中国区块链技术和产业发展论坛标准

CBD-Forum-003-2020

区块链 电子合同存证应用指南

Blockchain—Electronic contract deposit guidelines

2020-07-31 发布　　2020-07-31 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《标准化工作导则 第1部分：标准的结构和编写》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。

本标准起草单位：京东数字科技控股股份有限公司、中国电子技术标准化研究院、北京百度网讯科技有限公司、易见供应链管理股份有限公司、中国电子科技网络信息安全有限公司、厦门安妮股份有限公司、北京中电普华信息技术有限公司、中国平安保险（集团）股份有限公司、浙江大学、杭州趣链科技有限公司、深圳市腾讯计算机系统有限公司、智度科技股份有限公司。

本标准主要起草人：翟欣磊、李鸣、庞玉燕、李佳秾、田鑫、彭涛、肖伟、刘天成、白健、郝汉、陈宋科、张春光、李努锲、陶祥忍、谭伟亮、刘文婧、周晓健、王思宁、冯承勇、蔡亮、陈晓丰、武杨、王乐庆、王鹏飞。

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

区块链 电子合同存证应用指南

1 范围

本标准提供了区块链电子合同存证的一般原则，给出了电子合同存证的相关方、数据格式、关键技术过程和业务要求。

本标准适用于：

a） 为计划使用区块链技术实现电子合同业务存证目的的组织和机构提供参考，指导组织和机构建立、实施、保护和改进电子合同存证体系；

b） 为使用区块链存证功能的相关数据安全和互联网司法应用提供参考。

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 7408-2005 数据元和交换格式 信息交换 日期和时间表示法

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子签名 electronic signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

注：数据电文是指以电子、光学、磁或者类似手段生成、发送、接收或者存储的信息。

[GB/T 36320-2018，定义 3.9]

3.2

电子合同 electronic contract

当事人之间通过电子信息网络、以电子的形式达成的设立、变更、种植民事权利义务关系的合同。

3.3

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加而形成的分布式账本。

3.4

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。

[T/CESA 1048-2018，定义 3.1.4]

3.5

区块链电子合同存证 electronic contract depository of blockchain

依托区块链数字存证服务为电子合同签约的全过程提供相关数据电文的证据保管和验证服务。

3.6

数字签名 digest 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伪造和抵赖。

注：改写 GB/T 25069-2010，定义 2.1.2。

3.7

数字证书 digital certificate

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。

[GB/T 9387.2-1995，定义 3.3.26]

3.8

电子数据 electronic data

以电子手段生成、发送、接收或者储存的信息。

3.9

加密 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]

3.10

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。

[T/CESA 1048-2018，定义 3.1.15]

3.11

智能合约 smart contract

存储在分布式账本中的计算机程序。

注：智能合约用于程序化的记账或自动化交易执行，其共识执行结果都记录在分布式账本中。

4 缩略语

下列缩略语适用于本文件。

CA：数字证书颁发机构（Certificate Authority）

SaaS：软件即服务（Software-as-a-Service）

SDK：软件开发工具包（Software Development Kit）

5 一般原则

5.1 隐私保护原则

电子合同存证服务方宜列明电子合同存证所需的用户信息，提供简便、可靠、易操作的授权方式和多角色授权机制。电子合同服务各相关方未经用户授权许可，不宜将用户信息泄露给非授权的第三方。

注：法律强制披露的情况不适用于上述原则。

5.2 合规原则

用户在使用电子合同相关服务过程中产生所有用户数据宜采用由国家密码主管部门发布的密码行业标准规定的算法进行加密和签名。

5.3 有效原则

有效性原则包含下列内容：

—— 电子数据存、取证执行各方的身份真实有效，存证证明机构有能力验证电子合同的真实性和有效性；

—— 电子合同存、取证的各个关键时间点宜采用由国家授时机构出具的时间，并使用时间戳技术将上述时间封装后记录在系统中；

—— 所有与合同生成及存储过程有关的电子数据宜有效存证，存证的核验通过公开渠道或平台进行。

5.4 可追溯原则

电子合同的签署过程具备全流程可追溯的特性。可追溯的信息宜包含用户信息、个人或企业授权行为、签署行为、最终合同签署完毕的有效时间及内容、数字签名信息等内容。

5.5 安全原则

安全性原则包含下列内容：

—— 电子合同存证数据和信息宜多份存储，同一合同的数据和信息宜分散存储，并通过去中心化的存证平台将业务系统和存储系统分离；

—— 基于现有平台的除证书信息之外的用户实名信息宜进行二次加密后再存储；

—— 电子合同存证服务提供方宜为用户提供统一的数据共享、查阅和验证存证平台，提供多种数据的共享和多方验证方式，并可对数据进行多源验证。

6 相关方

6.1 概述

区块链电子合同存证相关方一般包含电子合同业务相关方和区块链存证服务相关方。区块链电子合同存证过程中各相关方之间的关系信息见图 1。其中：

a） 电子合同平台相关方通过电子合同平台完成电子合同业务；

b） 区块链数字存证平台内部相关方为电子合同平台输出的电子合同数据提供存证服务，为区块链存证平台提供运营和维护服务；

c） 区块链数字存证平台外部相关方对电子合同平台和区块链存证平台进行监管和授权。

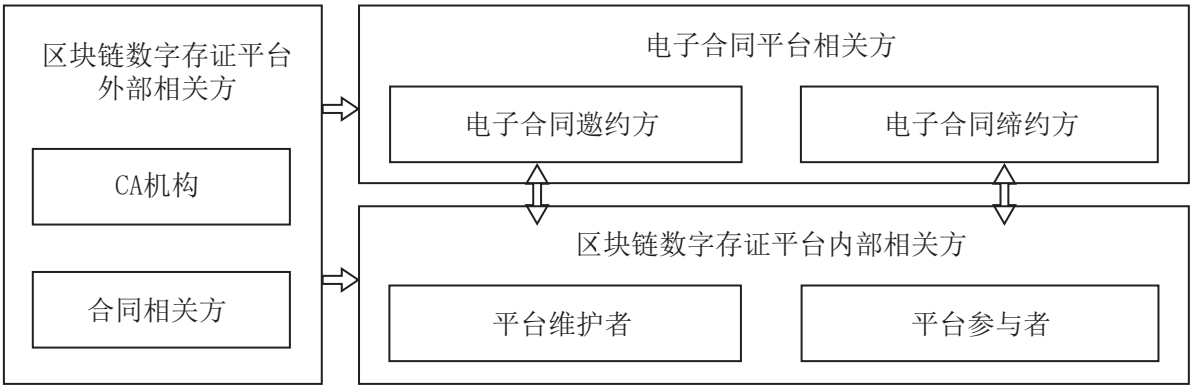


图1　区块链电子合同存证相关方关系

6.2　电子合同平台相关方

电子合同平台相关方包含下列角色：

a） 电子合同邀约方，指在订立电子合同的过程中，发出邀约和接受邀约的一方；

b） 电子合同缔约方，指使用电子合同订立系统的合同当事人。

6.3　区块链数字存证平台相关方

6.3.1　内部相关方

区块链数字存证平台内部相关方包含下列角色：

a） 平台维护者，指平台系统的开发者和维护者；

b） 平台参与者，指平台系统的参与者，为平台系统提供数据存储服务。

6.3.2　外部相关方

区块链数字存证平台外部相关方包含下列角色：

a） CA 机构，指证书授权中心，是电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任；

b） 合同相关方，指订立电子合同和使用电子合同订立系统的合同当事人。

7　存证数据格式

7.1　基本信息

电子合同基本信息宜包含用户注册信息、个人身份信息、企业实名信息、数字证书发放信息、签署意愿存证信息、合同签署信息和系统日志信息。表 1 给出了上述电子合同存证数据信息名称、字段内容和附加内容。

表 1　电子合同存证数据基本信息

名称	字段内容	附加内容
用户注册信息	用户 ID	用户 ID，用户 IP

表 1　电子合同存证数据基本信息（续）

名称	字段内容	附加内容
个人身份信息	姓名、身份证号、手机号和银行卡号	用户 ID，用户 IP，身份证号
企业实名信息	企业名称，企业组织机构代码	用户 ID，用户 IP，企业组织机构代码
数字证书发放信息	CA 证书文件	用户 ID，用户 IP，CA 证书文件名，CA 机构
签署意愿存证信息	手机号、短信文本	用户 ID，用户 IP，合同编号，签署方（甲方、乙方）
合同签署信息	合同文件	合同编号，合同名称，甲方用户 ID、乙方用户 ID
系统日志信息[a]	日志文件	文件名，日志创建日期（YYYY-MM-DD 格式）
[a] 日志创建日期宜采用 GB/T 7408-2005 中 5.2.1.1 的完全表示法扩展格式进行描述。		

7.2　电子合同证书

证书内容包含平台存证编号、存证方、存证内容、存证大小、存证时间、存证哈希、司法机构存证编号、扫码查验等信息。

7.3　电子合同报告

报告内容数据值使用文件名、原始内容和原始哈希散列三种方式表示。

8　电子合同存证关键技术过程

8.1　存证数据上链

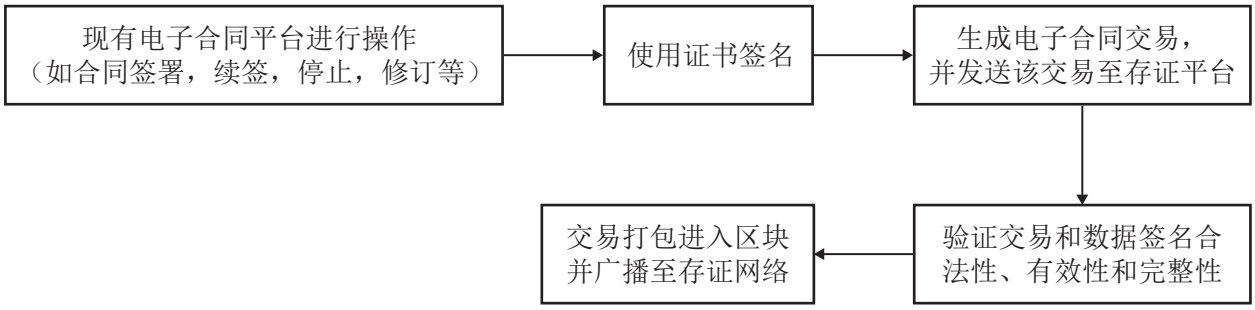


图2　存证数据通过交易方式上链流程

8.1.1　通过交易方式上链

用户或电子合同平台通过存证平台，向特定用户（地址）发起一笔存证交易，该交易由存证平台其他节点验证通过后，打包进入区块，并完成网络同步和存证上链的工作。图 2 给出了通过交易方式将合同数据上链存证的主要流程，包含下列主要步骤：

a）电子合同缔约方通过现有电子合同平台创建账号，完成合同的签署、续签、变更、停止等相关操作；

b） 选择电子合同的证书签名方式，包含本地签署、电子合同平台签署和区块链数字存证平台签署；
c） 生成电子合同交易，并发送该交易至区块链数字存证平台：
1） 生成电子合同交易，通过私钥签名交易和加密对应数据，将该交易上传至区块链数字存证平台；
2） 区块链数字存证平台将交易数据进行加密和离散化处理，生成对应的数据树；
3） 构造一个上传交易，由私钥和电子合同平台私钥共同签署，交易发起方为用户，接收方为所属的电子合同平台。
d） 区块链数字存证平台节点通过用户和电子合同平台的公钥对交易和数据签名的合法性、完整性和有效性进行验证；
e） 如交易和数据验证通过，验证节点生成数据区块，并同步至区块链数字存证平台。

8.1.2 通过智能合约上链

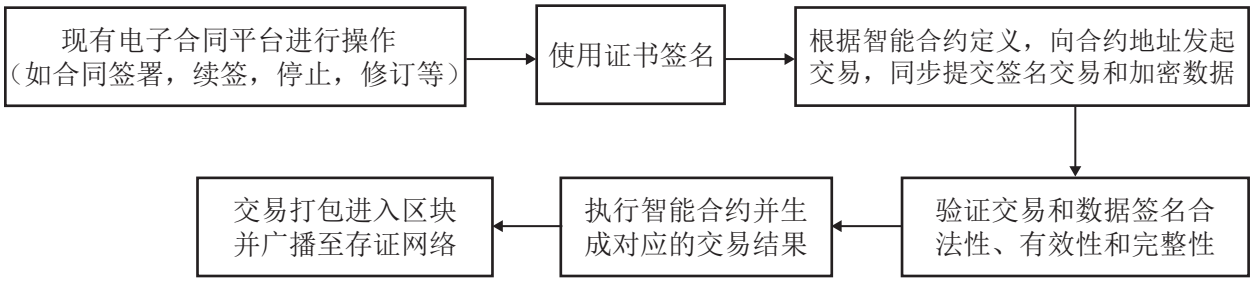


图3 存证数据通过智能合约方式上链流程

智能合约由存证平台或各电子合同平台创建。智能合约的执行宜通过向合约地址发起交易的方式触发。图 3 给出了存证数据通过智能合约方式上链的主要流程，包含下列主要步骤：
a） 电子合同缔约方通过现有电子合同平台创建账号，完成合同的签署、续签、变更、停止等相关操作；
b） 选择电子合同的证书签名方式；
c） 根据智能合约定义，向合约地址发起交易，电子合同平台将该交易数据进行加密和离散化处理，生成对应的数据树；
注：该交易发起方为用户，接收方为对应的智能合约地址，由用户私钥和电子合同平台私钥共同签署。
d） 由电子合同平台将该交易和对应的数据提交至区块链数字存证平台，用户和电子合同平台的公钥对该交易以及数据签名的合法性、完整性、有效性进行验证；
e） 如交易和数据验证通过，验证节点加载对应的智能合约至虚拟机中，将交易相关参数传入智能合约并执行；
f） 将智能合约执行结果生成数据区块，并同步至区块链数字存证平台。

8.2 电子证据托管

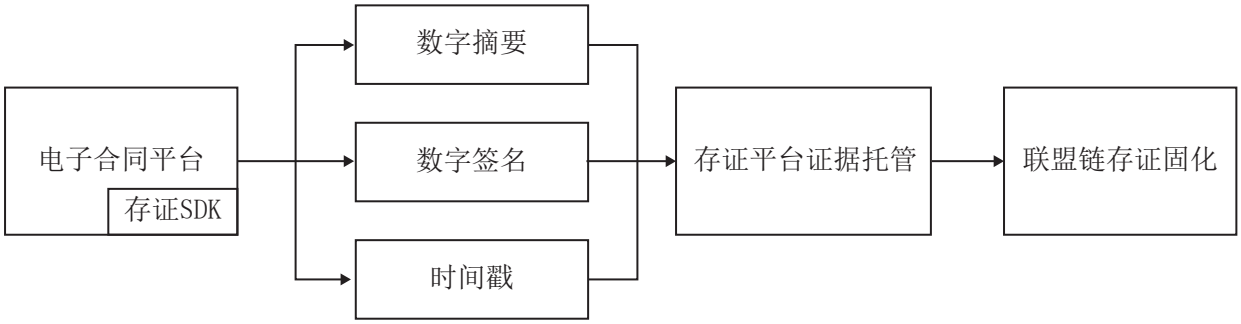


图4 电子证据托管过程

图 4 给出了电子证据托管的关键技术过程，包含下列主要步骤：

a） 电子合同平台在本地集成区块链数字存证平台 SDK，通过调用 SDK 使用存证服务；

b） 电子合同平台调用 SDK，本地生成电子数据数字摘要，使用私钥对数字哈希进行电子签名，并对电子数据加盖时间戳；

c） 将电子证据的数字摘要、数字签名、时间戳数据上传至区块链数字存证平台，平台对这些关键证据托管存储；

d） 电子数据同步至链上，以交易及数据区块的方式固化存证。

8.3 存证数据取证

8.3.1 交易数据取证

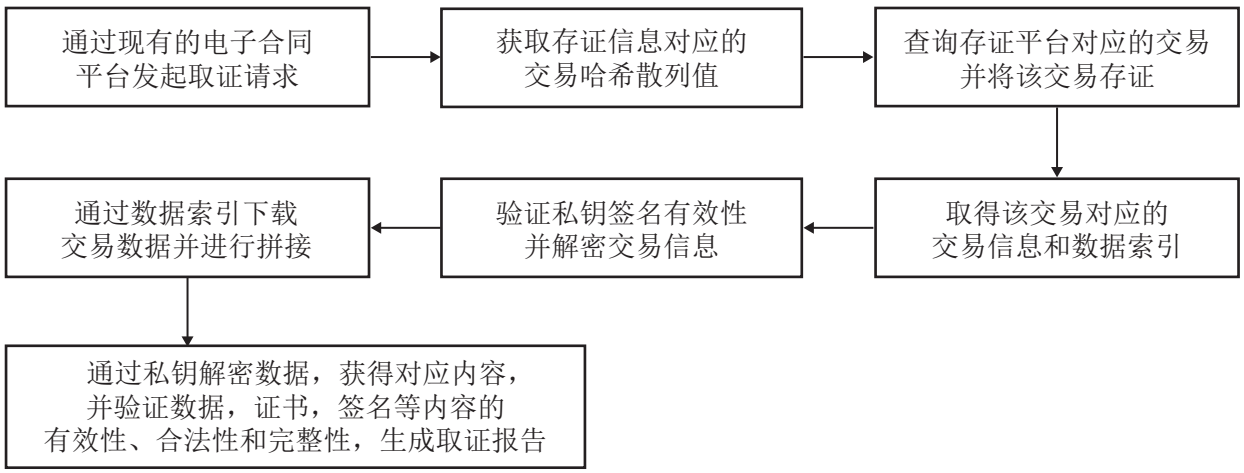


图5 交易数据取证流程

存证数据取证查询宜按照图 5 给出的主要流程进行，包含下列主要步骤：

a） 用户通过现有电子合同平台发起取证请求；

b） 如合同对应的存证信息存放在区块链数字存证平台，则获取存证信息对应的交易哈希散列值；

c） 通过交易哈希散列值在区块链数字存证平台查询对应的交易，获得区块、交易以及对应的数据信息；

d） 取得该交易对应的交易信息和数据索引，通过用户或电子合同平台的私钥信息，验证是否可以解密该交易信息；
e） 验证用户或平台的私钥签名有效性，解密交易信息；
f） 通过数据索引下载从区块链数字存证平台下载交易数据信息并正确拼接；
g） 解密交易数据，验证解密后的交易信息和数据的有效性、合法性和完整性，完成取证工作，并在电子合同平台生成对应的取证报告。

8.3.2 智能合约取证

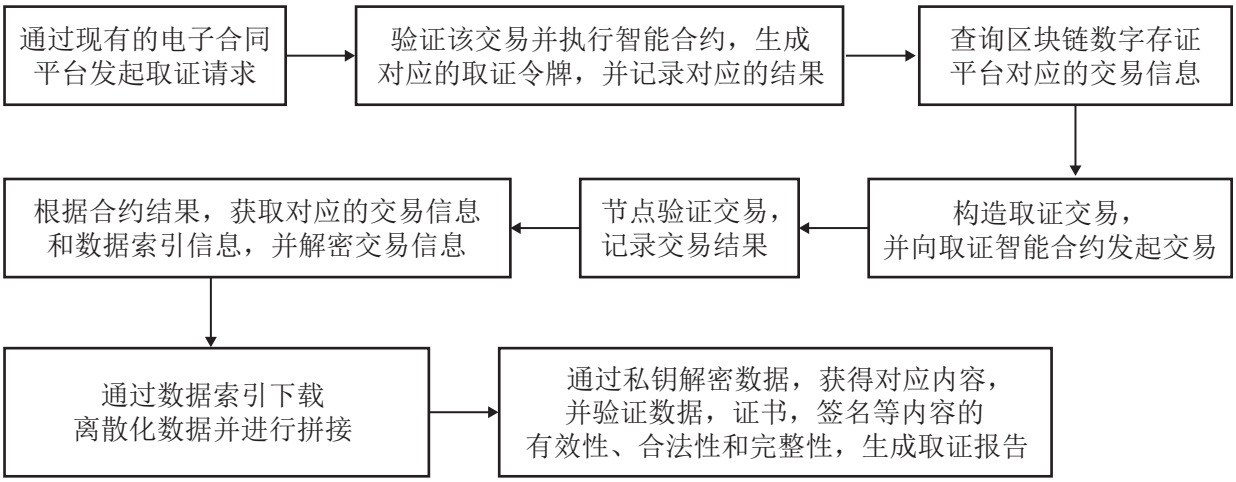


图6 智能合约取证流程

电子合同平台宜提供智能合约用于存证数据的取证工作。图 6 给出了智能合约取证的基本流程，包含下列主要步骤：

a） 构造取证请求，并向取证智能合约发起取证交易；
b） 区块链数字存证平台节点验证该交易并执行智能合约，生成对应的取证令牌，并记录对应的结果；
c） 通过交易哈希散列值在区块链数字存证平台查询对应的交易，获得区块、交易以及对应的数据信息；
d） 构造取证交易，向取证智能合约发起该交易，并在区块链数字平台解密交易信息；
e） 节点验证交易，并按照交易执行对应的取证验证，同时记录交易结果；
f） 根据合约结果获取对应的交易信息数据和数据索引信息，并解密该信息；
g） 通过数据索引从区块链数字存证平台下载离散化数据，并正确拼接；
h） 解密交易数据，验证解密后的交易信息和数据的有效性、合法性和完整性，完成取证工作，并在电子合同平台生成对应的取证报告。

9 电子合同存证关键业务要求

9.1 业务数据存证

业务数据存证宜注意下列要点：

a） 在电子合同业务存证前对存证业务相关方进行身份核验，确保电子数据生成、收集、存储、传输所依赖的硬件、软件及网络环境安全、可靠，并处于正常运行状态；

b） 电子合同业务存证时，存证业务相关方通过区块链节点将电子数据的原文或完整性校验值、附加信息等数据传输至区块链数字存证平台进行存证；

c） 除电子合同本身外，区块链数字存证平台提供记录业务存证时的硬件设备信息、软件系统信息、网络信息及过程数据等功能，计算相关信息的完整性校验值，并将记录的数据与对应的完整性校验值同时进行区块链存证。

注：互联网法院审判和公证处赋强公证是电子合同存证应用的最佳实践之一，详情见附录 A。

9.2 业务存证公示和查询

电子合同业务存证的公示和查询宜注意下列要点：

a） 支持以网站或公共接口方式进行公示和查询；

b） 公示体现真实的存证数据，授权用户可通过区块链网络中的节点进行查询验证。

9.3 业务存证提取

提取的电子合同业务存证宜从区块链网络上直接获取。提取存证时：

a） 确保取证过程所依赖的硬件、软件及网络环境安全、可靠；

b） 电子合同平台支持将提取过程重现的功能，提取过程的记录按时间先后连续排列；

c） 确保提供的电子合同存证证书或存证报告符合第 7 章的要求；

d） 确保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。

9.4 业务存证验证

区块链数字存证平台宜支持具备相关资质的第三方机构进行电子合同存证的验证。验证时，第三方机构宜：

a） 基于原始数据验证电子数据；

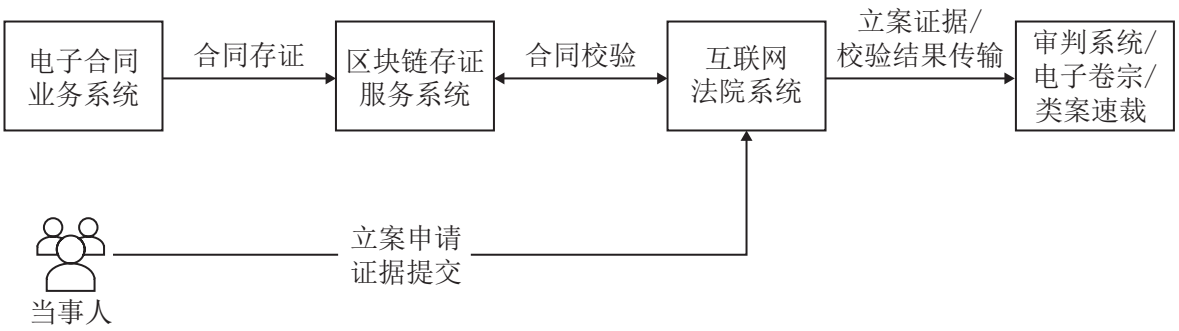
b） 根据特定且公开的算法对电子合同进行验证；

c） 提供相关证明文件。

附 录 A
（资料性附录）
司法延伸服务构建模型

A.1 电子合同区块链存证与互联网法院审判联动模型

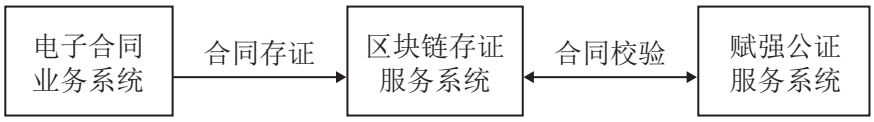
电子合同区块链存证的首要目的是提高当事人纠纷中检验证据真实性的效率。电子合同区块链存证与互联网法院对接联动，可将线下审判的全流程移植至线上，减少电子证据的中间系统过度，规避证据篡改风险。同时，为司法端提供智能证据校验，减少法官判案过程中的工作量，提高司法效率。基于区块链存证和人工智能辅助裁判技术建立的标准产品速裁系统，可以实现标准产品案件批量化处理，实现证据快速提交、核验和裁判，有助于法院快速批量处理类案，加快债务清收和呆账释放，引领司法创新。图 A.1 给出了司法存证模型的业务模型。



图A.1 司法存证模型

A.2 电子合同区块链存证与公证处赋强公证联动模型

赋强公证具有从源头控制纠纷产生，减少法院诉源的作用，但是其中的重要环节是相关证据的现状固定，作为发生纠纷时的重要根据，达到预防纠纷的目的。在赋强公证服务中，使用区块链技术对电子合同签署时的状态进行存证，可以保证赋强公证中的链上证据真实有效。图 A.2 给出了公证处赋强公证的业务模型。



图A.2 赋强公证存证模型

参 考 文 献

[1] GB/T 9387.2-1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构
[2] GB/T 25069-2010 信息安全技术 术语
[3] GB/T 36298-2018 电子合同订立流程规范
[4] GB/T 36319-2018 电子合同基础信息描述规范
[5] GB/T 36320-2018 第三方电子合同服务平台功能建设规范
[6] SF/T 0076-2020 电子数据存证技术规范
[7] T/CESA 6001-2016 区块链 参考架构
[8] T/CESA 1048-2018 区块链 存证应用指南
[9] 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）
[10] 中华人民共和国电子签名法
[11] 中华人民共和国密码法

CBD-Forum-003-2020

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