中国区块链技术和产业发展论坛标准

CBD-Forum-003-2018

区块链 存证应用指南

Blockchain—Application guidelines for proof of existence

2018-12-18 发布　　2018-12-18 实施

中国区块链技术和产业发展论坛　　发 布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由中国区块链技术和产业发展论坛提出。

本标准负责起草单位：厦门安妮股份有限公司、中国电子技术标准化研究院、众安信息技术服务有限公司、深圳前海微众银行股份有限公司、上海万向区块链股份公司、中国平安保险（集团）股份有限公司、浙江蚂蚁小微金融服务集团有限公司、北京京东尚科信息技术有限公司、易见供应链管理股份有限公司、上海复星高科技（集团）有限公司、福建省海峡区块链研究院、三六零科技有限公司、永辉超市股份有限公司、上海金丘信息科技股份有限公司、普华永道中天会计师事务所（特殊普通合伙）。

本标准主要起草人：郝汉、李鸣、杨胜、周海平、宋文鹏、李斌、杜宇、郝玉琨、翟欣磊、闫莺、张卫中、孙琳、落红卫、瞿争、徐磊、鞠鹏、陈钟、高敏源、邹涛、刘天成、赵阳、陈家乐、齐宁宁、李立、张凯文、赵伟、杨智浩、郝佳诺、洪蜀宁、赵冉、高辉、莫寒、锐东、高林辉、朱振博、张开翔、汤丰、岳峰、林森、程雅丽、肇洽宇、卢修禄、宋汶键、赵晓晨、张林、宋晓亮、王琰、洪双燕、张康荣、李永正、张作义。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国电子技术标准化研究院（中国区块链技术和产业发展论坛　秘书处）联系。

电话：010-64102801/2804

电子邮件：cbdforum@cesi.cn

通信地址：北京东城区安定门东大街 1 号（100007）

为了推动本标准的持续改进，使其内容更加贴近用户组织的实际需求，欢迎社会各方力量参加本标准的持续改进，本标准的更多信息欢迎关注中国区块链技术和产业发展论坛官方网站和公众号。

http://www.cbdforum.cn

引　言

近年来，在政策、法律、技术、市场等多方推动下，区块链技术正加速脱虚向实，助力实体经济高速发展。与此同时，区块链标准建设对我国形成数字经济产业生态、探索共享经济模式、提升行业治理和公共服务水平具有重要意义。

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。本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。

区块链 存证应用指南

1 范围

本标准给出了包括有效性原则、相关方和存证关键过程的区块链存证应用指南，界定了区块链存证的术语、定义和缩略语。

本标准适用于：

a) 为计划使用区块链存证系统的组织和机构提供参考；

b) 指导组织和机构建立、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

下列文件对于本文件的应用是必不可少的。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 25069-2010 信息安全技术 术语

GB/T 32399-2015 信息技术 云计算 参考架构

CBD-Forum-001-2017 区块链 参考架构

ISO/IEC 9804-1998 信息技术．开放系统互连．托付、并发和恢复服务元素的服务定义（Information technology-Open Systems Interconnection-Service definition for the Commitment, Concurrency and Recovery service element）

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069-2010、GB/T 32399-2015、CBD-Forum-001-2017、ISO/IEC 9804-1998 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 25069-2010、GB/T 32399-2015、CBD-Forum-001-2017、ISO/IEC 9804-1998 中一些术语和定义。

3.1.1

非对称密钥对 asymmetric key pair

一对相关的密钥，其中私有密钥规定私有变换，公开密钥规定公开变换。

[GB/T 25069-2010，定义 2.2.2.33]

3.1.2

鉴权机制 authentication mechanism

验证用户是否拥有访问系统权利的机制。

3.1.3

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。

[CBD-Forum-001-2017，定义 2.2.1]

3.1.4

区块链存证 blockchain proof of existence

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。

3.1.5

共识算法 consensus algorithm

区块链系统中各节点间为达成一致采用的计算方法。

[CBD-Forum-001-2017，定义 2.2.3]

3.1.6

共识机制 consensus mechanism

通过特殊节点投票，完成对交易的验证和确认。

3.1.7

摘要算法 digest algorithm

摘要函数；Hash 函数

通常通过将任意长度的消息输入变成固定长度的短消息输出来保障数据的完整性。

[CBD-Forum-001-2017，定义 2.2.4]

3.1.8

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[GB/T 25069-2010，定义 2.1.2]

3.1.9

分布式应用 distributed application

使用开放式系统互联环境中的两个或更多个应用实体调用来完成信息处理。

[ISO/IEC 9804:1998，定义 2.1.3]

3.1.10

分布式账本 distributed ledger

可以在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的资产数据库。

[CBD-Forum-001-2017，定义 2.2.5]

3.1.11

分布式账本技术 distributed ledger technology

实现分布式账本的技术的集合。

[CBD-Forum-001-2017，定义 2.2.6]

3.1.12

电子数据 electronic data

以电子手段生成、发送、接收或者储存的信息。

3.1.13

加密 encipherment; encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

[GB/T 25069-2010，定义 2.1.4]

3.1.14

功能组件 functional component

参与活动所需的，可实现的一个功能性基本构件块。

[GB/T 32399-2015，定义 2.1.5]

3.1.15

存证过程 proof of existence process

在区块链网络中，电子数据生成、收集、存储、传输的过程。

3.1.16

角色 role

一组服务于共同目的的活动的集合。

[GB/T 32399-2015，定义 2.1.9]

3.1.17

智能合约 smart contract

以数字形式定义的能够自动执行条款的合约。

[CBD-Forum-001-2017，定义 2.2.7]

3.1.18

第三方证明 the third party’s certification

非存证执行主体之外的可信组织提供的证明服务。

3.2 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

API：应用编程接口（Application Programming Interface）

BRA：区块链 参考架构（Blockchain - Reference Architecture）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DLT：分布式账本技术（Distributed Ledger Technology）

DPoS：股份授权证明机制（Delegate Proof of Stake）

ECC：椭圆曲线加密（Elliptic Curve Cryptography）

PoW：工作量证明（Proof of Work）

PoS：权益证明（Proof of Stake）

4 区块链存证应用模型

区块链存证应用模型包含有效性原则、相关方和区块链存证关键过程，见图 1。

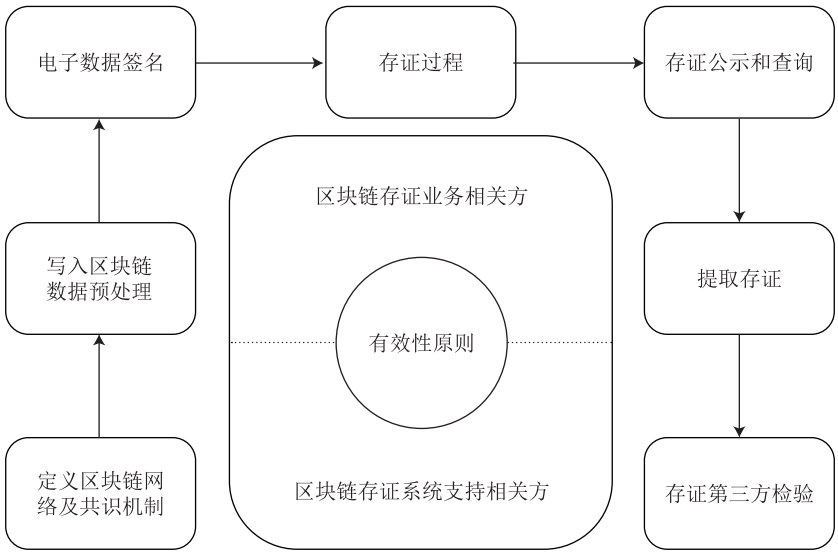

图 1 区块链存证应用模型

有效性原则包括存证业务系统、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。相关方分为区块链存证业务相关方与区块链存证系统支持相关方。区块链存证关键过程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，以及存证第三方验证。

区块链应用全景图可参考附录 A。

5 有效性原则

注：区块链存证的有效性可参考附录 B 分级。

5.1 业务系统

业务系统宜：

a) 具备完善的存证业务逻辑，可记录完整电子数据，可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，可对存证人的身份真实性进行认证和校验，可完整记录用户操作日志；

c) 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；

d) 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 电子数据存取的有效性

电子数据存取的有效性需考虑：

a) 存证过程中电子数据的哈希值具备唯一性；

b) 取证全过程可验证；

c) 多方存证、取证和相互验证。

5.3 时间的有效性

时间的有效性需考虑：

a) 避免电子数据中证明性时间的本地化采集；

b) 引入独立授时机构，为电子数据提供可信、可查验、可追溯的时间戳核验服务；

c) 电子数据时间戳、区块链系统记录时间可被核验；

d) 取证过程满足多个时间点的认证核验。

5.4 存证证明机构的有效性

存证证明机构的有效性需考虑：

a) 区块链存证系统引入中立的、具有公信力的机构节点，如法院、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；

b) 引入机构的节点存证数据与其他节点存证数据保持实时同步；

c) 机构节点与其他节点的通信通道做加密处理；

d) 机构节点提供的对外服务接口做加密处理。

5.5 存证核验的有效性

存证核验的有效性需考虑：

a) 电子数据的元数据信息可被核验；

b) 核验按时间顺序执行；

c) 核验支持联线状态或脱机状态。

6 相关方

注：区块链存证相关方与关键活动参考附录C。

6.1 区块链存证业务相关方

6.1.1 内部相关方

区块链存证系统内部相关方可包括存证业务的使用者、区块链存证系统的开发者、区块链存证系统的运行维护者、运营部门、最终用户及协助完成区块链存证过程的其他成员。

6.1.2 外部相关方

区块链存证系统可以依据业务需求引入外部参与者作为鉴证节点，以对电子数据内容有效性做出独立判断。外部相关方包括：

a) 司法机关：行使司法权的国家机关，是国家机构的基本组成部分，是为了保证法律实施而建立的相关组织；
b) 公证处：依法独立行使公证职能、承担民事责任的证明机构；
c) 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；
d) 司法鉴定中心：利用科学技术或专门司法知识为司法相关问题提供鉴定意见的机构；
e) 授时服务机构：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；
f) 数字身份认证中心：提供数字证书的颁发、核验服务的机构；
g) 其他。

6.2 区块链存证系统支持相关方

区块链存证系统支持相关方可分为记账节点和非记账节点。

a) 记账节点是指区块链网络中可获取记账和发布区块权限的节点。区块链网络中，记账节点的选取方式由区块链网络类型决定；
b) 非记账节点是指不参与记账和发布区块权限的节点。区块链网络中，非记账节点可包含业务系统节点、区块链接口节点、系统支持节点、数据节点等。

7 区块链存证关键过程

7.1 定义区块链网络及共识机制

在建立存证系统时，可按需要定义或选择区块链网络的共识机制。存证的共识机制包括基于工作量的共识机制、基于投票的共识机制、基于公信力节点的共识机制和其他共识机制。具体内容如下：

a) 基于工作量的共识机制：基于行为量化等特定算法来确定记账节点的共识机制；
b) 基于投票的共识机制：基于资源量化等特定算法来确定记账节点的共识机制；
c) 基于公信力节点的共识机制：由单个或多个具备公信力的节点进行鉴证，通过该节点执行强制校验的共识机制；
d) 其他共识机制。

7.2 写入区块链数据预处理

写入区块链数据预处理时宜：

a) 检查区块链系统外电子数据是否满足存证要求；

b) 检查电子数据的内容是否符合法律法规要求；

c) 检查电子数据的隐私内容是否已脱敏，是否涉及其他隐私内容；

d) 对电子数据相关信息进行有效性验证。

7.3 电子数据签名

对存证内容做电子数据签名时：

a) 宜使用合法授权的身份数字证书；

b) 用户不宜使用被确认泄漏或因其他原因失效的私钥；

c) 用户宜使用本人的私钥进行数字签名；

d) 已签名的数据可在区块链网络内验证。

7.4 存证过程

存证过程中宜：

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；

c) 通过节点向区块链存证系统发起电子数据存证请求进行存证。

7.5 存证公示和查询

存证数据可利用多种方式进行公示和查询，确保所有区块链网络参与者可查询存证公示信息。

a) 公示可采用网站或公共接口方式；

b) 查询等功能可使用区块链浏览器完成；

c) 公示宜体现真实的存证数据，并可通过区块链网络中的节点进行查询验证；

d) 可直接使用区块数据查询进行数据验证。

7.6 提取存证

取证的电子数据应从区块链网络上直接获取。提取存证时宜：

a) 确保取证过程所依赖的计算机系统的硬件、软件环境安全、可靠；

b) 可重现、提取过程的记录是连续的；

c) 取证后的出证信息包括原始存证信息、存证参与者身份信息、存证时间信息、必要的数据传输网络地址信息、出证结论、其他必要信息。

7.7 第三方机构验证

第三方机构符合相关法律、法规要求，具备相关资质。存证第三方机构验证时：

a) 第三方机构可验证的电子数据基于原始数据；

b) 第三方机构根据特定且公开的算法对电子数据进行验证；

c) 第三方机构能提供相关证明文件。

附 录 A
（资料性附录）
区块链存证应用全景图

如图 A.1 所示，区块链存证应用全景图给出了区块链存证应用的主要关系，表达了如下主要过程：

a） 用户通过使用业务功能将存证需求传递到业务系统；

b） 业务系统处理输入的电子数据，在第三方服务支持下进行生成时间戳、电子签名与哈希值计算等处理形成预存证数据；

c） 业务系统对预存证数据进行脱敏、加密等操作后，调用存证接口，将存证请求发送给区块链存证系统；

d） 区块链存证系统经过验证、预处理、共识等过程后出块发布；

e） 用户或机构通过浏览网站或使用区块链浏览器等公示工具查看存证信息；

f） 用户或机构使用工具提取存证信息，并通过相关服务核验相应内容。

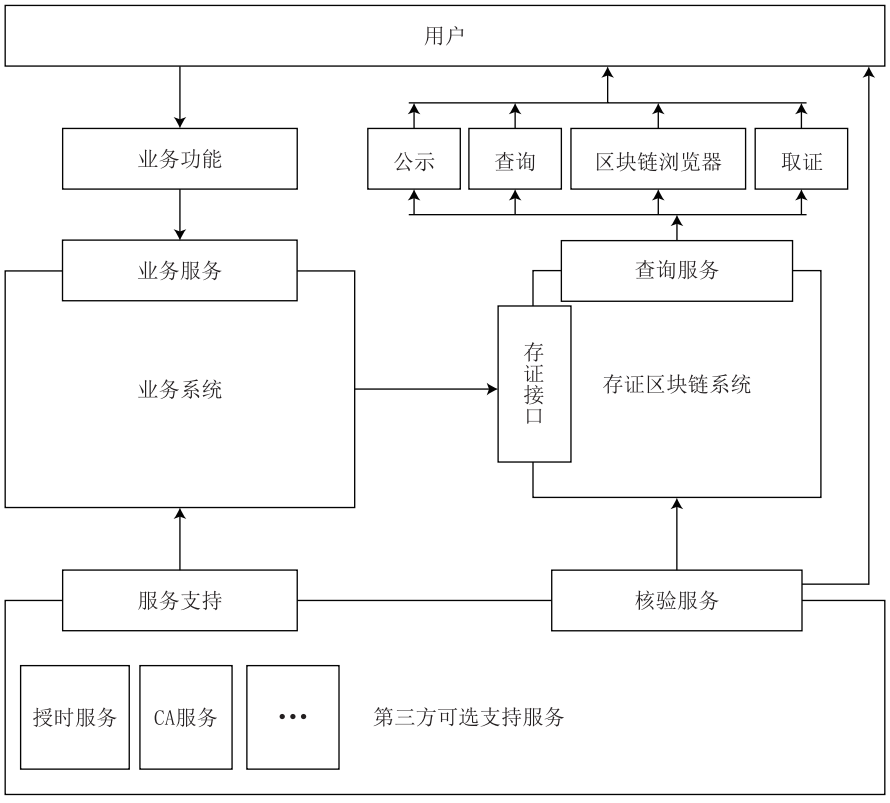

图 A.1 区块链存证应用全景图

附 录 B
（资料性附录）
存证系统评级

B.1 概述

区块链存证系统依据存证内容的有效性原则，可分为声明级、自证级和验证级。相关机构可依据此分级方式对相关业务或系统进行评价。

B.2 声明级

声明级，当存证人仅对存证内容声明时，可通过转账或智能合约写入等方式在公共的区块链上声明内容，仅用以证明该存证内容的存在性，无法验证真实性，无法验证内容归属人。

B.3 自证级

在声明级基础上，当存证人需要对存证内容做自证时：

a) 可通过公开的信息摘要算法验证内容的完整性；
b) 可通过数字身份认证与数字签名信息验证内容的归属权；
c) 可通过其他方式证明存证真实性。

B.4 验证级

在自证级基础上，当存证人需要第三方机构协助验证时：

a) 系统可通过有效性鉴定，如符合国家相关司法鉴定标准；
b) 存证内容可通过身份核验，如国家认可的数字身份认证中心进行身份验证；
c) 存证内容可通过时间核验，如授时服务机构的可信时间核验；
d) 存证内容可通过内容核验，如著作权管理部门对数字内容的独创性审核。

附 录 C
（资料性附录）
区块链存证相关方与关键活动映射表

区块链存证系统业务包括运维、运营、服务、公示、查询、取证等，支持服务方包括数字身份认证中心、司法鉴定中心、仲裁机构等。区块链存证相关方在关键活动中的角色关系，可参考表 C.1 所示。

表 C.1 区块链存证相关方与关键活动映射表

编号	关键活动	区块链存证相关方
1	定义区块链网络及共识机制	区块链存证系统建设者
2	写入区块链数据预处理	运营相关方
3	电子数据签名	颁发证书的数字身份认证中心
4	存证过程	服务节点、记账节点
5	存证公示与查询	区块链存证系统使用者
6	提取存证	运营相关方、区块链存证系统使用者
7	存证第三方验证	法院、数字身份认证中心、授时服务机构、司法鉴定中心、仲裁机构、公证处等第三方机构

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 25069-2010 信息安全技术 术语

[4] GB/T 32399-2015 信息技术 云计算 参考架构

[5] CBD-Forum-001-2017 区块链 参考架构

[6] ISO/IEC 9804-1998 信息技术．开放系统互连．托付、并发和恢复服务元素的服务定义（Information technology-Open Systems Interconnection-Service definition for the Commitment, Concurrency and Recovery service element）

CBD-Forum-001-2018

电话：010-64102801/2804
电子邮件：cbdforum@cesi.cn
网址：http://www.cbdforum.cn