ICS 35.240
CCS L 70

中华人民共和国国家标准

GB/T 43580—2023

区块链和分布式记账技术 存证通用服务指南

Blockchain and distributed ledger technology—General service guidelines for preserve evidence

2023-12-28 发布　　2024-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国区块链和分布式记账技术标准化技术委员会(SAC/TC 590)归口。

本文件起草单位：厦门安妮股份有限公司、上海万向区块链股份公司、北京版全家科技发展有限公司、中国电子技术标准化研究院、深圳市前海智慧版权创新发展研究院、深圳前海微众银行股份有限公司、华为技术有限公司、深圳市腾讯计算机系统有限公司、蚂蚁科技集团股份有限公司、杭州趣链科技有限公司、国网数字科技控股有限公司、众安信息技术服务有限公司、工业和信息化部电子第五研究所、国家工业信息安全发展研究中心、北京大学、复旦大学、中国科学院国家授时中心、湖南天河国云科技有限公司、四川长虹电器股份有限公司、国家应用软件产品质量检验检测中心、江苏恒为信息科技有限公司、北京大数据先进技术研究院、蚂蚁区块链科技(上海)有限公司、华为云计算技术有限公司、腾讯云计算(北京)有限责任公司、北京微芯区块链与边缘计算研究院、上海零数众合信息科技有限公司、南京鑫智链科技信息有限公司、广州南方投资集团有限公司、永旗控股(北京)有限公司、上海阵方科技有限公司、联通数字科技有限公司、上海树图区块链研究院、中国民航信息网络股份有限公司、上海奥若拉信息科技集团有限公司、上海分布信息科技有限公司、达阔机器人股份有限公司、浙商银行股份有限公司、中国物流与采购联合会区块链应用分会、昆仑数智科技有限责任公司、北京安妮全版权科技发展有限公司、香港理工大学、中央财经大学、华东师范大学、深圳市版权协会、中国科学院深圳先进技术研究院、西南林业大学、敏于行(北京)科技有限公司、数智枫桥(北京)信息技术研究院有限公司、北京文化产权交易中心有限公司、深圳博思互联科技有限公司、广东大音音像出版社、北京信任度科技有限公司、江西开创数码科技有限公司、恒宝股份有限公司、道赞有限公司、深圳市明源云链互联网科技有限公司。

本文件主要起草人：郝汉、李鸣、胡怀勇、周平、杜宇、张杰、李斌、张小军、李克鹏、彭晋、李伟、王栋、宋文鹏、于秀明、相里朋、李卫、陈钟、华宇、杨征、李努锲、王威、张何东、刘天成、张晓蒙、郭凯、王乐庆、董进、兰春嘉、陶立春、阚海斌、王保春、劳卫伦、龚自洪、谢云龙、晏海水、谢辉、杨国正、笪鸿飞、潘海洪、杨胜、郝佳诺、朱建明、陈彦、曲强、梁志宏、欧昀、廖鸿程、隆旭光、杨俊、马臣云、钱京、王荆楠、张凯文、季静婷、林森、王晨辉、康信伟、孙琳、彭涛、于明亮、王子博、高玉翔、陈晓丰、曹建农、金澈清、李达、包小敏、刘齐军、黄德俊、张雁、刘冕宸、周子茗、翟耀超、崔春生、杜娟、杨珍、王泽昊、孙林、臧铖、郝玉琨、华崇鑫、肇雨濛、耿学玉、崔可、杨文锋、龙晶、靳芯、王立军。

引　言

近年来，在政策、法律、技术、市场等多方面推动下，区块链技术加速“脱虚向实”，总体发展格局初步形成。区块链标准建设对我国形成数字经济产业生态、提升行业治理和公共服务水平具有重要意义。

区块链存证是基于区块链技术实现多节点共识的电子数据存证，能够保证链上电子数据信息的完整性和真实性。基于共识机制，与中心化系统相比，区块链存证采用多方证明的方式，电子数据存证信息一旦上链则不可篡改，从而更加真实可信。基于跨链技术，区块链存证能进一步确保电子数据信息的可信共享，提升业务协同效率。

随着区块链技术尤其是联盟链技术的发展，区块链存证已被广泛应用于包括司法取证、版权确权、商品溯源、供应链金融、电子政务、电子商务等在内的各个领域。由于缺乏统一的标准，区块链存证应用存在信息上链过程不规范、服务质量参差不齐等问题，导致所存证电子数据的有效性尚未得到普遍性认可，亟需统一标准以规范区块链存证应用体系建设。

本文件为各行业使用区块链存证技术提供了通用服务指南，可以规范基于区块链技术的电子数据存证过程，用于指导组织或机构建立、实施和改进区块链存证应用体系，并推动行业健康有序发展。

区块链和分布式记账技术 存证通用服务指南

1 范围

本文件确立了区块链存证应用服务模型，包括相关方、有效性原则、存证过程、数据指南、服务指南和安全指南等，提供了基于区块链技术的存证通用服务指南。

本文件适用于：

a） 规范基于区块链技术的电子数据存证过程；

b） 指导组织或机构建立、实施和改进区块链存证应用体系；

c） 为计划建设区块链存证应用系统的组织或机构提供参考。

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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 32399—2015 信息技术 云计算 参考架构

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 43572—2023 区块链和分布式记账技术 术语

3 术语和定义

GB/T 25069—2022、GB/T 32399—2015、GB/T 43572—2023 界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

使用密码链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 43572—2023，3.6]

3.2

电子数据 electronic data

以电子手段生成、发送、接收或者储存的信息。

3.3

存证 preserve evidence

通过技术手段对电子数据进行保存和验证的行为，保证其完整性和真实性并可追溯。

3.4

区块链存证 blockchain preservation

基于区块链技术实现多节点共识的电子数据存证。

3.5

存证过程　preservation process

由电子数据生成存证内容，并存储、传输上链的过程。

3.6

共识机制　consensus mechanism

使节点间达成共识的规则和程序。

[来源：GB/T 43572—2023，3.12]

3.7

数字签名　digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。

[来源：GB/T 25069—2022，3.576]

3.8

加密　encipherment encryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 25069—2022，3.278]

3.9

智能合约　smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

[来源：GB/T 43572—2023，3.72]

3.10

存证唯一标识码　unique identifier of preserve evidence

存证信息的唯一标识符号，通常为一组字符串。

3.11

多签　multisig

多方对链上电子数据信息进行签名的行为。

3.12

二次存证　secondary preservation

基于存证唯一标识码，多条存证信息建立映射关系的行为。

3.13

存证服务提供者　digital preservation provider

提供电子数据存证服务的机构或组织。

3.14

存证服务使用者　digital preservation user

使用电子数据存证服务的组织或个人。

4　应用服务模型

区块链存证应用服务模型包含相关方、有效性原则和区块链存证关键过程。

相关方分为区块链存证业务相关方和区块链存证系统支持相关方。

有效性原则包括存证业务相关方的有效性、电子数据存取的有效性、存证时间的有效性以及存证核验的有效性。

区块链存证关键过程包括存证应用开发、电子数据预处理、电子数据签名、电子数据上链、链上存证

数据公示和查询、链上存证数据提取、链上存证数据验证。

区块链存证应用服务模型见图1。

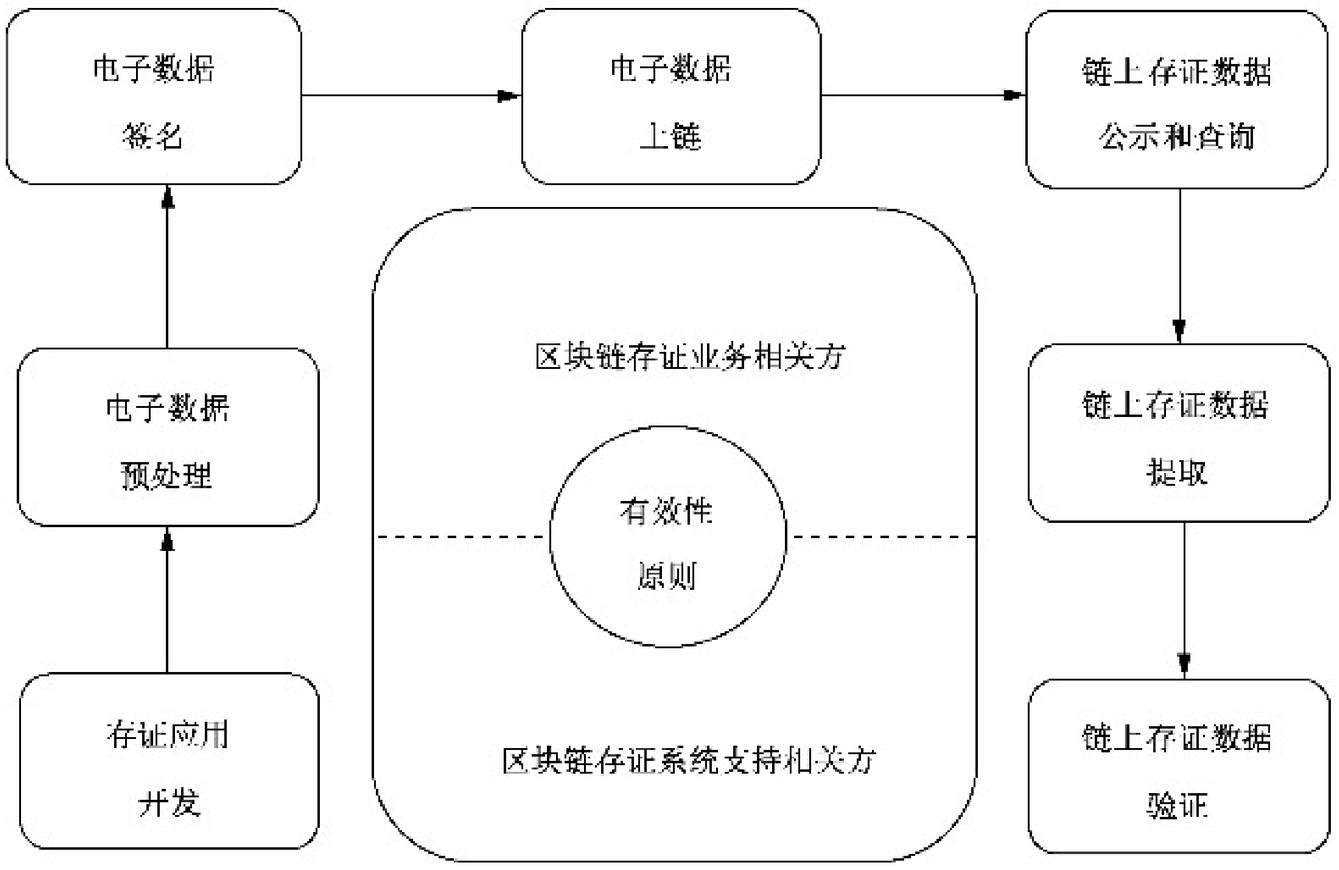

图1 区块链存证应用服务模型

5 相关方

5.1 业务相关方

5.1.1 业务内部相关方

区块链存证业务内部相关方包括：

a) 存证服务使用者；

b) 存证服务提供者；

c) 其他。

5.1.2 业务外部相关方

区块链存证业务外部相关方可作为见证节点，以对所存证的电子数据内容组成部分的有效性做出独立判断，包括：

a) 行业监管部门：根据法律规定对该行业进行监督管理的相关机构；

b) 司法机关：行使司法权的国家机关，为保证法律实施而建立的相关组织；

c) 公证处：依法独立行使公证职能、承担民事责任的证明机构；

d) 仲裁机构：通过仲裁方式解决民事争议，作出仲裁裁决的机构；

e) 司法鉴定中心：利用技术或知识为司法相关问题提供鉴定意见的机构；

f) 授时中心：承担标准时间的产生、保持与发播，提供标准时间授时服务的机构；

g) 审计机构：从事审计工作的机构；

h) 数字身份认证中心：提供数字证书的颁发、核验服务的机构；

i) 其他。

5.2 系统支持相关方

区块链存证系统支持相关方包括：

a） 区块链服务技术提供方；
b） 区块链服务治理方；
c） 区块链服务审计方；
d） 其他。

6 有效性原则

6.1 相关方的有效性

6.1.1 业务内部相关方

区块链存证业务内部相关方的有效性，宜具备以下要素：
a） 具备完善的存证业务逻辑，能够记录完整的电子数据存证信息，能够提供存证信息查询功能；
b） 具备完善的鉴权机制和身份认证功能，能够对存证服务使用者的身份真实性进行认证和校验，能够完整记录用户操作日志；
c） 采用能够确保数据完整性、机密性的技术机制，如运用哈希校验、电子签名、数据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；
d） 拥有与服务规模相适应的技术人员和专业能力，并且具有完善的管理机制。

6.1.2 业务外部相关方

区块链存证业务外部相关方的有效性，宜具备以下要素：
a） 引入中立的、具有公信力的机构节点，如行业监管部门、司法机关、公证处、仲裁机构、司法鉴定中心、授时中心、审计机构及数字身份认证中心等；
b） 保持该机构的节点存证数据与其他节点实时同步；
c） 对该机构节点与其他节点的通信通道做加密处理；
d） 为该机构节点提供的对外服务接口提供访问控制措施。

6.1.3 系统支持相关方

区块链存证系统支持相关方的有效性，宜具备以下要素：
a） 采用安全可靠的开源区块链技术；
b） 具备友好的行业监管接口，支持服务审计；
c） 具备良好的区块链服务治理能力。

6.2 电子数据存取的有效性

电子数据存取的有效性，宜具备以下要素：
a） 电子数据的完整性算法具备唯一性；
b） 电子数据的校验值具备唯一性；
c） 支持存证提取的全过程验证和追溯；
d） 支持多方存证、取证和相互验证。

6.3 存证时间的有效性

电子数据存证时间的有效性，宜具备以下要素：
a） 避免电子数据中证明性时间的本地化采集；
b） 引入授时中心，为电子数据提供可信、可追溯的可信时间标识核验服务；

c) 支持电子数据存证时间、区块链系统记录时间可被核验；

d) 支持按照时间顺序核验存证过程。

6.4 存证核验的有效性

存证核验的有效性，宜具备以下要素：

a) 电子数据存证信息能够通过核验；

b) 电子数据的元数据和原文能够通过核验(如适用)；

c) 核验过程按时间顺序执行；

d) 核验过程实时在线。

7 存证过程

7.1 存证应用开发

区块链存证应用开发，宜：

a) 基于开源可控的底层链技术搭建区块链存证网络，并具备安全机制，包括鉴权及准入机制、节点安全加固机制、安全传输机制等；

b) 采用成熟可靠的共识机制，参与共识的节点不少于4个；

c) 采用成熟可靠的编程语言编写并部署存证业务相关智能合约，可支持多签和二次存证功能；

d) 具备跨链机制，支持不同区块链网络之间的数据交互、共享和验证，并可追溯。

7.2 电子数据预处理

存证前，需要对待存证的电子数据进行预处理，宜：

a) 检查电子数据是否符合存证要求；

b) 检查电子数据、元数据和原文(如适用)的内容是否符合法律法规要求；

c) 对电子数据的内容进行隐私保护处理；

d) 对电子数据相关信息进行完整性校验值计算和验证。

7.3 电子数据签名

对待存证的电子数据进行链下数字签名时，宜：

a) 使用合法授权的数字证书；

b) 使用符合安全性要求的密钥进行数字签名；

c) 不再使用被确认泄漏或因其他原因失效的密钥；

d) 能够在区块链网络内和区块链网络外验证数字签名信息。

7.4 电子数据上链

待存证的电子数据上链过程中，宜：

a) 确保存证内容生成、传输、存储和介质保管所依赖的环境安全、可靠；

b) 通过节点向区块链存证系统发起请求，进行电子数据存证；

c) 调用存证合约的多签功能完成链上签名的过程(如适用)；

d) 调用存证合约的二次存证功能完成链上存证信息补充或修正的过程(如适用)；

e) 实时反馈存证结果，并具备容错处理能力。

7.5 链上存证数据公示和查询

链上存证的电子数据支持公示和查询。存证公示或查询时，宜：

a） 采用网站或公共接口等多种方式进行存证公示；

b） 提供通过关键词和时间等条件进行检索的服务；

c） 提供区块链浏览器等工具，使用区块数据进行直接验证；

d） 支持通过区块链网络中的任一节点进行查询验证；

e） 提供多节点查询交叉验证方法；

f） 同一条存证具备多重签名信息的，给出多签列表（如适用）；

g） 同一个存证唯一标识码具备多条二次存证记录的，给出完整信息（如适用）。

7.6 链上存证数据提取

链上存证的电子数据可从区块链网络上直接提取。提取存证时，宜：

a） 保证提取过程所依赖的计算机系统的硬件、软件环境安全、可靠；

b） 保证提取过程可重现且记录是连续的。

7.7 链上存证数据验证

7.7.1 验证对象

链上存证的电子数据的验证对象包括所存证的电子数据、元数据和原文（如适用）、存证使用者身份、存证多签列表及签名者身份（如适用）、存证时间和其他。

7.7.2 验证过程

链上存证的电子数据在验证时，宜：

a） 基于所存证的电子数据、元数据和原文（如适用）进行验证；

b） 基于与存证时相同的完整性校验算法计算校验值进行验证；

c） 基于数字签名信息验证存证使用者身份；

d） 基于智能合约验证多签列表中签名者身份（如适用）；

e） 支持通过可信的数字身份认证中心进行验证；

f） 支持通过授时中心的可信时间服务进行验证；

g） 支持其他验证对象在其来源的官方网站进行在线验证。

7.7.3 验证结果信息

链上存证的电子数据验证结果信息宜包括：

a） 存证唯一标识码；

b） 链上存证的电子数据和完整性校验值；

c） 二次存证记录及相关信息（如适用）；

d） 存证使用者信息和数字证书颁发机构信息；

e） 多签列表和签名者身份信息（如适用）；

f） 存证时间和可信时间标识信息；

g） 存证过程日志信息；

h） 元数据和原文（如适用）；

i） 链上和链下验证过程说明和验证结论；

j） 其他信息。

7.7.4 验证结论

链上存证的电子数据验证宜给出明确结论，如通过或未通过。

7.7.5 其他

链下信息的服务提供者可提供相关权威性证明文件（如适用），包括：

a） 服务能力证明，如通过行业评测或符合行业鉴定标准的证明文件；
b） 著作权登记证明；
c） 其他证明文件。

8 数据指南

8.1 数据格式

区块链存证电子数据宜采用 JSON 或 XML 等标准化数据格式以便于解析。

8.2 数据内容

使用区块链技术存证电子数据信息，其数据内容宜包括：

a） 存证唯一标识码；
b） 所存证电子数据；
c） 完整性校验值及所使用的完整性校验算法；
d） 数字签名信息；
e） 元数据和原文（如适用）；
f） 存证时间和可信时间标识；
g） 完整的日志信息，以及存证过程中关键节点的可信时间标识、服务使用者、操作内容、对象和存储路径等信息；
h） 其他。

9 服务指南

9.1 存证前

存证前，其过程宜具备以下要素：

a） 存证服务提供者对存证服务使用者进行身份核验；
b） 存证服务使用者检查存证使用的计算机信息系统硬件、软件以及网络环境可靠、安全，并处于正常运行状态，条件允许时将相关信息也进行存证。

9.2 存证中

存证中，其过程宜具备以下要素：

a） 存证服务使用者使用存证服务提供者提供的网站、应用程序或编程接口，将电子数据的原文或完整性校验值、数字签名信息等数据同步传输至存证服务平台；
b） 存证服务提供者记录存证服务平台的硬件设备信息、软件系统信息、网络信息及过程数据等，并计算相关信息的完整性校验值，将记录的数据与对应的完整性校验值同时进行存证；

c) 进行原文存证的，提交存证内容电子数据原文到存证服务平台；不进行原文存证的，存证服务平台进行风险告知，以防原文篡改或丢失导致无法验证的情况出现。

10 安全指南

10.1 系统安全

存证服务平台宜达到 GB/T 22239—2019 规定的第三级基本要求，宜具备以下要素：

a) 所使用的物理设备及环境具备完善的监控体系，保证 7×24 小时稳定运行，系统具备高可用性（99.99%以上）；

b) 采取措施保障存证服务平台的安全，预防非授权的访问或破坏，对于非授权的访问或破坏具有防护措施和应急预案；

c) 定期检查，防止网络攻击、病毒和非法网络代理的使用。

10.2 存储安全

存证服务平台确保存储安全，宜具备以下要素：

a) 具备冗余备份和存储扩展的能力，并具备异地容灾能力；

b) 存储内容符合国家有关规定；

c) 采用符合国家密码管理主管部门认证核准的密码技术对数据进行加密传输和存储，并对密钥采取必要的保护机制；

d) 密码安全强度不低于国密相关要求。

10.3 传输安全

存证服务平台宜保证电子数据存储和传输过程涉及的系统和软件安全可控，宜具备以下要素：

a) 对存证服务使用者身份进行可信认证，并保留认证记录；

b) 保证传输过程中数据的机密性；

c) 采用完整性校验技术对存证服务使用者和存证服务提供者的传输数据进行校验，确保传输数据的完整性；

d) 接口及系统配置安全可靠，避免系统代码被反编译或篡改。

10.4 可信指南

10.4.1 数据可信

存证服务平台保证所存证的电子数据可被验证和追溯；所存证的电子数据除采用哈希数值、数字签名信息等形式外，在有必要的情况下可在平台上保存原文信息。

10.4.2 身份可信

存证服务使用者宜采用可信的数字身份认证服务进行身份鉴别和验证。

10.4.3 时间可信

存证服务平台的系统时间宜从可信时间源（如国家授时中心）进行授时并守时。

10.5 隐私保护

存证服务平台符合 GB/T 35273—2020 相关规定，宜具备以下要素：

a) 仅采集和保存存证业务所必需的存证服务使用者信息；
b) 检索结果中不可显示非该服务使用者的存证信息；
c) 数据访问被记录且支持追溯和审计；
d) 涉及个人敏感信息的数据进行脱敏处理。

10.6 数据检索

存证服务平台宜仅向已认证的服务使用者提供数据检索服务。

10.7 监管

区块链存证应用服务应符合国家相关法律法规与行业监管要求。

参 考 文 献

[1] GB/T 5271.18—2008 信息技术 词汇 第18部分:分布式数据处理
[2] GB/T 11457—2006 信息技术 软件工程术语
[3] GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范
[4] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南