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 authentication of QMS

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国国家认证认可监督管理委员会　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：

本文件主要起草人：

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技术，对质量管理体系认证活动的信息进行存储、验证和查询的指南。

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指导；

b）指导认证机构和区块链存证系统相关方使用区块链技术建立、实施、维持和改进存证系统；

c）为使用区块链存证系统验证和查询质量管理体系认证活动信息的使用方提供参考。

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 27021 管理体系认证机构要求

GB/T 37043 智慧城市 术语

GA/T976 电子数据法庭科学鉴定通用方法

GM/T 0004 SM3密码杂凑算法

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]

3.3

区块链存证 blockchain authentication

为了保证存证信息的完整性和真实性，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， 有修改]

4 工作原理

4.1 信息存储原理

利用区块链技术防篡改、可追溯的特点，区块链存证系统可存储质量管理体系认证活动信息的哈希值，也可存储质量管理体系认证活动的明文信息。

4.2 信息验证原理

利用哈希算法单向性和抗碰撞性的特点，通过对比哈希值是否一致确认被验证数据和原始数据的一致性。明文信息通过比对进行验证。

4.3 信息保护原理

利用存证的哈希值无法逆运算的特点，无法得到质量管理体系认证活动信息的原始数据，且认证活动信息的哈希值上传到区块链存证系统之后不可篡改，不会造成原始数据的泄露。

5 主要相关方及其职责

5.1 认证机构

认证机构宜承担以下职责：

a) 存证质量管理体系认证活动的信息；

b) 培训、指导和监督相关人员存证信息；

c) 确保存证的信息与质量管理体系认证活动的原始数据一致。

5.2 区块链存证系统相关方

5.2.1 具备存证数据完整性、机密性的技术机制，如运用电子签名 、可信时间戳、哈希值校验等技术手段防止存证数据被篡改。

5.2.2 符合相关法律法规要求，确保区块链存证系统的安全。

5.2.3 适宜时，对存证信息的完整性和时效性进行审定，完整性和时效性宜：

a)满足认证机构的要求；

b)满足使用方查询和验证的要求。

5.3 使用方

在质量管理体系区块链存证系统上进行验证和查询。

6 信息存证

6.1 存证的信息

存证的信息可包括质量管理体系认证活动的所有信息，其中关键活动的信息见附录 A。

6.2 信息存证工具

存证工具包括存证过程中适用的相关软件和系统，如界面化的存证工具、接口调用、 信息批量存证软件、信息审核管理平台等。

6.3 信息存证流程

6.3.1 认证机构可根据需要，确定存证的信息及其存证形式，见附录B。同一认证活动的信息可根据实际情况多次存证。

6.3.2 认证机构将待存证信息，通过信息存证工具对信息进行运算并处理，形成待存证信息清单。

6.3.3 认证机构和区块链存证系统相关方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。

6.3.4 存证流程中宜：

a）确保待存证信息生成、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）确保存储的方式和手段符合认证机构的要求。

7 信息验证

7.1 验证的信息

存证的信息可被验证。

7.2 信息验证工具

验证工具包括适用的相关软件和系统， 如界面化的验证工具、接口调用、 信息批量验证软件、信息审核管理平台等。

7.3 信息验证流程

7.3.1 哈希值的验证

通过验证工具运算出被验证信息的哈希值，与系统存证的哈希值进行比对。

7.3.2 明文信息的验证

检索已存证的明文信息，与被验证的明文信息进行比对。

8 信息查询

8.1 查询的信息

区块链存证系统可查询的信息包括存证的明文信息和存证的哈希值。

8.2 查询工具

信息查询过程中适用的相关软件和系统， 如界面化的查询工具、接口调用、 信息批量查询软件、信息审核管理平台等。

8.3 查询流程

可通过存证信息的索引进行查询。

附 录 A
（资料性）
质量管理体系认证关键活动的信息示例

认证机构可以自行确定其存证的信息。可存证质量管理体系认证活动的所有信息，也可只存证关键活动的信息，可存证其哈希值、可公开的明文信息或图片，如编号，名称等。本附录给出了关键活动的信息示例。

A.1 文件化信息的示例

A.1.1 申请评审信息：

a) 认证合同；
b) 申请阶段申请组织提交的资料；
c) 认证机构对申请组织的认证申请进行评审的证据；
d) 双方就审核中应用信息通信技术（ICT）遵守信息安全与数据保护的措施达成一致意见的证据（适用时）；
e) 对申请组织的审核过程适用信息通信技术的评审证据（适用时）；
f) 认证机构对申请组织审核过程适用信息通信技术进行评审的证据（适用时）。

A.1.2 审核策划信息：

a) 对每次审核和周期内审核进行审核方案策划的证据；
b) 对审核过程适用信息通信技术的策划证据（适用时）。

A.1.3 审核实施信息：

a) 审核计划（适用时）；
b) 对审核过程明确采用信息通信技术的范围的证据（适用时）；
c) 审核首次会的签到证据；
d) 审核末次会的签到证据；
e) 审核过程采用信息通信技术的证据（适用时）；
f) 审核报告。

A.1.4 监督/再认证/特殊审核的策划信息：

a) 基于组织当前现状进行方案策划的证据；
b) 对组织申请的变更进行针对性策划的证据（适用时）。

A.1.5 认证决定信息（包括授予/暂停/撤销/变更认证的决定）：

a) 实施认证决定的证据；
b) 对采用信息通信技术的审核确定后续跟踪验证的证据（适用时）。

A.1.6 认证证书信息

A.2 关键活动的信息结构化数据的示例

A.2.1．初次认证的信息：

--社会统一信用代码号；
--生产经营场所地址，多场所地址；
--员工人数；
--组织体系负责人；
--活动分包信息；
--认证覆盖的产品或服务主要标准；
--质量管理体系运行时间；
--审查确认时间；

--审查确认人员；
--完成审核所需时间；
--影响认证活动的因素；
--合同签订时间；
--合同编码；
--组织名称变更；
--生产经营地址变更；
--认证范围变更、关键工艺设备和产品范围变更；
--管理体系负责人变更；
--重大负面信息（包括质量事故、行政处罚、重大投诉、负面舆情）；
--审核时间和现场审核时间；
--审核组信息（包括姓名、注册资格、专业），包括技术专家（专业、职称、单位）和实习审核员（姓名、注册资格）；
--审核过程重要节点时间：（包括首次会议时间、末次会议时间，初次审核包括第一阶段审核时间和地点）；
--场所抽样信息（包括抽样的场所、审核时间）；
--终止审核理由（适用时）；
--审核报告提交时间；
--终止审核项目报告提交时间（适用时）；
--不符合纠正和纠正措施及其结果有效性验证时间（适用时）；
--认证决定时间；
--认证决定人员；
--认证结论；
--证书编号；
--认证依据；
--证书起止时间；
--认证证书的认证业务范围；
--多场所名称和地址信息；
--认可标识；
--认证机构名称。

A.2.2.监督审核的信息：

--监督审核时间；
--监督审核人日数；
--监督审核的审核组；
--监督审核结论。

A.2.3.再认证的信息：

--再认证现场审核时间；
--再认证人日数；
--再认证审核组；
--不符合项实施纠正和纠正措施并通过验证的时间；
--证书编号；
--认证依据；
--换发认证证书起止时间；

--认证证书的认证业务范围；
--多场所名称和地址信息；
--认可标识；
--认证机构名称。

A.2.4. **证书变更的信息：**

--证书暂停起止时间；
--证书暂停原因；
--证书恢复时间；
--证书撤销时间；
--证书撤销原因；
--证书信息变革信息。

附 录 B
（资料性）
存证信息分类和确定存证形式的方法示例

认证机构可以进行评估，确定通过区块链存证系统存证的信息及存证形式。本附录给出了信息分类的原则及存证形式的示例。

B.1. 原始数据区块链存证分类原则

认证机构宜确定原始数据是否使用区块链存证并公开，原始数据的分类基于以下原则：

--可执行性：避免数据分类规则过于复杂，确保数据分类工作的可行性。

--自主性：结合认证机构自身管理需要，如战略需要、业务需要、对认证活动相关方的承诺、风险接受程度等，在本标准的框架下自主确定区块链存证的原始数据。

B.2. 存证信息分类

认证机构可考虑如下因素，对拟存证信息的原始数据进行分类。

B.2.1 分类要素

B.2.1.1 影响对象

影响对象指认证机构使用区块链存证原始数据并公开后受到影响的对象，包括机构权益、客户权益和个人权益等。

B.2.1.2 影响程度

影响程度是指认证机构使用区块链存证原始数据并公开后，可能造成的影响程度。影响程度从高到低可分为有危害、无危害两类。

注：对不同影响对象进行影响程度判断时，采取的基准不同。如影响对象是组织或个人权益，则以该组织或本人的总体利益作为判断影响程度的基准。

B.2.2 原始数据分类结果

原始数据根据其影响对象和影响程度，划分为使用明文信息存证和使用哈希值存证两类：

B.2.2.1 以下原始数据宜使用明文信息存证：

a） 法律法规要求认证机构必须公开的原始数据；

b） 行业内默认应公开，或已经普遍公开的原始数据；

c） 认证机构认为对影响对象造成影响程度为无危害的原始数据。

B.2.2.2 不满足 B.2.2.1 要求的原始数据，宜使用哈希值存证。

B.3 原始数据分类后存证

使用明文信息存证的原始数据，存证明文信息；使用哈希值存证的原始数据，存证哈希值。表 B.1 为存证形式示例。

认证阶段	关键活动的信息	分类
认证策划	认证申请书	哈希值存证
	认证申请评审表	哈希值存证
	认证合同	哈希值存证
	认证客户内审计划	哈希值存证
	认证客户内审报告	哈希值存证
	认证客户管理评审计划	哈希值存证
	认证客户管理评审报告	哈希值存证
	认证客户合格供方评价表	哈希值存证
认证审核	审核任务书	明文信息存证
	审核计划	哈希值存证

	二阶段首次会议签到表和/或照片和/或视频	哈希值存证
	二阶段现场巡视、关键设备或重要过程的照片或视频	哈希值存证
	二阶段末次会议签到表和/或照片和/或视频	哈希值存证
	二阶段审核材料	哈希值存证
认证决定	合格评定表	哈希值存证
认证结果	认证证书	明文信息存证

参 考 文 献

[1] GB/T 25069《信息安全技术 术语》

[2] GB/T20271《信息安全技术 信息系统通用安全技术要求》

[3] GB/T25058《信息安全技术 信息系统安全等级保护实施指南》

[4] GB/T20270《信息安全技术 网络基础安全技术要求》

[5] GB/T20272《信息安全技术 操作系统安全技术要求》

[6] GB/T20273《信息安全技术 数据库管理系统安全技术要求》

[7] GB/T21028 《信息安全技术 服务器安全技术要求》

[8] GB/T20269《信息安全技术 信息系统安全管理要求》

[9] GB/T20282 《信息安全技术 信息系统安全工程管理要求》

[10]GB/T22239《信息安全技术 信息系统安全等级保护基本要求》

[11]BICB-001-2019 北京互联网法院天平链应用接入管理规范

[12]BICB-002-2019 北京互联网法院天平链应用接入技术规范

[13]GA/T671《信息安全技术 终端计算机系统安全等级技术要求》

[14]CBD-Forum-001-2017 区块链 参考架架构

[15]《中国区块链技术和应用发展白皮书（2016）》工信部发

[16]《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

[17]《质量管理体系认证规则》认监委发〔2016〕20 号

[18]《最高人民法院关于民事诉讼证据的若干规定》法释〔2019〕19 号

[19]《最高人民法院关于互联网法院审理案件若干问题的规定》法释〔2018〕16 号