ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

基于区块链的环境监测数据溯源技术指南

Technical Guide for Traceability of Environmental Monitoring Data Based on Block chain

（工作组讨论稿）

（本草案完成时间：2026 - 6 - 12 ）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　　发 布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

基于区块链的环境监测数据溯源技术指南

1 引言

生态环境监测是生态文明建设的基础性支撑，监测数据的真实可信、完整可溯是生态环境科学决策、精准治污、依法行政的核心依据。当前，生态环境监测数字化转型持续推进，传统数据管理模式存在信息孤岛、中心化存储易篡改、全流程溯源缺失、司法采信不足等问题，制约了生态环境治理现代化与跨区域数据互通互认。区块链具备不可篡改、全程可追溯、分布式共识、多方互信的核心优势，可有效破解监测数据全生命周期监管难题。为贯彻落实生态文明、数字中国建设战略部署，统一全国区块链生态环境监测数据溯源技术标准，构建安全可控、权威统一的数据存证溯源体系，提升监测数据公信力与司法效力，支撑智慧生态环境监管建设，特制定本文件。规范了区块链生态环境监测数据溯源系统的架构体系、数据标准、存证核验、安全运维等全维度要求，为全国各类监测主体开展溯源系统建设、数据上链存证与合规应用提供统一技术依据。

2 范围

规定了基于区块链技术的生态环境监测数据溯源体系的术语和定义、缩略语、总体架构、技术参考框架、数据格式与上链规范、数据采集与存储要求、溯源核验工作流程、系统性能与网络安全要求、常态化运维管理规范等核心内容。适用于全国各级生态环境监测机构、检验检测实验室、排污单位自行监测体系、第三方监测运维服务机构开展区块链生态环境监测数据溯源系统建设、数据全生命周期上链存证、溯源核验、数据合规管理等相关工作。各级生态环境监管部门的数据审计、监督核查、执法取证工作可参照执行，国土、水利、农业农村等相关领域生态环境监测数据区块链溯源应用可参照本文件执行。

3 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 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

GB/T 11457-2006 信息技术软件工程术语

GB/T 25069-2022 信息安全技术术语

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 39786-2021 信息安全技术信息系统密码应用基本要求

GB/T 42570-2023 信息安全技术区块链技术安全框架

GB/T 42752-2023 区块链和分布式记账技术参考架构

HJ 630-2011 环境监测质量管理技术导则

HJ 8.2-2020 生态环境档案管理规范生态环境监测

CJJ/T 182-2014 城镇供水与污水处理化验室技术规范

RB/T 214-2017 检验检测机构资质认定能力评价检验检测机构通用要求

IETF RFC 6960 在线证书状态协议（OCSP）

IETF RFC 5246 传输层安全协议（TLS 1.2）

4 术语和定义

GB/T 25069-2022、GB/T 42752-2023、HJ 630-2011 界定的以及下列术语和定义适用于本文件。

4.1 区块链

一种使用密码技术将共识确认的区块按顺序追加而形成的分布式账本，具备分布式共识、不可篡改、全程可追溯、多方共治的技术特征。

[来源：GB/T 42752-2023，3.1]

4.2 生态环境监测数据

在大气、水质、土壤、噪声、固体废物、生态质量等各类生态环境监测活动中产生的原始监测记录、指标监测数值、统计分析结果、质控数据及配套元数据的总称，是生态环境治理的核心基础数据资源。

4.3 数据溯源

完整记录、全程追踪生态环境监测数据从采集生成、加密传输、合规存储、审核使用、归档留存的全生命周期行为，实现数据来源可查、去向可追、责任可究、篡改可证的全过程管控机制。

4.4 数据上链

将生态环境监测原始数据、报告数据、运维日志数据本体或其加密数字指纹（哈希值），通过合规流程写入区块链分布式账本，并生成唯一法定存证标识的标准化存证过程。

4.5 智能合约

存储在分布式记账技术系统中的可自动执行的计算机程序，所有触发条件、执行动作、执行结果均全程记录于分布式账本，实现监测数据存证、核验、授权、审计的自动化、合规化管控。

[来源：GB/T 42752-2023，3.14]

4.6 时间戳

基于密码签名技术，对原始监测数据、签名参数、生成时间、操作主体等信息进行加密签名的数字凭证，具备法定存证效力，可证明原始数据的真实存在性与时序唯一性。

4.7 哈希值

通过国密哈希算法将任意长度的生态环境监测数据压缩生成的固定长度二进制数字串，是监测数据唯一、不可逆、可核验的数字指纹。

5 缩略语

下列缩略语适用于本文件：

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

CA：证书认证机构（Certificate Authority）

DApp：去中心化应用（Decentralized Application）

IoT：物联网（Internet of Things）

JSON：JavaScript 对象表示法（JavaScript Object Notation）

PKI：公钥基础设施（Public Key Infrastructure）

REST：表述性状态传递（Representational State Transfer）

SDK：软件开发工具包（Software Development Kit）

SM2：国产椭圆曲线公钥密码算法

SM3：国产密码杂凑算法

SM4：国产分组密码算法

TPS：每秒交易数（Transaction Per Second）

XML：可扩展标记语言（Extensible Markup Language）

6 总体架构

基于区块链的生态环境监测数据溯源系统应立足国家生态环境数字化治理体系建设要求，构建分层解耦、安全可控、多方共治、全域互通的总体架构，自上而下分为数据源层、区块链网络层、应用服务层、用户交互层四层体系，适配全国统一监测数据监管、跨区域数据互认、司法存证采信的国家级应用需求。

6.1 架构组成

系统四层架构功能定位如下：

6.1.1 数据源层：作为系统数据底座，涵盖全国各类标准化生态环境监测终端，包括大气、水质、土壤、噪声自动监测站、便携式监测仪器、实验室精密分析设备、全域物联网感知传感器网络，同时兼容人工合规录入终端、各级生态环境监管平台、企业自行监测系统等第三方合规数据接口，实现多源监测数据的标准化汇聚。

6.1.2 区块链网络层：采用国家规范的联盟链架构，构建多方共治的可信区块链网络，由权威共识节点、合规记账节点、轻量化接入节点共同组成，部署国产化合规智能合约体系，实现监测数据标准化存证、完整性核验、分级授权访问、全程审计追溯，筑牢数据可信底座。

6.1.3 应用服务层：面向国家级、省级、市县级生态环境监管及行业应用需求，搭建标准化功能模块，涵盖多源数据采集适配、合规上链存证管理、全维度溯源查询核验、数据质量统计分析、异常风险预警、系统合规配置、安全审计管控等核心能力，支撑常态化监管应用。

6.1.4 用户交互层：构建分级分类的访问服务体系，面向各级生态环境监管部门、检验检测机构、排污主体、第三方审计机构、社会公众等不同主体，提供合规 Web 端、移动端、标准化 API 接口多元化访问方式，实现分级授权、按需使用、全程可控。

6.2 溯源数据流

生态环境监测数据全生命周期溯源数据流应遵循源头可信、全程加密、链证分离、双向映射、可验可溯的国家级规范，具体流向如下：

6.2.1 数据源层完成监测数据标准化采集，通过国密算法加密处理，经主体数字签名、SM3 哈希计算生成唯一数据指纹，从源头保障数据真实不可抵赖；

6.2.2 加密数据指纹通过安全 API 网关合规提交至区块链网络，经分布式节点共识验证、合规校

验后打包上链，生成不可篡改的链上存证记录；

6.2.3 原始监测数据本体、影像资料、原始报表等大容量数据，存储于国家合规可信数据库或分布式可信文件系统，与链上哈希指纹形成唯一映射关系，兼顾链上存证公信力与系统运行效能；

6.2.4 开展数据溯源核验时，通过实时比对待核验数据哈希值与链上固化存证指纹，快速验证数据完整性、真实性，输出法定核验结果，支撑监管执法与司法采信。

6.3 参与角色与职责

立足国家生态环境协同治理体系，明确系统多方参与主体权责，构建权责清晰、各司其职、相互监督、全程可究的共治机制：

6.3.1 数据生产方：各级监测机构、检测实验室、排污单位等主体，承担监测数据标准化采集、合规封装、加密签名、规范上链的主体责任，对原始数据的真实性、准确性、完整性承担法定责任；

6.3.2 节点运营方：经监管部门备案的区块链节点运维主体，负责区块链网络节点合规部署、常态化运维、共识参与、账本维护，保障全网稳定运行、数据合规存证；

6.3.3 监管方：各级生态环境主管部门，拥有全网最高权限，可开展全量链上数据审计、溯源核验、合规督查、执法取证，统筹区域内监测数据溯源体系规范化建设；

6.3.4 公众/第三方主体：经监管授权、合规备案的社会公众、审计机构、科研单位等，可依规查询特定存证数据的核验状态、溯源信息，接受社会监督，提升生态环境治理公开透明度。

7 技术参考框架

系统技术框架严格遵循国家网络安全、密码应用、区块链技术、生态环境监测相关国家标准与行业规范，坚持国产化、标准化、安全化、普惠化建设原则，适配全国规模化推广应用需求。

7.1 区块链网络选型

7.1.1 架构选型：生态环境监测数据溯源系统统一采用合规联盟链架构，由生态环境主管部门牵头，联合检测机构、认证机构、行业龙头单位、科研机构等多方主体共建共治，平衡数据隐私安全、多方互信协作、监管公开透明的国家级应用需求，适配跨区域、跨层级、跨主体的数据互通互认场景。

7.1.2 共识机制：系统共识机制优先选用实用拜占庭容错（PBFT）及国产化改进算法，保障交易高效确认、账本一致性与容错能力，单共识组有效节点数量不少于 4 个，交易最终确认时延不超过 3 秒，满足生态环境监管实时核验、快速取证的业务需求。

7.1.3 智能合约适配：区块链网络全面支持标准化智能合约部署，优先选用安全性高、适配性强的

Solidity、Go 等主流合规合约语言，所有上线合约代码必须经过第三方权威机构安全审计，杜绝合约漏洞风险，保障链上业务逻辑合规可控。

7.2 密码安全要求

系统密码体系全面落实国家密码管理政策，严格符合 GB/T 39786-2021 第三级及以上密码应用安全要求，全面采用国产化密码算法，构建自主可控、安全可靠的密码应用体系。

7.2.1 数据哈希计算统一采用 SM3 国产密码杂凑算法，固定输出 256 比特哈希值，作为监测数据唯一数字指纹；

7.2.2 数据数字签名、身份验签全程采用 SM2 国产椭圆曲线公钥密码算法，密钥长度 256 比特，保障数据确权可追溯、操作不可抵赖；

7.2.3 数据传输加密采用 SM4 国产分组密码算法或 TLS 1.2 及以上安全传输协议，密钥更新周期不超过 90 天，常态化防范数据传输泄露、篡改风险；

7.2.4 所有主体私钥严禁明文存储，必须存储于硬件安全模块（HSM）或可信执行环境（TEE），落实国家级信息安全防护要求。

7.3 智能合约设计

围绕生态环境监测数据存证、核验、授权、审计全流程管控需求，部署四大核心标准化智能合约，实现业务流程自动化、规范化、法治化管控。

7.3.1 存证合约：标准化接收监测数据哈希值、全量元数据，自动生成合规时间戳，固化写入分布式账本，完成法定存证；

7.3.2 核验合约：自动比对待核验数据哈希值与链上原始存证记录，精准判定数据完整性、真实性，输出标准化核验结果；

7.3.3 授权合约：分级分类管理监管部门、监测机构、第三方主体的系统访问、数据查询、业务操作权限，落实最小权限原则；

7.3.4 审计合约：全程记录所有链上操作行为、业务日志、核验记录，支持全维度审计追溯与责任认定。

7.3.5 智能合约支持安全合规的版本迭代升级机制，所有重大升级操作须经不少于 3 家核心节点运营方多签确认、全程留痕，保障系统迭代可控。

7.4 API 接口规范

为实现全国系统互联互通、数据共享共用，统一标准化 API 接口规范，支撑各级系统对接、跨平台数据交互。

7.4.1 系统统一提供 RESTful 风格标准化 API 接口，数据交换优先采用 JSON 格式，兼容 XML 格式，适配各类业务系统对接需求；

7.4.2 数据上链接口必须包含 data_hash（SM3 哈希值）、timestamp（ISO 8601 标准时间）、org_id（机构唯一标识）、device_id（设备唯一编号）、signature（机构数字签名）五大必填参数，缺一不可；

7.4.3 系统接口响应效率满足国家级监管业务需求，单次数据上链请求响应时长不超过 5 秒，单次溯源核验请求响应时长不超过 3 秒。

8 数据格式与上链要求

为构建全国统一的生态环境监测数据区块链存证标准，规范数据格式、上链范围、确权规则与隐私保护机制，实现全国数据统一存证、互通互认、合规采信。

8.1 上链数据分类

8.1.1 强制上链数据：为保障监测数据全流程可追溯、可核验，以下核心数据必须 100%上链存证：监测原始数据 SM3 哈希值、监测报告哈希值及全套元数据、监测设备校准记录时间戳与哈希值、数据修改操作记录及审批留存信息。

8.1.2 宜上链数据：监测系统运维操作日志哈希值宜常态化上链存证，实现运维行为全程监管。

8.1.3 非上链数据：原始监测数据本体、现场影像资料、超大体积附件等大容量文件，不直接上链存储，统一存储于合规可信存储系统，仅将唯一哈希指纹上链，平衡存证公信力与系统运行效能。

8.2 数据元结构

全国统一生态环境监测数据上链元数据结构，所有上链存证记录必须包含标准化字段，确保数据规范性、统一性、可比对性。

8.2.1 全国统一生态环境监测数据上链元数据结构，每条上链存证记录需包含以下标准化字段，所有字段规范、格式、必填要求如下：

1. record_id：字符型（String），长度 64 字符，为必填项，是存证记录唯一标识（UUID v4），实现全国记录唯一识别；

2. data_hash：字符型（String），长度 64 字符，为必填项，为 SM3 算法生成的十六进制哈希值，是监测数据唯一数字指纹；

3. data_type：字符型（String），长度 32 字符，为必填项，用于标注数据类型，包含原始值、监测报告、运维日志等类别；

4. monitoring_type：字符型（String），长度 16 字符，为必填项，用于区分监测类别，涵盖水质、大气、土壤、噪声等生态环境监测类型；

5. org_id：字符型（String），长度 32 字符，为必填项，填写数据生产方统一社会信用代码，作为机构唯一确权标识；

6. device_id：字符型（String），长度 64 字符，为必填项，为监测设备唯一编码，实现监测设备源头溯源；

7. monitoring_time：时间格式（DateTime），遵循 ISO 8601 标准，为必填项，记录监测任务起始时间；

8. submission_time：时间格式（DateTime），遵循 ISO 8601 标准，为必填项，记录数据区块链上链提交时间；

9. geo_location：字符型（String），长度 64 字符，为选填项，记录监测点 GCJ-02 标准经纬度坐标，实现监测点位精准定位；

10. batch_no：字符型（String），长度 32 字符，为选填项，填写样品批号或监测任务编号，用于样品与任务溯源；

11. operator：字符型（String），长度 32 字符，为必填项，填写操作人员唯一标识，落实岗位责任到人；

12. signature：字符型（String），长度 128 字符，为必填项，为数据生产机构 SM2 算法数字签名，实现数据合法确权、防抵赖。

8.2.1 所有数值型监测指标必须标注法定计量单位，常规数据精度统一保留小数点后 2 位，特殊行业指标严格遵循对应国家监测标准精度要求。

8.3 数据确权与签名

8.3.1 所有数据生产主体必须申领国家权威 CA 机构颁发的合法数字证书，作为数据确权、签名、验签的唯一法定凭证，纳入全国统一 PKI 信任体系。

8.3.2 数据上链前必须通过主体私钥完成加密签名，签名对象包含数据哈希值、标准时间戳、机构唯一标识，验签不合格、信息不完整的数据严禁上链，从源头杜绝虚假数据、违规数据存证。

8.4 数据隐私保护

立足国家数据安全、个人信息保护、商业秘密保护相关法律法规要求，构建分级分类的监测数据隐私保护机制。

8.4.1 涉及企业商业机密、敏感监测点位、涉密区域的监测数据，必须完成合规脱敏处理，或采用

零知识证明等隐私计算技术实现数据选择性披露，兼顾数据可信核验与隐私安全。

8.4.2 严格落实数据授权访问制度，无主体合法授权、无监管部门法定调阅指令的任何机构及个人，不得违规访问、调取、使用原始监测数据，筑牢生态环境数据安全防线。

9 采集与存储规范

严格落实国家生态环境监测质量管理、数据安全存储相关规范，建立源头可控、传输安全、存储合规、备份完备的数据采集存储体系，保障监测数据全流程安全可信。

9.1 数据采集要求

9.1.1 各类自动监测设备必须标配国产化加密、数字签名模块，实现数据生成即加密、生成即确权，从设备源头杜绝数据篡改、伪造风险。

9.1.2 人工采样监测数据必须在采样完成后 24 小时内完成标准化录入、审核、上链存证，全程记录操作人员、操作时间、修改轨迹、审核信息，实现人工数据全程可追溯。

9.1.3 高频次连续监测数据可采用批量哈希打包上链模式，以 1 小时为最小单位聚合生成数据块哈希值上链存证，在保障数据真实性的前提下，降低链上存储压力，提升系统运行效率。

9.1.4 所有监测采集终端设备安全等级不低于 GB/T 22239-2019 第二级要求，满足国家网络安全防护标准。

9.2 数据传输规范

9.2.1 监测数据传输全程采用加密通道，启用 TLS 1.2 及以上安全协议，严禁敏感监测数据明文传输，防范传输链路窃取、篡改、劫持风险。

9.2.2 所有传输数据附加端到端校验码，实现传输完整性校验，确保数据传输无损坏、无篡改、无丢失。

9.2.3 针对断网、链路故障等异常场景，终端支持本地合规缓存数据，最大缓存时长不超过 72 小时，网络恢复后自动补传上链并标记延迟上链状态，保障监测数据连续性、完整性。

9.3 存储管理

建立“链上存证、链下存数、双向映射、永久可查”的国家级存储管理体系。

9.3.1 链上仅存储轻量化哈希指纹与标准化元数据，单条存证记录容量不超过 2KB，保障区块链账本高效运行；原始数据本体统一存储于国家合规数据库或分布式可信存储系统。

9.3.2 原始监测数据存储留存周期不少于 6 年，符合生态环境档案管理、执法取证、溯源追责的法

定留存要求；链上存证记录永久固化保存，实现终身可核验、可追溯。

9.3.3 存储系统必须具备异地多活容灾备份能力，恢复点目标（RPO）不超过 30 分钟，恢复时间目标（RTO）不超过 4 小时，保障国家级数据安全与业务连续性。

9.3.4 数据访问、修改、调取日志留存时长不少于 180 天，日志文件同步生成哈希值备查，实现存储操作全程监管。

10 溯源核验流程

统一全国生态环境监测数据溯源核验标准流程，构建标准化、法治化、智能化的核验体系，保障核验结果权威有效、可司法采信。

10.1 溯源信息查询

10.1.1 标准化溯源查询结果必须包含五项核心内容：数据哈希与链上存证比对结果、数据上链时间戳及对应区块高度、数据生产主体资质及数字证书有效状态、数据全生命周期操作追溯记录、历次合规核验查询日志记录。

10.1.2 溯源查询响应时长不超过 3 秒，满足监管快速核查、应急取证、批量核验的业务需求。

10.2 完整性核验方法

10.2.1 全国统一采用 SM3 哈希比对核验法，对待核验数据实时计算哈希值，与链上固化的原始哈希指纹精准比对，一致则判定数据完整、未被篡改，不一致则判定数据存在篡改、失效作废，核验结论具备唯一权威性。

10.2.2 所有核验操作自动生成带权威时间戳的标准化核验报告，支持 PDF、JSON 两种标准格式输出，核验报告哈希值可按需上链存证，固化核验结果，提升司法采信效力。

10.3 跨链溯源

适配全国多平台、多区域区块链系统数据互通互认需求，建立标准化跨链溯源机制。

10.3.1 跨系统、跨区域数据互认场景下，需部署合规跨链桥接或侧链协议，实现不同区块链账本数据可信互通。

10.3.2 跨链数据核验必须附带原始区块链存证证明及共识节点联合签名，杜绝跨链数据伪造、篡改，保障全国范围内数据互认统一、权威有效。

11 性能与安全要求

立足全国规模化推广、高并发应用、高安全防护的国家级建设需求，明确系统核心性能指标与安全防护标准，保障系统稳定、安全、高效、合规运行。

11.1 系统性能指标

系统核心性能需满足全国多级监管、多主体并发应用需求，具体指标如下：

系统核心性能需满足全国多级监管、多主体并发应用需求，具体指标如下：

11.1.1 系统核心性能指标需满足全国多级监管、多主体高并发应用需求，各项指标技术要求如下：

1. 链上交易吞吐量：不低于 500 TPS，保障批量监测数据高效上链存证；

2. 交易确认时延：不大于 3 秒，满足监管快速存证、实时核验的业务需求；

3. 查询响应时间：不大于 3 秒，适配大规模溯源查询、批量数据核验场景；

4. 系统可用性：不低于 99.9%，保障系统全年稳定连续运行；

5. 节点同步时延：不大于 2 秒，确保全网节点账本数据实时一致；

6. 支持节点数量：不少于 15 个，满足全国多主体、跨区域节点组网共治需求。

11.2 安全保护等级

系统整体安全防护严格落实国家网络安全等级保护制度，区块链网络及配套应用系统全面达到 GB/T 22239-2019 第三级安全保护等级要求，覆盖全维度安全防护：

a) 身份鉴别：启用双因素认证机制，严格落实密码复杂度、有效期、防破解管理规范；

b) 访问控制：基于角色分级授权，严格执行最小权限原则，杜绝越权操作；

c) 安全审计：全程记录所有系统操作、链上行为、数据访问日志，日志留存不少于 180 天；

d) 数据完整性：依托区块链技术实现链上数据永久防篡改、防删除；

e) 数据保密性：敏感监测数据全程加密传输、加密存储；

f) 入侵防范：部署防火墙、网络入侵检测系统（IDS），常态化抵御网络攻击、恶意入侵风险。

11.3 容灾与备份

构建国家级高可用容灾备份体系，保障系统持续稳定运行、数据绝对安全。

11.3.1 区块链节点采用多区域分布式部署模式，部署物理区域/可用区数量不少于 3 个，单一区域故障不影响全网共识与业务运行；

11.3.2 区块链账本数据执行每日全量备份机制，备份数据留存时长不少于 30 天；

11.3.3 制定标准化容灾应急预案，每 6 个月至少开展一次全流程容灾切换演练，提升突发故障应急处置能力。

12 运维管理要求

建立规范化、制度化、常态化、可审计的运维管理体系，适配全国统一监管、长效运行的国家级应用需求，保障溯源体系持续合规、高效运行。

12.1 节点管理

12.1.1 区块链节点新增、退出、变更必须经不少于 2/3 的现有合规节点投票审议通过，全程公示、全程留痕，杜绝节点随意变更影响网络稳定性；

12.1.2 各节点运营方定期上报节点运行状态，涵盖节点在线率、区块同步时延、共识参与有效性、异常故障情况等核心指标，接受监管部门常态化督查；

12.1.3 节点核心私钥采用硬件安全模块防护，私钥备份实行多人拆分保管、分级管控，杜绝私钥泄露、丢失、滥用风险。

12.2 数据质量审计

建立国家级常态化数据质量审计机制，强化监测数据全生命周期质量管控。

12.2.1 各级生态环境监管部门每季度开展链上存证数据随机抽样审计，抽样比例不低于当期存证数据总量的 5%；

12.2.2 审计核心内容包含数据哈希一致性、数字签名有效性、元数据规范性、上链流程合规性，全面排查数据造假、违规操作风险；

12.2.3 审计工作完成后 15 个工作日内，审计报告必须标准化上链存证，固化审计结果，实现审计工作可追溯、可督查。

12.3 系统更新与维护

建立安全可控、兼容迭代的系统更新维护机制，保障全国系统统一迭代、平稳升级。

12.3.1 智能合约升级、共识算法调整、核心架构变更等重大系统迭代，须经不少于 5 家核心节点运营方多签确认，变更方案公示 7 天无异议后方可实施；

12.3.2 系统版本迭代必须全面兼容历史数据格式，保障历年监测存证数据可正常核验、有效追溯；

12.3.3 系统安全漏洞补丁发布后 7 天内完成全覆盖部署，常态化筑牢系统安全防线。

12.4 人员管理

构建规范化、专业化、高保密的运维人员管理体系，落实岗位责任与安全管控。

12.4.1 系统核心运维、管理人员必须通过严格背景审查，签订终身保密协议，明确数据安全与运

维责任；

12.4.2 私钥管理、合约部署、批量数据操作等核心关键操作，必须执行双人复核、双人监督机制，全程留存操作日志与影像记录；

12.4.3 每年至少组织一次全员安全培训、合规考核与技能测评，提升运维团队专业化、规范化、合规化作业能力。