ICS 35.240
CCS L 70

团 体 标 准

T/GZBD XX—XXXX

数据流通区块链存证技术规范

Technical Specification for blockchain evidence preservation in data circulation

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

贵州省大数据发展促进会　　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这些专利的责任。

本文件由中电科大数据研究院有限公司提出。

本文件由贵州省大数据发展促进会归口。

本文件起草单位：中电科大数据研究院有限公司、

本文件主要起草人：xxx

本文件首次发布。

数据流通区块链存证技术规范

1 范围

本文件规定了数据流通区块链存证的术语和定义、技术架构、存证网络、数据存证、存证服务、存证安全、检测与评估等。

本文件适用于数据流通区块链存证的设计、开发、服务和应用。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918.1 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.3 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GB/T 32918.4 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GB/T 32918.5 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 41819 信息安全技术 人脸识别数据安全要求

GB/T 42752 区块链和分布式记账技术 参考架构

GB/T 43572 区块链和分布式记账技术 术语

GB/T 43580 区块链和分布式记账技术 存证通用服务指南

GB/T 43697 数据安全技术 数据分类分级规则

3 术语和定义

GB/T 42752、GB/T 43572、GB/T 43580界定的以及下列术语和定义适用于本文件。

3.1

数据产权 data property right

权利人对特定数据依法享有的财产性权利，包括数据持有权、数据使用权和数据经营权等。

3.2

数据权益 data rights and interests

自然人、法人或其他组织对特定数据依法享有的权利和利益，包括数据隐私权、数据财产权、数据知识产权等。

4 缩略语

下列缩略语适用于本文件。

ABAC：基于属性的访问控制（Attribute-Based Access Control）

AI：人工智能（Artificial intelligence）

API：应用编程接口（Application Programming Interface）

CA：证书颁发机构（Certificate Authority）

DID：分布式身份标识符（Decentralized Identifier）

RBAC：基于角色的访问控制（Role-Based Access Control）

SDK：软件开发工具包（Software Development Kit）

5 技术架构

数据流通区块链存证技术架构包括以下部分，见图1。

a) 存证网络：由共识节点、区块链平台、协议机制、网关与接口组成。

b) 数据存证：由存证对象、存证手段和存证阶段组成。存证对象包括数据流通各存证阶段涉及的数据哈希值、数据产权、数据权益、控制策略、操作行为等。存证手段包括数据加密、数据脱敏、数字签名、智能合约等。存证阶段包括数据采集、数据存储、数据传输、数据登记、数据共享、数据开放、数据运营、数据产品交易、数据应用、数据回收、数据销毁等。

c) 存证服务：由存证查询、存证提取、存证验证、存证追溯等服务组成。

d) 存证安全：由系统安全、存储安全、传输安全等组成。

e) 监测与评估：由网络监测、行为监测、存证有效性评估等组成。

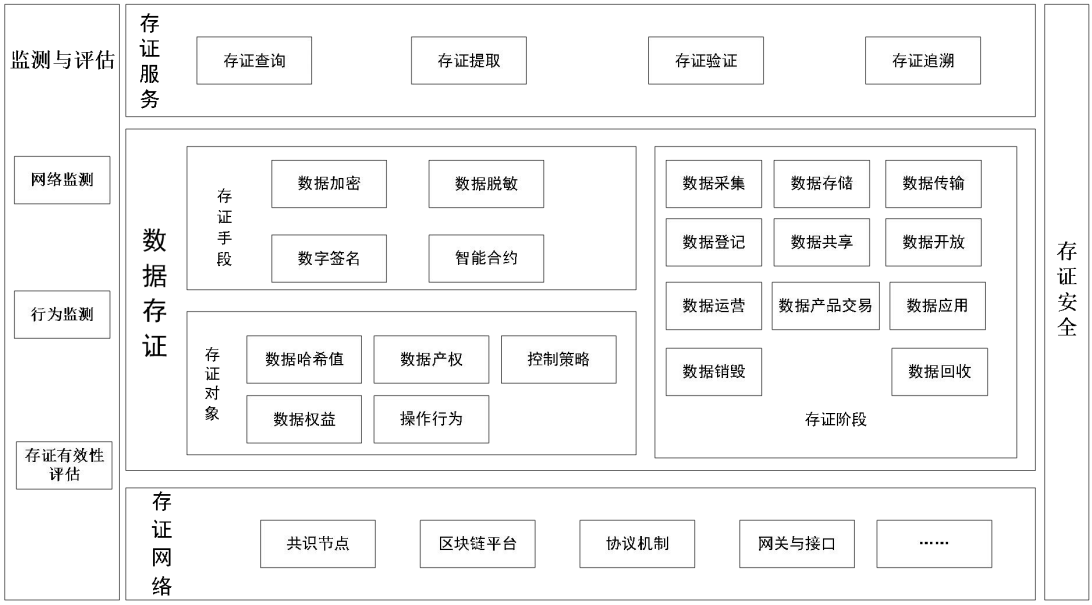

图 1 数据流通区块链存证技术架构

6 存证网络

6.1 共识节点

6.1.1 宜支持对网络中的存证交易进行验证（如身份合法性、数据完整性检查），符合规则的交易被打包成候选区块，经共识算法确认后加入区块链。
6.1.2 宜具备维护全网账本一致性，确保所有节点存储相同的存证记录，支持司法取证时的数据可验证。
6.1.3 宜支持多节点冗余部署（如分布式集群）避免单一节点失效影响网络。

6.2 区块链平台

6.2.1 宜支持将数据的哈希值或完整数据存储在区块链上，确保数据的真实性、完整性和不可篡改。
6.2.2 宜支持对存证数据的统一管理，包括数据的查询、检索、分类等。
6.2.3 宜支持对区块链网络中的节点进行管理，包括节点的添加、删除、状态监控等。
6.2.4 宜支持智能合约的部署和执行，通过自动化脚本代码实现存证流程的自动化、规范化。

6.3 协议机制

6.3.1 宜支持数据存储和加密机制，将任意长度数据转换为固定长度哈希值，用于数据完整性校验。
6.3.2 宜支持分层组网结构和节点通信，支持全节点存储完整区块链数据和轻节点仅存储哈希索引，并保证节点间高效传输区块、交易等数据。

6.4 网关与接口

6.4.1 宜支持将外部系统的非区块链协议（如 HTTP、WebService）转换为区块链网络支持的通信协议（如 P2P、gRPC）。
6.4.2 宜支持通过 API 密钥机制验证调用方身份，确保仅授权用户或系统可访问存证网络。
6.4.3 宜提供 Java、Python、Go 等多语言 SDK，简化开发者接入流程。
6.4.4 宜允许开发者通过调用链上智能合约实现自动化存证。

7 数据存证

7.1 存证对象

7.1.1 数据哈希值

7.1.1.1 应采取与数据相契合的国密算法（如 SM3 等），确保哈希值能有效地代表数据内容，避免数据篡改。
7.1.1.2 应支持与算法相契合的哈希值长度，确保哈希值足够唯一且具有抗碰撞性。
7.1.1.3 应具有数据来源方信息，在存证时应记录数据来源方的相关信息，确保数据的来源可追溯、可验证。

7.1.2 数据产权

7.1.2.1 应具有数据产权方信息，包括产权方身份信息、联系方式等，确保数据的产权清晰可追溯。
7.1.2.2 应具有数据资源或数据产品唯一标识符，确保每个标识独立且不重复，以供查询和验证。
7.1.2.3 宜具有数据产权变更记录，如转让、授权、许可等，确保数据产权的变动过程透明可追溯。

7.1.3 数据权益

7.1.3.1 应具有数据权益方信息，包括权益方身份信息、联系方式等，确保权益关系清晰、明确。
7.1.3.2 应具有数据权益生效时间，确保数据权益的开始时间可追溯，避免权益生效时间混乱或不明确。
7.1.3.3 应具有数据权益详细信息，包括数据权益的具体内容（如使用权限、分配比例、限制条件等），确保权益条款完整，以供核对与验证。

7.1.4 控制策略

7.1.4.1 应具有详细控制策略信息，包括数据使用规则、访问权限、数据共享限制等，确保控制策略的全面性和可执行性。
7.1.4.2 应具有控制策略生效时间，确保在策略变更或合约执行过程中能准确追溯控制的时效性。

7.1.5 操作行为

7.1.5.1 应具有操作行为涉及的多方信息，包括操作方、受影响方等，确保操作行为的责任方和相关方明确。
7.1.5.2 宜具有与操作行为相关的数据资源或数据产品唯一标识符，确保操作行为与数据资源或数据产品一一对应。
7.1.5.3 应具有操作行为的类型和时间信息，以供行为追溯和验证。

7.2 存证手段

7.2.1 智能合约

7.2.1.1 应具备防篡改和抗抵赖性。
7.2.1.2 应具备生命周期管理能力，包括合约创建、部署、升级、触发、执行、废止等。
7.2.1.3 合约的每次修改应重新部署。
7.2.1.4 应具备可终止性，对其所能支配的资源进行有效限制，防止资源被恶意滥用。
7.2.1.5 应具备数据上链、传输、访问、修改、销毁等功能，并记录操作主体（数字身份标识）、操作类型及时间戳、数据版本号或状态变更记录。

7.2.2 数据加密

7.2.2.1 使用的密码产品与密码模块应通过国家密码管理部门核准。
7.2.2.2 应确保已上链存储密文无法被破解。
7.2.2.3 应遵守敏感信息最小化暴露原则，仅加密敏感字段（如身份证号），非敏感字段（如时间戳）可明文存证。
7.2.2.4 应支持零知识证明，在不暴露原始数据的情况下验证数据属性（如证明年龄≥18 岁）。

7.2.3 数据脱敏

7.2.3.1 脱敏后的数据无法通过技术手段还原原始数据（特殊授权场景除外）。
7.2.3.2 脱敏后的数据应保持数据间的逻辑关系。
7.2.3.3 脱敏后的数据应满足业务分析或开发测试需求。
7.2.3.4 脱敏后数据的唯一性应与原始数据的唯一性保持一致。

7.2.4 数字签名

7.2.4.1 数字签名应与特定的消息和签名者唯一对应。
7.2.4.2 数字签名应具有不可抵赖性。
7.2.4.3 应支持通过签名者公钥和相应的验证算法来验证数字签名的有效性。
7.2.4.4 数字签名技术应与区块链平台的技术架构和共识机制相兼容。

7.3 存证阶段

7.3.1 数据采集

7.3.1.1 应支持将数据生成时间、数据来源标识（如采集设备 ID、IP 地址、传感器编号等）及采集方身份信息上链存证。
7.3.1.2 应支持将存证方的公钥或区块链地址上链存证。
7.3.1.3 应制定统一的数据格式和元数据规范等数据标准，并支持将数据标准上链存证。
7.3.1.4 应支持 RESTful API、gRPC 等接口协议，Kafka、RabbitMQ 等消息队列，实现数据同步和异步采集，并将数据拉取方式和数据拉取记录上链存证。
7.3.1.5 应支持从外部区块链（如以太坊、联盟链）获取数据（如资产状态、交易记录），经共识验证后写入目标链。

7.3.2 数据存储

7.3.2.1 应支持将原始数据的密码学哈希值（如 SM2、SM3 等）、存储地址、存储方式、存储方身份信息等上链存证。
7.3.2.2 应支持将数据上链的精确时间及数据的元数据信息（包括数据的类型、格式、版本号等）进行存证。
7.3.2.3 应支持将智能合约地址、区块链交易哈希值（TxHash）及区块高度上链存证，用于快速检索验证。
7.3.2.4 应支持对同一数据的不同版本（如合同修订、文件更新）生成独立哈希值，通过区块链的链式结构记录版本演变历史，将历史数据版本上链存证。
7.3.2.5 应支持将大文件分割为多个数据片，分布存储于不同节点/服务器，将数据的分布情况进行存证。

7.3.3 数据传输

7.3.3.1 应支持将数据传输双方的身份信息上链存证，包括发送方和接收方的唯一标识符、认证信息等。
7.3.3.2 应支持将数据资源唯一标识符上链存证。
7.3.3.3 宜采用数字签名和加密技术（如 SM2），确保数据在传输过程中的完整性、保密性和不可篡改性。
7.3.3.4 可支持数据传输失败后的重传机制，确保在数据丢失或传输错误的情况下，能自动或手动进行数据重传，确保数据完整性。重传机制应具备自恢复能力，确保在不同的网络环境下能顺利完成数据传输。

7.3.4 数据登记

7.3.4.1 应支持对数据登记信息上链存证，包括数据资源/产品的唯一标识符、产权方信息、产权类型、产权生效时间及终止时间、权益方信息、权益类型、权益生效时间和限制条件等。
7.3.4.2 宜采用数字签名验证数据的登记，确保登记过程中数据的完整性、合法性及不可篡改性。

7.3.4.3　宜采用数据水印技术对登记数据进行隐式标识，确保数据在流通过程中可追溯来源。

7.3.5　数据共享

7.3.5.1　应支持将参与共享的多方资质文件上链存证，支持多方联合签名技术（如阈值签名技术），确保不可篡改。
7.3.5.2　应支持通过智能合约定义数据共享范围、使用期限及分成规则，合约触发后自动执行数据授权与结算（如按结果调用次数计费），并将数据授权与结算信息自动上链存证。
7.3.5.3　应支持在多方协作场景下，通过技术手段实现数据的安全流动与联合计算，确保共享过程合规、可控、可追溯。
7.3.5.4　应支持强制采用联邦学习、安全多方计算或可信执行环境进行数据联合计算，确保原始数据不出域。
7.3.5.5　宜支持构建全链路数据血缘图谱，记录数据从提供方到使用方的流转路径（如某基因数据经3次共享后用于某药物研发），并将数据流转路径自动上链存证。
7.3.5.6　宜支持通过中继链或原子交换协议实现跨链数据验证。
7.3.5.7　宜支持实时监测共享数据的使用行为（如异常高频下载），触发自动熔断（如暂停API访问）或人工复核。
7.3.5.8　宜支持黑白名单机制，限制高风险IP或机构参与共享。
7.3.5.9　可支持根据智能合约规则，将数据使用收益（如模型训练费用）按比例自动分配至数据提供方、计算节点及平台账户，并将数据使用收益分配信息自动上链存证。

7.3.6　数据开放

7.3.6.1　应支持将开放数据相关说明信息（包含数据来源、用途限制、脱敏标准等）上链存证，并与数据开放接口绑定。
7.3.6.2　应对开放数据绑定唯一哈希标识，并将其哈希标识和开放时间戳自动上链存证。
7.3.6.3　应提供统一API接口，支持按需获取脱敏后的数据（如基因统计结果），接口应强制身份认证和流量限速（如每秒10次请求）。
7.3.6.4　应支持通过逻辑隔离（如独立命名空间）或物理隔离（如专用节点）区分开放数据与内部数据，防止未授权访问。
7.3.6.5　宜支持基于智能合约定义数据开放规则（如仅限科研用途），自动拦截违规请求（如商业公司访问未授权字段），并将数据开放规则自动上链存证。
7.3.6.6　宜支持对开放数据的时效性（如基因数据更新频率）、完整性（如字段缺失率≤1%）进行实时监测，异常时自动暂停开放服务，并将监测异常信息自动上链存证。

7.3.7　数据运营

7.3.7.1　资质审核

7.3.7.1.1　应支持将企业营业执照、数据运营授权或许可证书等关键资质文件上链存证，确保不可篡改。
7.3.7.1.2　应支持实时验证资质有效性，通过API对接相关系统，自动检查资质状态。
7.3.7.1.3　应支持将敏感信息的脱敏证明（如数据匿名化处理记录）、安全审计报告及/或伦理审查报告上链存证。
7.3.7.1.4　宜支持将数据提供方过往违规记录（如数据泄露事件）上链存证。
7.3.7.1.5　可支持使用AI技术自动解析资质文件内容，对比模板库识别伪造或篡改痕迹。

7.3.7.1.6　可支持根据监管政策动态调整审核条件（如新增个人信息保护条款时自动更新校验逻辑），将变更信息上链存证。

7.3.7.2　协议签订

7.3.7.2.1　应支持提供标准化协议模板（如数据开发利用协议、收益分成协议），支持关键参数自定义（如分成比例、有效期）。
7.3.7.2.2　应支持合约签署后自动上链存证，绑定双方数字签名（如基于 CA 证书）及时间戳。
7.3.7.2.3　应支持根据协议条款自动触发数据访问授权、收益结算等操作(如按流量计费时实时扣款)，并将操作行为自动上链存证。
7.3.7.2.4　宜支持跨机构多方在线签署，确保协议版本一致性，避免篡改风险。
7.3.7.2.5　宜支持对接司法链或第三方存证平台，生成电子证据包。
7.3.7.2.6　可支持允许通过链上投票机制（如需超 75%参与方同意）动态修改协议条款。
7.3.7.2.7　可支持使用自然语言处理分析协议文本，自动标记法律风险点（如模糊权责描述）。

7.3.7.3　数据授权

7.3.7.3.1　应支持基于 RBAC 或 ABAC 控制数据访问范围（如仅允许药企访问脱敏后的基因统计结果）。
7.3.7.3.2　应支持将所有授权操作（如权限分配、撤销等）自动上链存证，支持操作溯源。
7.3.7.3.3　宜支持采用联邦学习、安全多方计算等技术授权数据使用，避免原始数据外泄。
7.3.7.3.4　宜支持通过中继链或预言机跨链同步授权状态，确保权限一致性。
7.3.7.3.5　可支持预设审批规则（如低风险申请自动通过），减少人工干预。
7.3.7.3.6　可支持对授权数据的实际使用行为（如下载、分析）进行全流程监控，异常操作实时告警，并将使用行为和告警信息自动上链存证。

7.3.7.4　产品开发

7.3.7.4.1　应支持提供 RESTful API 或 SDK，支持开发方快速接入授权数据，接口需强制身份认证（如 OAuth 2.0），并将接入数据的开发方身份信息和接入时间戳自动上链存证。
7.3.7.4.2　应支持提供隔离的测试环境，内置模拟数据（如合成基因序列）供产品开发调试，防止真实数据泄露，并将隔离策略上链存证。
7.3.7.4.3　宜支持对开发过程中使用的数据质量（如完整性、一致性）进行实时监测，异常时自动暂停服务，并将监测异常信息自动上链存证。
7.3.7.4.4　宜支持将产品迭代版本上链存证，并关联原始数据哈希值，确保结果可复现。
7.3.7.4.5　宜支持对产品进行测试，验证其是否符合开发需求、合规要求、安全要求等，并将测试验证结果上链存证。

7.3.7.5　收益分配

宜支持根据产品实际收益（如销售额）自动按协议比例分配至数据提供方账户，并将收益分配信息自动上链存证。

7.3.8　数据产品交易

7.3.8.1　合规审查

7.3.8.1.1　应支持将合规审查产品的基本信息上链存证，包括但不限于产品名称、类型等基本信息。
7.3.8.1.2　应支持将合规审查结果上链存证，包括审查结论、存在的风险点、合规性分析报告等。

7.3.8.1.3 应支持将合规审查责任方信息上链存证，如审查单位、负责人等。
7.3.8.1.4 宜支持将合规审查提供方信息上链存证，包括提供审查服务的内部机构或第三方服务方。
7.3.8.1.5 可支持 AI 合规审查结果自动记录算法版本及训练责任方，并与审查结论链上绑定。

7.3.8.2 产品上架

7.3.8.2.1 应支持将产品提供方信息自动上链存证，包括产品提供方的名称、联系方式等信息。
7.3.8.2.2 应支持将上架产品的基本信息自动上链存证，包括产品名称、类别、数据类型等。
7.3.8.2.3 应支持将产品上架时间自动上链存证，确保准确记录每个产品上架的时间戳。
7.3.8.2.4 应支持将产品上架后的变更记录自动上链存证，包括价格、描述、使用限制等信息的变更记录。

7.3.8.3 供需撮合

7.3.8.3.1 应支持将线上撮合的双方信息自动上链存证，包括供方和需方的身份信息、联系方式等。
7.3.8.3.2 应支持将线上撮合记录自动上链存证，包括撮合的时间、撮合条件、撮合结果等。
7.3.8.3.3 宜支持采用基于规则引擎或机器学习的智能撮合引擎，提高数据供需精准匹配效率。

7.3.8.4 交易签约

7.3.8.4.1 应支持将交易签约双方的信息上链存证，如身份信息、联系方式等。
7.3.8.4.2 应支持将交易产品的基本信息上链存证，包括产品名称、类型、规格、价格等。
7.3.8.4.3 应支持将交易合同上链存证，包括合同唯一标识符及合同内容等。
7.3.8.4.4 可支持采用自然语言处理技术结合规则引擎，对合同文本进行语义分析和合规性校验。
7.3.8.4.5 可记录对合同条款进行合规性审查的结果，如是否符合相关法律法规、是否通过第三方审核等，并将相关审查记录上链存证。

7.3.8.5 产品交付

7.3.8.5.1 应支持将交付产品的基本信息上链存证，包括产品名称、类型、规格、数量、交付形式等，确保存证信息完整。
7.3.8.5.2 应支持将产品交付时间上链存证。
7.3.8.5.3 应支持将交付完成的确认信息上链存证，包括接收方的确认签字或电子确认等。
7.3.8.5.4 宜支持对数据传输链路进行监控，实时检测异常并及时告警，保障交付过程顺利完成。

7.3.8.6 支付结算

7.3.8.6.1 应支持将支付信息上链存证，包括支付方和收款方信息、支付金额、支付方式、支付时间，以及支付关联的合同唯一标识符、产品基本信息等。
7.3.8.6.2 应支持将支付结算的状态变化上链存证，如支付已完成、支付失败、结算已确认等。
7.3.8.6.3 宜支持与第三方支付平台、银行接口对接，满足多种支付方式需求。

7.3.8.7 产品下架

7.3.8.7.1 应支持将下架产品的基本信息、提供方信息、下架时间等上链存证。
7.3.8.7.2 应支持将下架原因上链存证，如产品下架通知、产品过期、市场需求变化等。

7.3.9 数据应用

7.3.9.1 需求申请

7.3.9.1.1 应按照数据分类分级使用要求制定需求申请原则（如按需申请、最小权限原则）并上链存证。
7.3.9.1.2 应支持将需求申请方的区块链地址或数字身份凭证及数字签名上链存证。
7.3.9.1.3 应对每项需求申请赋予唯一标识符，并支持将数据申请唯一标识符、申请目的、申请内容、应用场景、申请操作时间戳等信息上链存证。

7.3.9.2 需求审核

7.3.9.2.1 应支持将被申请数据的哈希值、申请方的区块链地址、审核方的区块链地址、数字签名或机构证书哈希值、需求审核唯一标识符、审核操作、审核意见等上链存证。
7.3.9.2.2 应支持将访问控制策略、相关的法律条文哈希值等上链存证。
7.3.9.2.3 应通过 DID 或 CA 证书实现参与方的实名认证，确保数据申请方、提供方身份真实可信。
7.3.9.2.4 应对每项需求审核赋予唯一标识符，并与需求申请唯一标识符关联绑定。

7.3.9.3 应用开发

7.3.9.3.1 应支持将开发方的区块链地址或 DID、智能合约的部署信息等上链存证。
7.3.9.3.2 应支持将开发应用描述、应用场景、应用版本号、开发文档、开发日志等上链存证。
7.3.9.3.3 应对开发应用赋予唯一标识符，并与需求申请唯一标识符和需求审核唯一标识符关联绑定。
7.3.9.3.4 应支持将应用开发的 API 网关、智能路由、数据中间件、ETL 工具等上链存证。
7.3.9.3.5 应支持不同区块链网络之间的数据流通与互操作，并将多链环境下的数据（如跨链数据交易、跨链身份认证）存证上链。

7.3.9.4 成效反馈

7.3.9.4.1 应支持将数据应用涉及的数据生成者身份、上链操作者地址、前序相关交易哈希值，以及关键业务指标、用户反馈意见等信息上链存证。
7.3.9.4.2 涉及个人信息的成效反馈应先脱敏或加密后再上链。
7.3.9.4.3 保留历史版本哈希值的同时应支持成效反馈数据版本的更新。
7.3.9.4.4 高频更新成效反馈数据宜采用"链上指针+链外存储"模式。

7.3.10 数据回收

应支持将数据回收相关信息上链存证，包括数据资源/产品唯一标识符、回收原因（如数据不再使用、过期失效、不合规等）、回收时间，以及回收后数据的处理方式（如回收数据是否销毁、存档或转交第三方）等。

7.3.11 数据销毁

应支持将数据销毁全过程记录上链存证，包括数据资源/产品唯一标识符、销毁原因（如法规要求、隐私保护、防止数据恢复等）、参与节点、销毁方式（如物理销毁和逻辑销毁）、销毁时间、销毁状态、销毁确认等。

8 存证服务

8.1 存证查询

8.1.1 应支持根据特定条件（如存证数据的唯一标识符、时间戳、责任方等）准确查询到相关存证数据。
8.1.2 应快速响应查询请求，响应时间应不高于 2 秒。
8.1.3 宜支持多维度查询方式，包括按数据内容、存证时间、存证类型、数据产权等多个维度进行灵活查询。
8.1.4 可支持查询权限控制，按权限级别控制查询相应的存证信息，防止未授权用户访问敏感数据。

8.2 存证提取

8.2.1 应支持根据特定条件（如存证数据的唯一标识符、时间戳、责任方等）准确提取到相关存证数据。
8.2.2 应快速响应提取请求，响应时间应不高于 2 秒。
8.2.3 宜支持批量提取功能，允许用户一次性提取多个存证数据。
8.2.4 可支持提取权限控制，按权限级别控制提取相应的存证信息，防止未授权用户访问敏感数据。

8.3 存证验证

8.3.1 应支持验证存证数据的真实性、完整性和有效性。
8.3.2 应快速响应验证请求，响应时间应不高于 2 秒。
8.3.3 宜支持多种验证方式，包括但不限于基于哈希值的完整性校验、数字签名验证、时间戳验证等多种方式，以适应不同场景和需求。

8.4 存证追溯

8.4.1 应支持完整追溯数据存证历史记录，包括存证数据的来源、变更历史以及相关操作等。
8.4.2 宜支持可视化追溯工具，通过图形化界面展示数据存证全生命周期的变更历史、操作流程及关键节点。

9 存证安全

9.1 网络安全保护能力应符合存证活动所处的行业或业务安全要求，等级符合 GB/T 22239 的规定。
9.2 信息系统的密码应用应符合 GB/T 39786 的规定。
9.3 个人信息安全应符合 GB/T 35273 的规定，其中，人脸识别安全应遵循 GB/T 41819 的规定。
9.4 采用 SM3 加密算法应符合 GB/T 32905 的规定，采用 SM2 加密算法应符合 GB/T 32918.1、GB/T 32918.2、GB/T 32918.3、GB/T 32918.4、GB/T 32918.5 的规定。
9.5 应按照 GB/T 43697 的规则对存证数据及相关业务数据进行分类分级管理。
9.6 应采用符合国家密码管理部门认证核准的密码技术进行加密存储，确保存证数据可用不可见。
9.7 所有存储操作应记录在链，支持全生命周期审计。
9.8 应具备冗余备份和存储扩展能力，并具备异地容灾能力，防止单点故障导致丢失。
9.9 应在区块链节点之间应建立安全连接，使用加密技术进行传输。
9.10 应利用数字证书来验证节点的身份，确保只有合法的节点能接入区块链网络并进行数据传输。
9.11 在传输过程中，宜对每个数据包或数据块计算哈希值，并将哈希值与数据一起传输。
9.12 宜利用智能合约来定义和管理数据的访问权限，对不同的用户或节点授予不同的访问权限。

10 监测与评估

10.1 网络监测

10.1.1 应支持实时监测节点在线状态、区块同步进度、交易吞吐量等核心指标。
10.1.2 应支持自动触发告警机制（如节点宕机、网络延迟超阈值）。
10.1.3 应支持监控异常流量（如 DDoS 攻击）、恶意节点行为（如双重支付尝试）及智能合约漏洞。
10.1.4 应支持记录攻击日志并生成安全报告，支持快速溯源。
10.1.5 宜支持监测存证数据是否合规，自动标记敏感操作。
10.1.6 可支持监控跨链交易状态和资产锁定/解锁过程。
10.1.7 可支持对常见问题（如节点失联）触发预设脚本自动修复（如重启服务）。

10.2 行为监测

10.2.1 应支持记录用户操作日志（如数据上传、查询、修改权限），绑定数字签名确保不可抵赖性。
10.2.2 应支持检测异常高频操作（如短时间内多次数据覆盖请求）。
10.2.3 应支持监控合约调用参数、Gas 消耗及执行结果，识别潜在逻辑漏洞或恶意代码注入。
10.2.4 宜支持对不同角色（如管理员、普通用户）的操作权限分级审计，防止越权访问。
10.2.5 宜支持操作日志与用户身份（如 CA 证书）绑定，确保行为可追溯至具体责任人。
10.2.6 宜支持内置法规模板，自动标记违反隐私政策的操作（如未脱敏数据上链），并生成合规报告。
10.2.7 可支持基于机器学习分析用户行为模式，预测潜在攻击（如内部人员数据窃取），提前触发防御机制。
10.2.8 可支持监控跨链操作的关联性（如数据资产转移与合约调用的匹配性），防止双花或资产丢失。

10.3 存证有效性评估

10.3.1 应建立多层级验证机制，建立节点共识验证（≥3 个独立节点）、时间戳比对、哈希值校验的三重验证体系，确保数据完整性与时序可信。
10.3.2 应采用适当的区块链分析工具，检测智能合约漏洞、共识算法偏差等风险。
10.3.3 应建立定期巡检机制，重点检查节点失效或共识异常情况。
10.3.4 应审查数据流通存证内容和过程的合规性。
10.3.5 应结构化输出评估报告，包含存证有效性评分及风险修复建议，重要数据应附加全链路元数据及安全评估证明。
10.3.6 应根据评估报告中的改进建议，采取纠正措施，提升存证有效性，如优化存证过程，规范存证内容，优化存证节点配置（如调整共识算法权重）及更新安全策略（如加密算法升级）等。

参考文献

[1] 工业和信息化部 中央网络安全和信息化委员会办公室 工信部联信发〔2021〕62 号 关于加快推动区块链技术应用和产业发展的指导意见

[2] 最高人民法院 法发〔2022〕16 号 关于加强区块链司法应用的意见

[3] 工业和信息化部 中央网络安全和信息化委员会办公室 国家标准化管理委员会 工信部联科〔2023〕260 号 关于印发《区块链和分布式记账技术标准体系建设指南》的通知

[4] 国家发展改革委 国家数据局 工业和信息化部 发改数据〔2024〕1853 号 关于印发《国家数据基础设施建设指引》的通知

[5] 国家数据局 国数资源〔2024〕119 号 关于印发《可信数据空间发展行动计划（2024—2028 年）》的通知