

国家标准

《信息技术 区块链和分布式记账技术 存证应用指南》

（征求意见稿）

编制说明

2022 年 6 月

目 录

一、工作简况.....	3
二、标准编制原则和确定主要内容的论据及解决的主要问题.....	7
三、主要试验情况分析.....	8
四、知识产权情况说明.....	9
五、产业化情况、推广应用论证和预期达到的经济效果.....	9
六、采用国际标准和国外先进标准情况.....	9
七、与现行相关法律、法规、规章及相关标准的协调性.....	10
八、重大分歧意见的处理经过和依据.....	10
九、标准性质的建议.....	10
十、贯彻标准的要求和措施建议.....	10
十一、替代或废止现行相关标准的建议.....	10
十二、其它应予说明的事项.....	10

一、工作简况

（一）任务来源

2020 年，根据国家标准化管理委员会（国标委发【2020】14 号）文件下达的国家标准制修订计划，《信息技术 区块链和分布式记账技术 存证应用指南》国家推荐性标准获批立项。

国家标准计划《信息技术 区块链和分布式记账技术 存证应用指南》由 TC590（全国区块链和分布式记账技术标准化技术委员会）归口上报及执行，主管部门为工业和信息化部。

（二）参加单位

本标准主要起草单位包括厦门安妮股份有限公司、中国电子技术标准化研究院、上海万向区块链股份公司、深圳市前海智慧版权创新发展研究院、华为技术有限公司、杭州趣链科技有限公司、深圳前海微众银行股份有限公司、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、蚂蚁区块链科技（上海）有限公司、深圳市腾讯计算机系统有限公司、湖南天河国云科技有限公司、四川长虹电子控股集团有限公司、北京版全家科技发展有限公司、国网数字科技控股有限公司、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、京东科技信息技术有限公司、北京微芯区块链与边缘计算研究院、上海零数科技有限公司、广东电网有限责任公司广州供电局、上海阵方科技有限公司、联通数字科技有限公司、上海奥若拉信息科技集团有限公司、达闼机器人股份有限公司、浙商银行股份有限公司、北京中科金财科技股份有限公司。

由中国电子技术标准化研究院组织，安妮股份牵头，主要负责标准相关资料的搜集和调研、标准框架编制、标准内容起草、组织讨论、反馈意见整理，以及标准报批等工作，编制组其他成员参与标准的技术讨论、标准的编写和修改工作。

（三）编制过程

1) 标准编制组成立及标准起草阶段

2018 年 12 月 18 日中国电子技术标准化研究院联合国内区块链领域的专家共同编写并发布了《中国区块链技术与应用发展研究报告（2018）》，系统分析了区块链技术和应用面临的机遇和挑战、区块链技术发展情况研究、区块链应用发展情况研究、区块链标准化最新进展研究，同时分析了存证、国际贸易融资、

电子营业执照等应用案例。

2018年8月至2019年3月，各参编单位就区块链存证有效性原则、区块链存证相关方以及区块链存证关键过程等方面展开讨论，细化具体标准内容的编写，形成了标准草案。该草案除了明确标准的范围、给出规范性引用文件、术语和定义之外，重点描述了区块链存证系统的应用模型、相关方、有效性原则、存证过程、服务指南等。主要包括：

- 1 范围
- 2 规范性引用文件
- 3 术语和定义
- 4 应用模型
- 5 相关方
- 6 有效性原则
- 7 存证过程
- 8 服务指南

2020年11月25日，中国电子技术标准化研究院组织召开了国家标准启动会。会上首先各参编单位介绍了与标准相关业务成果和技术能力，电子标准院介绍了标准制定的流程和注意事项。电子标准院专家介绍了标准的思路，初步的提纲，各参编单位就提纲进行了交流讨论，提出了调整意见，并对修改工作进行了分工。最后，会议形成如下主要修改意见：

1. 引言**错误!未定义书签**。删除“部署、测试、运行和维护”等文字，恢复前言中的“运维”。

2. 3.1.1 非对称密钥对 asymmetric key pair 与 3.1.2 鉴权机制 authentication mechanism 去掉，因正文做了修改。

3. 3.1.3 更新区块链、共识算法、分布式账本、智能合约等到最新的定义。

4. 删除：AES、API、BRA、DLT、DPoS、ECC、PoW、PoS 等缩略语，正文未体现。

5. 第4章：从存证过程看，电子证据经历了数据的生成、收集、储存、传递、认证、验证6个阶段。在生成、收集、储存、传递这4个环节中，电子证据是有可能发生变动的（来自《人民司法》最高人民法院机关刊载文，这些司法

用语文中没有体现) 存证过程阶段的用语使用“生成、收集、储存、传递、认证、验证”等司法标准用语, 有关司法的文字, 改动后下次会议沟通。

6. 5.1 增加国密的描述, 什么时候推荐使用什么算法, 需要细化每一种过程里。

7. 第6章中外部相关方工作程序研究, 汇总一个, 没覆盖到的增加, 附录给出通用做法, 未来怎么做, 研究分工给不同单位。

8. 7.1 区块链网络定义中: 去掉“支持司法延伸服务”; 建立完善的网络机制, 去掉完善的。

9. 7.1 增加: “宜增加多节点查询交叉验证”等文字。

10. 对附录进行调整, 评价方法体系从技术、服务、应用角度。

2021年4月14日, 标准编制组召开第二次研讨会, 就上个版本草案进行了充分交流讨论。会议形成如下主要修改意见:

1. 引言部分补充修订最新进展。

2. 范围增加“相关要求”。

3. CBD-Forum-001-2017 区块链 参考架构国标名字更新。ISO/IEC 9804-1998 补充中文名字。

4. 3.1.5 存证过程“在区块链网络中, 电子数据生成、收集、存储、传输的过程”顺序及文字描述需要与后文统一。

5. 8.对应的要求, 要求中包括数据、传输、安全、可信等, 将现有第7章和8.6合并到第九章)。

6. 第4章关键过程删除“传输要求”。

7. 第五章和第七章有重叠, 建议将第五章扩充范围, 章节名字改为原则, 其中包括有效性原则、XXX原则。

8. 5.1 存证使用人、用户需要上下文统一。

9. 5.1 改为: 哈希算法密码强度不低于256位, 加密算法密码强度不低于128位。

10. 5.5 改为: 1) 调用机构节点提供的对外服务接口宜具备权限管理措施;
2) 调用机构节点提供的对外服务接口宜具备访问控制措施。

11. 5.5 “核验支持联机状态或脱机状态”改为“应支持在线核验验证”。

12. 6.2 改为相关方的节点参与方式，6.1 改为相关方，6.2 改为技术相关方。

13. 第8章：8.1 和 8.2 合并，简化内容，描述建立网络和定义共识主要作为前置条件（内容由趣链补充），不具体描述选择哪些网络、共识算法。

14. 梳理全文，上下文统一。例如“数据生成”“数据搜集”“预处理”等内容。

15. 8.6 放到第七章。

16. 删除附录 A。

17. 删除并选取部分补充至正文。

18. 删除附录 C（修改 6 相关方）。

会后，编制组根据修改意见完成了对《信息技术 区块链和分布式记账技术存证应用指南》第二版草案的修改，形成了第三个版本草案。

2021 年 9 月 17 日，标准编制组组织讨论，主要修改意见如下：

1. 1 范围删除“界定了区块链存证的术语、定义和缩略语”。

2. 3.1.17/3.1.18 增加：电子数据存证服务者/电子数据存证服务提供者的术语和定义。

3. 4 应用模型：关键过程中，删除传输要求；图中少字，补充为“电子数据签名”。

4. 5.1 业务系统由建议删除，改为存证服务提供者，内容并同步修改；密码强度改为：“相应密码安全强度”，不展开描述。。

5. 6.1.1 内部相关方已统一修改改为存证服务提供者，上下文一致，并做了具体界定。

6. 6.2 系统支持相关方由“支持相关方”改为“系统支持相关方”，内容做相应修改。

7. 7.1 原 8.1 和 8.2 合并且简化内容，描述建立网络和定义共识主要的前置条件。

8. 按要求做了相应调整，将原 7/8.6/9 章合为现在的章节 8。

9. 存证过程删除传输要求，同时挪到第八章的“安全要求”的“传输安全”中。

10. 补充相关参考文献。
11. 统一修改页码、编号。
12. 梳理全文，上下文统一。例如“数据生成”“数据搜集”“预处理”等内容。

会后，编制组根据修改意见完成了对《信息技术 区块链和分布式记账技术参考架构》第三版草案的修改，形成了第四个版本草案。

2021 年 10 月 19 日，召开线上会议，编写组真对标准草案在书写规范性、文字描述、配图格式等方面进行统一审核，形成了征求意见稿。

1. 1 IEEE P2418.2 非官方认可，去掉。
2. 3 术语定义宜直接参考《区块链和分布式记账技术 术语》中的标准 iso 标准 22739-2020（发布） 相对准确。
3. 6.2 系统支持相关方增加其他。
4. 7.8 系统对接增加扩展描述做相应修改；系统对接；修改措辞，弱化法院；符合本标准改为本文件，应改为宜。
5. 7.9 技术实现：存证过程增加技术实现一节：去掉。
- 6.8 服务指南（要求）服务要求改为服务指南，其下小章节名称做相应修改，尽量为“指南”与标准名称对应。
7. 增加参考文献：规范性引用文件中提到的需要增加到参考文献中；正文中参考的要提到规范性引用文件。
8. 全文应“需”修改为“宜”。

2022 年 4 月，召开线上会议，编写组真对标准草案在书写规范性、文字描述、配图格式等方面进行统一审核，完成了最后的修改；其后在此基础上形成了征求意见稿。

二、标准编制原则和确定主要内容的论据及解决的主要问题

（一）标准编制原则

标准的用语、格式按照 GB/T 1.1-2009 给出的规则起草。

标准内容的编制坚持以下原则：

- 1、结合产业实际情况

标准起草组在标准制定过程中，坚持产学研用相结合，听取各方意见，充分调研国内区块链行业的实际需求，给出了可供区块链相关各行业使用区块链技术进行存证的基本应用指南。

2、操作性

本标准以可操作性作为考虑的基本出发点，主要针对目前各行业使用区块链技术进行存证在设计、开发、部署、测试、运行和维护等环节，以更高效、便捷、准确的搭建区块链存证应用系统，为区块链技术发展提供范化与标准化存证应用模型，为构建整体的区块链生态提供规范的应用类资源框架，确保了本标准可在实际系统开发中具有指导意义。

（二）主要内容和解决的问题

1、区块链存证应用指南的主要内容和作用：本标准从存证应用的实际业务需求出发，规定了区块链存证有效性原则、区块链存证相关方以及区块链存证关键过程。标准规范了电子数据存证服务、存证平台和电子数据存证过程，指导组织和机构建立、实施、保护和改进区块链存证体系，可以为计划使用区块链存证技术的相关应用、为计划建设区块链存证系统的组织和机构、为采用了区块链存证技术的行业监管提供参考。

2、存证指南标准第4章应用模型内容：明确了区块链存证业务相关方与区块链存证系统支持相关方两类区块链存证相关方角色。

3、存证指南标准第5章业务相关方内容：明确了区块链存证业务相关方与区块链存证系统支持相关方两类区块链存证相关方角色。

4、存证指南标准第6章有效性原则内容：给出了区块链有效性原则，在业务系统、电子数据存取的有效性、时间的有效性、存证证明机构的有效性以及存证核验的有效性等五个方面给出了要求。

5、存证指南标准第7章存证过程内容：给出了区块链存证的七大关键步骤，包括定义区块链网络及共识机制、写入区块链数据预处理、电子数据签名、存证过程、存证公示和查询、提取存证和存证第三方验证等。

6、存证指南标准第8章服务指南内容：从数据格式、存证过程、安全、可信、隐私保护、数据检索、监管等方面给予指导。

三、主要试验情况分析

为了验证《区块链 存证应用指南》的适应性和可行性，安妮股份于 2019

年1月组织版权区块链联盟内部会议，对标准进行了宣贯。2020年7月29日，在第四届中国区块链开发大赛上介绍了本标准的工作；2020年9月29日，在南昌区块链大会对标准进行介绍推广等，多渠道多方式的宣讲及推广，促进了各相关方对标准内容的理解和相关企业对产品质量安全与品质管控的重视，有效推动了标准的实施。其次标准的应用实施试点工作，已应用于中央网信办“区块链+版权”创新应用试点、版权家综合服务平台、国家版权创新发展基地公共服务平台、深圳市知识产权金融公共服务平台等。通过促进区块链行业技术研发，结合区块链相关标准，实现标准固化创新成果，提高产业发展的综合竞争能力，为加快产业化进程奠定技术基础。

四、知识产权情况说明

本标准不涉及相关知识产权。

五、产业化情况、推广应用论证和预期达到的经济效果

随着区块链技术的发展，基于区块链技术的存证业务被广泛应用于各行业。根据最高人民法院于2018年9月7日公布的《最高人民法院关于互联网审理案件若干问题的规定》第十一条，“当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认”。由于缺乏规范统一的存证业务应用标准，各行业在存证业务的实施情况各不相同，区块链存证有效性未取得普遍认可，亟需统一标准以规范区块链存证系统建设，保障区块链存证行业健康有序发展。

区块链存证是基于区块链技术，采取多节点共识的方式，或联合法院、公证处、仲裁机构、司法鉴定中心、授时服务机构、审计机构及数字身份认证中心等权威机构节点的电子数据存证服务。区块链以及相关分布式账本技术可以保证存证信息的完整性和真实性，促进创新应用落地以及形成产业生态发展。

标准为各行业使用区块链技术进行存证给出基本应用指南，指导区块链存证应用的设计、开发、部署、测试、运行和维护等环节，以更高效、便捷、准确的搭建区块链存证应用系统，为区块链技术发展提供范化与标准化存证应用模型，为构建整体的区块链生态提供规范的应用类资源框架。

六、采用国际标准和国外先进标准情况

本标准没有采用其他国家标准和国际标准。

七、与现行相关法律、法规、规章及相关标准的协调性

在本标准的制定过程中，在术语等方面，规范应用了以下已有的信息技术相关标准，包括《信息安全技术：网络安全等级保护基本要求》GB/T 22239-2019、《信息安全技术 术语》GB/T 25069-2010、《信息技术 云计算 参考架构》GB/T 32399-2015、《信息安全技术 个人信息安全规范》GB/T 35273-2017、《信息技术 区块链和分布式记账技术 参考架构》（报批稿）、《信息技术 开放系统互连 托付、并发和恢复服务元素》ISO/IEC 9804-1998等国家标准和国际标准。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议

本标准是区块链存证应用相关的基础性标准，也可为其他行业或领域的相关标准提供借鉴和参考。建议该标准为推荐性标准。

十、贯彻标准的要求和措施建议

在区块链产品交付和系统实施过程中，建议根据标准规范对产品和系统进行符合性测试和验证。

十一、替代或废止现行相关标准的建议

无。

十二、其它应予说明的事项

无。

国家标准《信息技术 区块链和分布式记账技术 存证应用指南》编制工作组

2022 年 6 月