

ICS 03. 120. 10

A 00

R B

中华人民共和国认证认可行业标准

RB/T XXXXX—XXXX

质量管理体系区块链存证指南

Guidance on the blockchain platform authentication of OMS

(征求意见稿 9)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国国家标准认证认可监督管理委员会 发布

目 次

前 言	II
1 范围	3
2 规范性引用文件	3
3 术语和定义	3
4 工作原理	4
4.1 信息存证原理	4
4.2 信息验真原理	4
4.3 信息保护原理	4
5 主要相关方及其职责	4
5.1 认证机构	4
5.2 区块链存证平台	4
5.3 质量管理体系认证证书的使用者和查询者	5
6 信息存证	5
6.1 信息存证工具	5
6.2 信息存证流程	5+
7 信息验真	6
7.1 信息验真方法	6
7.2 信息验真工具	6
7.3 信息验真流程	6
8 信息查询	6
8.1 区块链存证平台可查询的信息	6
8.2 查询方式	6
8.3 查询工具	6
8.4 查询流程	6
附录 A（资料性附录）质量管理体系认证关键信息	8
参考文献	9

前 言

本文件按照GB/T 1.1—2020《标准化工作规则 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。

本文件由中国国家认证认可监督管理委员会提出并归口。

本文件起草单位：国家市场监督管理总局认证认可技术研究中心 北京井通数字科技有限公司...

本文件主要起草人：XXX XXX XXX XXX XXX XXX XXX XXX XXX

质量管理体系区块链存证指南

1 范围

本文件提供了利用区块链平台，对质量管理体系认证活动关键信息进行存证、验真和查询的指南。
本文件适用于：

- a) 为计划使用区块链存证系统的认证机构提供参考；
- b) 指导认证机构和区块链机构建立、实施、保护和改进区块链存证体系；
- c) 为使用区块链存证功能的相关应用提供参考。

2 规范性引用文件

下列文件的部分或全部内容构成本文件的要求。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 19000 质量管理体系 基础和术语

GB/T 19001 质量管理体系 要求

GB/T 19011 管理体系审核指南

GB/T 37043 智慧城市 术语

GM/T 0004 SM3密码杂凑算法

GA/T976 电子数据法庭科学鉴定通用方法

T / CESA 1048 区块链存证应用指南

YD/T 3747区块链技术架构安全要求

3 术语和定义

GB/T19000界定的以及下列术语和定义适用于本文件：

3.1

哈希值 Hash data

使用安全的哈希算法对数据进行计算获得的数据。

（来源：GA/T976-2012， 3.5）

3.2

区块链 Blockchain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

（来源：GB/T 37043-2018.2.5.8； YD/T 3747-2020, 3.1.1）

3.3

区块链存证 blockchain authentication

为了保证存证信息（电子数据）的完整性和真实性，采用区块链技术实现多节点共识的存证服务。

（来源：T/CESA1048-2018， 3.1.4）

4 工作原理

4.1 信息存证原理

可通过区块链平台将质量管理体系认证活动关键信息的哈希值进行存证，而非存储质量管理体系认证活动关键信息的原始数据。如需存证原始信息，必须事先得到认证机构的授权。

4.2 信息验真原理

利用哈希值是单向函数的性质，通过对比哈希值是否一致确认被验真数据和原始数据的一致性。信息的哈希值上传到区块链系统之后不可篡改，无法通过逆运算还原出原始数据，但相同的原始数据会运算出相同的哈希值。

4.3 信息保护原理

通过存证的哈希值无法逆运算得到质量管理体系认证活动关键信息的原始数据，不会造成原始信息的泄露。

5 主要相关方及其职责

5.1 认证机构

- a) 从事质量管理体系认证的机构可上链存证相关信息；
- b) 培训、指导和监督质量管理体系认证的项目管理人员、审核组成员、合格评定人员等相关人员上链存证信息；
- c) 宜确保上链信息哈希值与质量管理体系认证活动实际信息一致。

5.2 区块链存证平台

5.2.1 具备存证数据完整性、机密性的技术机制，如运用哈希校验、电子签名、密码加密等技术手段防止存证数据被篡改，确保存证数据在存储、传输过程中的安全，密码强度不宜低于 256 位等。

5.2.2 具备高可用性（99.99%以上），通过同城双活、异地容灾等机制保障业务连续性，可防御大流量 DDoS 等攻击，并具备完善的应急预案，定期演练。

5.2.3 设计、运营和维护平台，主要包括：

- 提供基于 BFT 共识机制的联盟链系统。
- 提供文件 HASH 摘要工具，用于对上链文件进行 HASH 摘要，生成文件的唯一数字指纹。
- 提供支持国密算法的签名系统，用于对文件进行确权签名和验签。
- 提供区块链浏览器，用于查询文件记录。
- 提供上链操作手册。

5.2.4 适宜时，对上链信息的完整性和时效性进行审定。

5.2.4.1 时效性宜考虑：

- b) 上链时间宜由认证机构与区块链平台提前约定；
- c) 电子数据时间戳或区块链系统记录时间可被核验；
- d) 避免电子数据中证明性时间的本地化采集。

5.2.5 存证平台节点与其他节点的通信通道宜做加密处理。

5.2.6 存证平台节点提供的对外服务接口宜做加密处理。

5.3 质量管理体系认证证书的使用者

可在质量管理体系区块链存证平台上查询其认证活动关键信息的哈希值或可公开信息，进行验真。

6 信息存证

6.1 信息存证工具

存证工具包括信息批量存证软件、信息审核管理平台和区块链系统等信息存证过程中适用的相关软件和系统。

6.2 信息存证流程

6.2.1 认证机构和区块链存证平台可根据需要，约定上链存证的信息及其上链形式，同一认证活动的信息可根据实际情况多次上链。

6.2.2 认证机构将待存证信息放入指定文件夹，通过信息批量存证软件对信息运算生成哈希值并匹配对应的明文索引，形成待存证信息清单。

6.2.3 区块链存证平台通过信息审核管理平台对信息存证清单的完整性和时效性进行审核，审核通过后，信息自动上传到区块链系统中，完成存证。

6.2.4 存证流程中宜

- a) 确保电子数据生成、收集、存储、传输所依赖的计算机系统的硬件、软件环境安全、可靠；

b) 明确电子数据存储、介质保管的方式和手段。

7 信息验真

7.1 信息验真方法

通过对比哈希值，确认被验真数据和原始数据的一致行进行验真。

7.2 信息验真工具

验真工具包括浏览器插件、区块链浏览器和区块链存证系统等信息验真过程中适用的相关软件和系统。

7.3 信息验真流程

7.3.1 运算

通过浏览器插件将被验真文件在本地运算出该文件的哈希值。

7.3.2 查询

复制该文件的哈希值，输入到存证平台区块链浏览器进行查询。

7.3.3 比对

将查询到的存证平台区块链浏览器的数据和验真文件的哈希值，明文索引进行比对？。

8 信息查询

8.1 区块链存证平台可查询的信息

区块链存证平台可查询的信息包括但不限于明文索引和哈希值。

8.1.1 明文索引

证书名称、认证类型、发证时间、证书编号、证书有效期、获证机构等。

8.1.2 哈希值

质量管理体系认证活动关键信息经运算得出的哈希值和证书或报告经运算得出的哈希值。

8.2 查询方式

信息查询可通过上链的用户地址查询，也可通过证书名称模糊查询。

8.3 查询工具

信息查询过程中适用的区块链浏览器。

8.4 查询流程

在区块链浏览器中输入明文索引？ 进行查询。

附 录 A
(资料性)
质量管理体系认证关键信息

质量管理体系认证活动中的关键信息可上链存证其哈希值，可公开的明文信息或图片，如编号，名称等，也可上链存储。下面是关键活动的示例：

A.1 认证策划

- a) 认证申请书；
- b) 认证申请评审表；
- c) 认证合同；
- d) 被审核企业内审计划、内审报告、管理评审计划和管理评审报告、合格供方评价表等。？

A.2 认证审核

- a) 审核任务书；
- b) 审核计划；
- c) 二阶段首次会议签到表和/或照片和/或视频；
- d) 二阶段现场巡视、关键设备或重要过程的照片或视频；
- e) 二阶段末次会议签到表和/或照片和/或视频；
- f) 二阶段审核材料。

A.3 认证决定

合格评定表。

A.4 认证结果

认证证书。

参考文献

- [1] 《中国区块链技术和应用发展白皮书（2016）》
- [2] 《关于加快推动区块链技术应用和产业发展的指导意见》工信部联信发（2021）62 号
- [3] CBD-Forum-001-2017 区块链 参考架架构