，则该区块链产品/服务将面临较大合规风险，应考虑向业务部门提

出红线风险警示。需要注意的是，募资性在某些场景下不一定以金钱对价呈现，如果是用区块链产品/服务代替了对参与者所贡献服务的法币付款义务，也可能被认定属于融资行为。

6.3.1.3 非法集资

区块链产品/服务涉及集资情形的，合规评审要点包括：

a) 是否未经有关部门依法批准或有其他合法背景；
b) 是否通过媒体、推介会、传单、手机短信等途径向社会公开宣传；
c) 是否承诺在一定期限内以货币、实物、股权等方式还本付息或者给付回报；
d) 是否面向不特定对象。

以上评估要点同时满足的，区块链产品/服务将面临较大的非法吸收公众存款罪刑事责任风险。如果产品/服务是采用虚构事实、隐瞒真相的方法意图永久非法占有社会不特定公众的资金，则可能构成集资诈骗罪，应考虑向业务部门提出红线风险警示。

6.3.1.4 传销

合规评审要点包括：

a) 是否存在“入门费”。即交钱加入后才可获得计提报酬和发展下线的“资格”。入门费在互联网或区块链服务场景下，可能以“平台服务费”、“技术服务费”等名义收取，需要仔细甄别。
b) 是否存在“拉人头”。即直接或间接发展下线，并按照一定顺序组成层级。且主要靠“拉人头”保持业务持续运营，靠“入门费”反哺上线的人头奖励费。
c) 是否存在“层级团队计酬”。即上线从直接或间接发展的下线的销售业绩中计提报酬，或以直接或间接发展的人员数量为依据计提报酬或者返利，上线存在不合理“躺赚”情形。

以上评估要点同时满足的，区块链产品/服务将面临较大的传销风险，应考虑向业务部门提出红线风险警示。需要注意的是，近年来由于社交电商等新型销售形式不断涌现，正常的社交电商与互联网传销之间需要理清界限：首先，在“入门费”的评估中，社交电商平台需要用户注册并缴纳会费成为会员，但会员获得的相应权益不应主要是发展下线，而是就平台商品/服务享有非会员无法享受的折扣或其他优惠条件。同时，会员也需要为购买相应的商品或服务付费，该对价如果相对于其获得的商品/服务价值而言具备合理性，则不宜认为属于“入门费”。其次，在“拉人头”的评估中，需要考察入门费是否为平台商业模式的核心，是否平台脱离入门费后业务无法持续运营，如果拉人头仅是社交裂变方式进行营销或拉新促活的，本质应不属于传销。再次，在“层级团队计酬”的评估中，由于社交电商中也可能存在多级分销结构和层级分润的情形，需要重点结合上线是否存在“躺赚”，分润是否具备合理正当性等，认定是否属于传销。

6.3.1.5 为虚拟货币活动提供服务

除不得发行和交易任何形式的虚拟货币之外，也不得为虚拟货币提供支持服务,可以从以下两点把握风险：

a) 禁止提供服务的对象。不得向虚拟货币发行及交易方（如 ETH、比特币买卖双方）、虚拟货币交易所（如币安、火币交易所等）提供服务。
b) 禁止提供的服务类型。禁止提供的服务包括金融服务、非金融性支持服务两类。金融服务包括用虚拟货币为产品和服务定价、承保与虚拟货币相关的保险业务或将虚拟货币纳入保险责任范围、提供虚拟货币登记、交易、清算、结算服务等。非金融性支持服务包括提供营销宣传、付费导流、区块链技术服务支持、身份认证等业务。此处需要特别注意的是，虽然各文件未明确提及“技术性支持服务”，但需注意在“包括但不限于”、“等”等监管要求下，需谨慎提供为虚拟货币活动提供便利的服务涵盖范围，比如提供区块链技术、交易身份验证服务等。

6.3.2 行业应用场景合规要求

除了以上非法金融业务合规外，由于区块链技术应用场景广泛，在目标场景中的特定行业合规要求也建议一并考虑。

6.3.2.1 行业主管部门许可、备案

如果以区块链信息服务提供者身份对社会公众提供服务的，根据区块链服务的具体应用场景，如医疗、教育、通信服务等场景，应结合服务提供实质内容，根据各行业主管部门相关行政许可或备案要求，获得行业资质后上线产品或服务。比如基于区块链技术提供企业征信服务的，应先按照《企业征信机构备案管理办法》取得备案方可展业；提供通信服务的，需要根据《中华人民共和国电信条例》获得相应类别的增值电信许可。如果仅以区块链技术服务提供者身份提供服务的，无需进行以上操作。

6.3.2.2 司法存证

合规评审要点包括：

a) 共识节点是否为国家司法机关或权威服务机构。应将司法机关、司法鉴定中心、国家授时中心等权威机构作为共识节点。

b) 技术方案是否按照《司法链区块链技术要求》和《司法链区块链管理规范》进行设计。电子数据应在正常业务中生成，存证所依赖的计算机系统运行正常且安全稳定，具备有效的错误监测、核查手段，存证方法应严密可靠。同时，电子数据应符合《中华人民共和国电子签名法》第五条、第六条所规定的原件形式要求和保存要求，符合《最高人民法院关于民事诉讼证据的若干规定》所规定的真实性要求，符合“高度盖然性”的证明标准。

c) 是否区分不同司法应用业务场景提供相关功能。

序号	场景分类	业务场景	子场景	业务场景描述	上链数据
1	高可靠性数据存证（面向数据存储、数据流转等过程中，对数据本身可靠性具有较高要求的业务提供存证验证服务，为数据防篡改提供支持）	多源诉讼证据存证	互联网电子诉讼证据存证防篡改	当事人或代理律师在电子诉讼平台提起诉讼，可将提交的证据材料上司法链存证，防止证据被篡改，承办法官可在办案过程中对此类证据核验。	当事人在诉讼服务网上提交的起诉状及证据等材料
2			微法院诉讼证据存证防篡改	当事人或代理律师在中国移动微法院提起诉讼，可将上传的证据材料上司法链存证，防止证据被篡改，承办法官可在办案过程中对此类证据核验。	当事人在微信小程序上传的起诉状及证据等材料
3			诉服中心电子诉讼材料存证防篡改	当事人或代理律师到法院诉讼服务中心提起诉讼或提交材料，可将提交的证据、材料上司法链存证，防止被篡改，承办法官可在办案过程中对此类证据核验。	当事人在诉讼服务中心提交的的起诉状及证据等材料
4		送达多渠道回执留证	短信送达查阅留证	短信送达时，当事人接收或查看送达文书时，对该行为上链留证，并同步反馈法官。	查看短信行为、查阅文书行为
5			微信送达查阅留证	微信送达时，当事人接收或查看送达文书时，对该行为上链留证，并同步反馈法官。	查看微信行为、查阅文书行为
6			网上公告送达留证	网上公告送达时，公告信息及当事人查看送达文书，对该行为上链留证，并同步反馈法官。	公告信息、点击文书行为
7			邮件送达查阅留证	邮件送达时，当事人接收或查看送达邮件时，对该行为上链留证，并同步反馈法官。	查看邮件行为、点击文书行为
8			线下送达签字凭证	线下送达文书时，当事人在终端上签名凭证，对该行为上链留证，并同步反馈法官。	签名录像、截图、签名行为
9	高公信力信息存证（面向诉讼当事人、社会组织机构提供法定文书、通知、调查令等人民法院高公信力信息的存证验证服务，为司法公信提供支持）	法院文书存证验证	法院文书存证验证	面向诉讼当事人、社会组织机构提供法定文书、通知等人民法院高公信力信息的存证验证服务，为司法公信提供支持	立案通知书、开庭通知书、调解书、终版裁判文书等
10		律师调查令存证验证	律师调查令存证验证	开展民事、刑事、执行案件律师调查令的电子化服务，对调查令文件数据上链，协助调查单位可在线验证真伪。	律师调查令文件
11		执行信息存证验证	执行信息存证验证	面向诉讼当事人、社会组织机构对外公开的失信被执行人、限制高消费名单等信息存证验证	失信被执行人、限制高消费名单等信息
12	高风险操作存证（面向信息系统使用过程中，功能权限需进行严格管理的相关用户操作行为提供存证验证服务，为信息系统安全运行和常态化审计提供支持）	高发违规行为审计	违规结案行为审计	案件结案时，数据上链存证，对修改已结案件时间、材料、结案状态等行为进行监管。	已结案件信息、结案材料及行为日志
13			网上卷宗调阅行为审计	网上阅卷时，调阅卷宗信息及行为上链存证，对违规查阅等行为进行监管。	调阅卷宗信息、阅卷行为日志
14		高风险执行行为管控	执行案款收支管理监管	执行案款的数额、收支、分发等数据和行为进行上链存证，对执行案款收支管理行为行为进行监管。	执行案款账户信息、案款金额等信息、被执行人信息、当事人信息、执行案款流转节点行为日志及前后案款信息
15			执行查控违规使用预防	执行查控时，被执行人信息、执行查控行为等数据上链存证，对非被执行人查控等违规操作行为进行监管。	执行案件信息、执行依据信息、被执行人信息、被执行人修改日志、执行查控日志、执行查控内容

图 2 场景化功能模块参考

6.3.2.3 版权保护

合规评审要点包括：

a) 版权存证对象宜尽可能具备证据链的完备性。存证对象宜包括确权证据（拍摄原图、精修后的商品图、首次公开的网页截图等）、侵权证据（如被侵权的网页截图是过程录屏）等。存证对象如可如实反映一个数字内容从原始设计草图、建模图、样品照片、成品照片、PR 报道、合同协议再到公开和被侵权的完整证据链路，将极大增加被司法程序采纳作为证据的可能性。

b） 版权存证上链信息范围。宜仅将图片文件的特征指纹、存证主体信息、可信时间戳三个核心信息上链存证以备核验。图片源文件宜仅保留在用户的个人存储空间，以最大限度避免原图上链后带来的被泄露或被侵权风险。

6.3.2.4 供应链金融

合规评审要点包括:

a） 区分区块链技术服务和其他金融服务的界限。供应链金融区块链服务的核心环节包括应收账款上链、应收凭证流转、应收账款登记确权、兑付信息上链等。如果超越区块链技术服务范畴，提供了支付结算、融资授信、担保保险等持牌经营相关业务，将引发违规从事金融或牌照相关业务的合规风险。因此，需确认需要持牌从事的业务由持牌主体合规经营，并确认区块链信息服务提供方不对金融产品进行任何形式的推荐，不对金融产品的可获得性做出任何保证或承诺，并清晰向用户揭示金融牌照类业务由持牌主体提供，并应按照监管要求在相应持牌主体域内进行等。以保险业务为例，非保险持牌机构及其平台不得从事以下行为：在其页面提供保险产品信息进行商业宣传推广（比如费率、保额、保费试算、报价比价等）；向消费者提供能够自主完成投保行为的功能，或者代办投保手续；提供保险产品咨询服务；为投保人设计投保方案；代收保费；使用“XX 保险”或“XX 保险平台”等容易混淆行业类别的字样或宣传用语。

b） 核心企业及相关参与方准入风控。由于核心企业的偿债能力决定供应链金融业务模式健康度，应本着平台稳健运营的目标，设定明确、合理的准入标准，重点审核核心企业的资质与信用，并谨慎选择是否接入。对于其他参与方如供应商、金融机构、其他服务机构等，应合理审慎选择合作方，共同维护供应链合规、健康生态。

c） 合理提示用户谨慎选择基础交易对手方并依此转让应收凭证。应通过业务规则，提示用户不与已知或潜在存在破产（包括和解、解散、清算）情形或潜在风险的用户之间进行应收凭证的流转，如用户了解到己方或任何用户存在上述破产情形或潜在风险的，应及时通知运营方及平台。鉴于应用场景为供应链金融场景，且用户的首次实名制身份核验在区块链平台，或应用端完成，如果未能准确核验用户身份，可能将潜在风险传导至金融机构等其他服务提供方。

d） 合理约束用户在应用之外转让应收凭证对应的链上账款。应通过业务规则，要求用户不得在应用之外以任何方式转让链上应收账款，或对应收凭证或应收凭证对应的链上账款设定权利负担。

6.3.2.5 数字政务

区块链技术目前广泛应用于政务客户场景，如电子票据、电子证照服务、数字农业溯源、危化品管理、数字政务等。合规评审要点包括:

a） 宜充分了解政务部门数据流转要求。比如税务数据，宜遵守“银税互动”等相关文件政策要求，为税局与银行或银保监部门提供数据直连模式下的区块链服务。对于政府部门指定 ISV 进行数据对接的，应在于数字政务协议中明确该委托关系，以确保第三方机构有权获得并处理相关政府数据。

b） 宜按照政府要求落实信息上链管理。比如农产品溯源场景下，宜按政府部门要求，对农产品生产、采摘、装箱、运输等环节关键信息上链机构做严格权限管理，或通过 IOT 设备等技术方式，最大限度保证上链信息源头可信。又如电子票据应用场景下，应严格按照财政部等要求进行链上票据生成，或者在票据链下生成后，通过 SDK 等技术手段在第一时间完成数据上链，以保障链上政务数据权威性、完整性及有效性。

6.3.2.6 数字文创

基于非同质化权证技术，为数字经济环境下的虚拟商品所有权提供可追溯的确权方案，实现用户身份和资产的绑定。合规评审要点包括：

a） 应积极防范金融化炒作及反洗钱风险。首先，应确认技术方案支持数字证书身份标识,并对商户及用户做账户实名认证，积极防止通过买卖账户从事炒作等违规行为。其次，应重点确认技术及商业方案上充分落实炒作风险管控机制,实现交易机制可控性。比如,不应出现第 6.3.1.2 节的行为，宣传或暗示数字文创商品有巨大升值空间；不应将数字文创商品进行份额化售卖，或以集中交易、持续挂牌、标准化合约等形态转让数字文创商品；不应支持虚拟货币作为数字文创发行交易的计价和结算工具，不应提供场内外融资支持；如开放免费转赠功能的，应通过对转赠频次或持有时间等进行有效限制，并确保没有二级市场交易功能，切实防范金融化风险。

b） 基于业务形态需求，对内容权属及价值风险进行准入核实，并具备相应行业监管资质。如果以平台形式展业的：首先应在确保所锚定的内容资产有充分价值支撑基础上，对知识产权权属真实性进行充分审核，包括要求 IP 商户或代理方提供著作权相关证明材料，以核实权属来源真实可靠，避免知识产权侵权纠纷和因权属争议纠纷回收数字文创商品而引发的消费者纠纷。其次应具备增值电信业务许可证、网络文化许可证等监管合规资质，如存在锚定音视频等格式文件的情况，由于涉及以文创商品的形式对消费者进行视听节目传播，应具备信息网络传播视听节目许可证。

6.3.2.7 消费者服务

除了防范消费者金融业务风险外，合规评审要点主要在于消费者权益保护：

a） 虚假宣传等侵害消费者权益的管控。在产品服务 2C 交互设计中，需要确认已遵循自愿、平等、公平、诚实信用原则，重点查看是否有剥夺消费者选择权、2C 页面的功能解释及广告宣传是否有不实或夸大描述等情况，比如原则上区块链技术仅能保证信息上链后的抗抵赖性，在未结合 IoT 等智能硬件自动获取上链信息的情况下,宣传区块链源头可信具有较大虚假宣传风险。

b） 通过建立用户投诉举报途径保障用户权益。在自然人用户权益保障方面，机构应积极接受社会监督，通过多种方式直接响应或协助响应用户举报及投诉，将舆情风险提前化解或最大限度降低其损害：首先，为个人用户设置便捷的投诉举报入口，由专人负责，并按照问题分类进行及时进行响应处理。比如在 APP 端内提供投诉举报选项，由用户描述基本问题后，系统根据投诉内容，确认由业务人员或技术人员给予用户书面、短信或电话技术反馈。其次，对于所有投诉举报内容及反馈记录应保存不少于 6 个月，并记录和统计投诉举报内容及数量，进行有针对性整改，例如若属于合作伙伴支持体验问题，根据投诉举报严重程度评估是否需要合作伙伴方进行整改。

6.4 数据合规

6.4.1 角色分类

在数据上链、流转环节中，区块链信息服务提供者应按照相关法律法规及国家标准要求，结合其业务内容,判断其属于数据控制者或数据处理者的角色定位,谨慎处理关于数据源合法合规性的相关承诺，并明确自身及相关方在数据采集、使用、共享等方面承担的权利义务及责任边界。

如果区块链信息服务提供者仅提供技术服务支持，则属于数据处理者角色，基于区块链业务服务提供者或链上其他节点的委托，基于特定业务场景完成数据上链及流转，或生成相应业务需求的区块链通证。秘钥是否托管在区块链技术服务提供者不影响其数据受托处理者角色的判断，但区块链技术服务提供者需承诺非经同意不得私自使用秘钥对链上信息进行解密。

如果区块链信息服务提供者本身即是业务运营方，可自主决定数据的采集、使用和共享方式，则宜被认为构成数据控制者，基于权利义务相对等原则以及个人信息保护的相关要求，需要承担较数据处理者更重的数据授权义务及责任。

6.4.2 上链数据合法合规性承诺

如果服务主体仅提供区块链技术服务，由于区块链技术特性，服务主体仅能保证数据上链后不可篡改，无法就数据源的合法合规性进行保证或增信，应由链上节点方就上链数据的真实性及合法合规性进行兜底和保证。

为避免区块链技术服务提供方在数据源合法合规性上进行过度承诺，在技术服务合同中宜在条款中向客户明确，上链后数据具有可追溯性、不可篡改性、可验证性等特征，但不保证该等数据反映上链节点业务的实际情况。比如，在物流行业区块链应用场景时，就物流订单、运单等物流数据的真实性及引发的相关责任，不宜由区块链技术服务提供方进行承诺或担保，而宜由物流链实际运营主体进行保证。

6.4.3 数据获取及使用

6.4.3.1 数据采集及使用

如果主体作为区块链业务服务提供者，则应先获得作为区块链信息服务使用者的个人或企业用户授权，方可采集相关业务数据。尤其对于个人信息的情形，需要确保在授权交互环节告知用户区块链服务方收集、使用个人信息的目的、方式和范围等规则，并获得用户的授权同意，对于个人敏感信息还应获得明示同意。如果服务主体仅作为技术服务提供者，应作为数据处理者而无需直接获得区块链信息服务使用者的授权，但处理数据的范围不应超出区块链信息服务使用者对区块链业务服务提供者的授权范围。

6.4.3.2 第三方数据源引入

区块链信息服务提供者可在上链数据外根据业务场景实际需要引入外部第三方非公开数据。如果作为区块链业务服务提供者，应在5.4.2.1要求外谨慎考察该第三方数据来源的合法合规性，包括但不限于判断其数据获取场景合理性、随机抽查用户协议、查看上游数据源相关授权函及合作协议、查验其他采购方相关资质等，必要时还应进行实地现场考察。同时，在测试阶段应签署保密协议，并对直接标识符进行加密处理以完成测试，以确保在测试阶段的数据交互合规性。如果作为区块链技术服务提供者，仅基于业务服务提供者委托引入第三方数据源的，则第三方数据源的合法合规性风险及责任宜由委托方承担。

6.4.3.3 互联网公开数据

区块链信息服务提供者亦可在上链数据外获取与业务场景合理相关的互联网合法公开数据，在遵守相应网站爬虫规范及公开数据合理使用目的前提下，采集及使用无需另行获得用户授权。

6.4.4 数据共享

数据在链上实现共享和流转，应就数据共享对象、数据类型及共享目的获得区块链信息服务使用者的个人或企业用户的授权，并对数据获取方进行个人信息安全影响评估(PIA)。如果主体是区块链业务服务提供者，还应获得个人或企业的直接授权，并在授权条款中应明确区块链业务服务提供者的主体名称。比如，在链上数据共享用于贷款场景时，需要明确授权相关金融机构可基于区块链信息服务使用者的请求，通过业务服务提供方的服务查询并调取链上企业/个人数据（明确数据类型），用于审核企业/个人的贷款申请。对于较复杂的数据融合共享场景，还可以结合零知识证明、TEE链技术、多方安全计算等技术，更好实现数据共享的业务目标。

6.4.5 个人信息主体的权利行使

如果提供区块链信息服务中涉及个人信息的，服务主体还应配合个人信息主体的请求，响应其个人信息查询、更正和删除等请求。其中在数据删除权的行使上，由于区块链不可篡改和信息在多节点分布式存储的技术特性，可在遵守相关法律法规要求的前提下，采取匿名化、删除密钥、断开区块链链接并将凭证打入地址黑洞、技术上无法关联到特定主体等方式实现删除。

6.4.6 行业性数据合规要求

数据合规性自评估还应考虑结合具体行业要求进行，比如金融、税务、医疗等特定行业领域数据合规方面均存在特别要求。比如对于个人金融信息，应遵守央行相关法规文件及金标委行业标准规范，符合以上文件提出的关于信息采集、使用和处理的特殊要求。同时对于个人金融信息的跨境传输，也需要

遵守相应监管要求，满足为处理跨境业务目的且经当事人授权的前提，并通过签订协议、现场核查等有效措施要求境外机构保密。又如人口健康信息，不得在境外的服务器中存储和托管。

6.5 客户/ISV 准入风险管理

在企业资质和信用等方面对客户、合作伙伴进行准入考察，可将以下因素纳入考量：

a) 是否具有资质合法性。确认被调查对象已注册相应工商实体，具备工商营业执照、税务登记证等有效证件，以及国家相关法律法规要求的所有合法资质；
b) 是否从事虚拟货币等受国家严格管控的业务；
c) 是否具有良好的商业信誉。应考虑进行与业务需求相适应的背景调查，确认被调查对象无明显资信瑕疵，在既往经营活动中没有违法记录，无影响公司发展运营的重大诉讼案件；
d) 制定合作伙伴管理规则。可制定与企业发展策略相适应的的合作伙伴引入规则，将合作伙伴进行分级分类管理。

7 合规风险自评估操作

基于自评估全生命周期覆盖原则，宜尽早介入产品/服务的合规性自评估：

a) 需求分析。应建立良好业务沟通机制，在业务需求阶段了解业务诉求、商业模式、服务客群等，如果有较大合规风险点需要及时进行披露和提示。如已为行业较成熟区块链应用场景的，可结合该应用行业现状和核心功能点，作为风险敞口较低的判断依据纳入当前需求的合规评估作为参考。同时，也可以积极发挥合规岗位工作积极性，探索并挖掘国内外新应用场景，向业务方进行推荐或共同研究。
b) 产品设计研发。产品、应用或功能进入涉及研发阶段后，需要结合产品需求文档、技术文档、页面交互设计文档进行整体合规风险评估。在此阶段，由于产品仍处于设计过程中，功能样态变动可能较大，宜在需求文档产出前就核心合规风险原则进行明确，并提出相应缓释建议；应主动掌握产品研发进程并参加产品研发系分评审，确保合规风险点缓释建议实际落地。
c) 发布部署。为了管控产品服务风险，可申请参与产品内/外灰度测试，以便进一步根据最终用户使用视角对合规风险点进行感知、调优及改善，以避免潜在相关风险因素在产品上线初期被放大。

8 区块链信息服务监管现场检查准备及应对

区块链信息服务可能接受中央及地方网信办、公安部等监管部门不定期现场检查。为保证现场检查有效应对，区块链技术服务提供方可根据需要组织内部工作人员组成迎检小组，完成以下工作：

a) 了解监管检查部门及需求。在接到监管部门现场检查通知后，需要首先与沟通现场检查的目标、内容和日期，并争取获得监管现场检查问题清单（示例见附录 C），对于检查内容有不明确的，需要尽可能在现场会前进行沟通确认。
b) 确定迎检方式并进行相应准备。按照监管检查清单，提前沟通监管检查的方式，比如是否需要查阅文档、现场了解询问、现场系统演示，以及服务器后台查看等。之后组织内部相关负责人员准备相应材料，如有现场配合系统演示要求的，需对演示内容和服务稳定性进行检查，确保现场检查顺利进行。可以监管检查为契机，推动业务及技术部门进一步提升产品/服务合规意识及水平。
c) 现场检查应对。应积极配合监管现场检查需求，安排相关技术及风险管理部门负责人如实回答问题，就监管关注重点及整改要求进行详细记录，并就企业及行业最佳实践、难点、卡点与监管机构进行充分沟通和互动。
d) 后续跟进及整改。对于现场检查中提出的监管整改意见，应及时提供合规整改方案，并积极组织业务、技术部门落实监管要求，并按监管机构要求如实反馈整改结果。

附 录 A
（资料性）
区块链备案 Q&A

A.1 阅读对象及版本

阅读对象	区块链产品、技术备案需求方		
日期	版本	说明	修订人
/年/月/日	1.0	初稿/修订	XXX

A.2 为什么需要备案

自2019年1月28日起，根据中央网信办《区块链信息服务管理规定》要求，需要对境内区块链服务在网信办进行备案。如果通过备案，对于商业推广及客户沟通有一定程度的辅助说明作用，尤其是区块链信息服务机构合作的正规机构，普遍会对信息服务机构是否完成备案进行审查。但不等于网信办为产品合规性或价值进行背书。说明如果未进行及时备案，可能面临产品被责令限期改正，情节严重将可能被给予警告并处1~3万元罚款。

A.3 何时需要备案

根据《区块链信息服务管理规定》要求，在上线之日起十个工作日内需要提交备案。

A.4 何时拿到备案号

目前网信办对备案结果采取分批通知，截止2020年10月已经有四批结果公示。我们会密切关注备案进展，在新批次消息公布出来后第一时间联系申请备案业务方。结果公示通知可参见：http://www.cac.gov.cn/2020-10/28/c_1605447893747716.htm

A.5 备案提交材料清单

信息项名称	信息项填写	说明及注意事项
服务名称		按照产品名称填写，比如“司法区块链”
网站URL或客户端下载地址		实际可访问地址，并保证链接稳定性
测试账号密码		提供一套可以体验基本功能的账密，无需管理员权限
开始运营时间		按照实际上线时间填写（如还未上线，建议上线时间确认后再进行备案）
服务说明		简要表述用户和服务场景、产品功能，100字以内
服务对象数量		请按照实际数量填写
服务对象列举		写明与服务对象数量相符的对象名称，如“最高人民法院”。有多个的，用“、”隔开
是否开源		根据实际情况填写
源代码地址		如果开源请填写

A.6 我是技术服务提供方，我如何协助我的客户完成备案？

需要提示客户完成备案系统主体注册、备案信息提交等操作。备案主体注册清单见下，备案信息见第5部分，可由技术服务提供方向客户提供。

业务合作方区块链备案材料清单

一、 备案依据

自 2019 年 1 月 28 日起，根据《区块链信息服务管理规定》第 2 条、第 11 条，需要对境内区块链服务在网信办区块链信息服务备案管理系统(https://bcbeian.ifcert.cn/)上进行备案。

二、扫描件材料

1. 营业执照副本（加盖公章彩色扫描）
2. 负责人身份证正反面
3. 材料真实性声明（加盖公章彩色扫描，内容见附件一）

二、在线填写所需信息

1. 负责人信息

2. 主体信息

附件一：

材料真实性声明

本公司/本人承诺在备案中提交的材料（包括附件材料）真实，备案申请和条件符合相关规定，对备案提交的材料真实性负责。若有虚假，本单位/个人愿意承担由此产生的一切后果。

负责人签字

单位公章

年 月 日

附 录 B
（资料性）
区块链相关核心法律法规文件

表B.1为区块链相关核心法律法规文件。

表 B.1 法律法规文件

序号	项目	发布单位	核心相关条文
1	《中国人民银行法》	全国人大/全国人大常委会	第20、45条等
2	《证券法》	全国人大/全国人会常委会	第9条等
3	《刑法》	全国人大/全国人会常委会	第176条、第192条
4	《防范和处置非法集资条例》	国务院	第2、19条等
5	《禁止传销条例》	国务院	第2、7条等
6	《关于新型传销活动风险预警提示》	国家工商行政管理总局	全文
7	《关于防范代币发行融资风险的公告》（2017）	中国人民银行、中央网信办 ，工信部、国家工商总局、银保监会、 证监会	全文
8	《关于防范比特币风险的通知》（2013）	中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会	全文
9	《关于防范虚拟货币交易炒作风险的公告》（2021）	中国互联网金融协会、中国银行业协会、中国支付清算协会	全文
10	《关于参与境外虚拟货币交易平台投机炒作的风险提示》	中国互联网金融协会	全文
11	《关于防范以区块链名义进行ICO与“虚拟货币”交易活动的风险提示》	中国互联网金融协会	全文
12	《关于防范各类以ICO名义吸收投资相关风险的提示》	中国互联网金融协会	全文
13	《关于“虚拟货币”、ICO、“虚拟数字资产”交易、“现金贷” 相关风险的提示》	北京市互联网金融行业协会	全文
14	《关于防范以“虚拟货币”“ICO”“STO”“稳定币”及其他变种名义进行非法金融活动的风险提示》	北京市互联网金融行业协会	全文
15	《关于防范以“虚拟货币”“区块链”“ICO” 及其变种名义进行非法集资的风险提示》	北京市互联网金融行业协会	全文
16	《证券经营机构参与打击非法证券活动工作指引》	中国证券业协会	第2条等

附 录 C
（资料性）
区块链现场检查问题清单示例

表C.1为区块链现场检查问题清单示例。

表 C.1 现场检查问题清单

类别	项目	序号	检查内容
项目简介	/	1	该项目运营模式、经营业务范围、用户数、参与单位、数据量等基本情况
基础建设	备案	2	网站或平台是否在网信、工信、公安人行等行业主管部门进行备案
	规范制度建设	3	是否有安全岗位管理制度
		4	是否有安全教育和培训制度
		5	是否有（终端）用户管理制度
		6	对新服务、新功能是否进行安全评估
		7	是否有（终端）用户投诉举报处理平台
		8	是否有信息发布审核、登记，合法资质查验和公共信息巡查机制
		9	是否有安全事件的监测、报告和应急处置制度
	记录保存	10	是否能提供公司日常会议记录、制度修订记录、人员培训记录、病毒查杀记录、安全事件记录等（记录可以是电子的）
管理节点	主体责任落实情况	11	是否有明确的责任主体
		12	链上成员上线（记账）前审批审核
	管理节点功能验证	13	是否设立管理节点
		14	是否具备可靠共识机制
		15	管理节点是否能有效履行管理职能
		16	管理指令执行及时
监督节点	监督节点功能验证	17	是否设立监督节点
		18	监督节点是否具备监测、溯源功能
	信息查询	19	是否能通过接口或界面的方式供有关部门进行链上信息查询
技术防范能力	信息审核制度	20	对用户发布信息内容是否进行审核
	技术防范措施	21	是否具有对链上的文本过滤屏蔽措施
		22	是否具有对链上图片、音视频过滤屏蔽措施
		23	是否能对特定（终端）用户进行应急封号
		24	是否能对特定内容进行应急管控
	用户投诉举报	25	用户投诉举报处置流程
用户管理制度措施	用户实名制	26	用户注册实名制
		27	认证措施
		28	是否建立用户黑名单机制
		29	用户法律法规告知
日志留存情况	注册信息	30	是否留存（终端）用户注册信息
	登录日志信息	31	是否留存登陆（上下线）日志
	行为轨迹信息	32	留leib存的其他信息

参 考 文 献

[1]《切实加强虚拟货币监管，牢牢维护国家货币发行权》，https://www.yicai.com/news/5413833.html

[2] Framework for “ Investment Contract ” Analysis of Digital Assets ， https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-asset