ICS
A 11

团　体　标　准

T/CIIA XXX—XXXX

区块链司法存证技术要求

Technical Requirement of Blockchain Juditial Evidence Preservation

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国信息协会　　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。

本文件由中国信息协会归口。

本文件起草单位： 国家信息中心电子数据司法鉴定中心、中国政法大学电子证据研究中心、中金金融认证中心、上海零数众合信息科技有限公司、腾讯云计算（北京）有限责任公司、北京天德科技有限公司、中国科学院国家授时中心、北京国信京宁信息安全科技有限公司。

本文件主要起草人：杨绍亮、王笑强、蔡维德、毛立明、张羽、王佳慧、王立梅、杜春鹏、马春旺、兰春嘉、易威、由凯、王自冲、刘波、王磊、杨珍、邓恩艳、马聪磊、苟军、华宇、刘云松、宋欣明、杨冬。

引　言

区块链司法存证技术要求

1 范围

本文件规定了区块链上链前电子数据的采集固定，区块链平台用于司法存证的可信共识算法特征、节点管理、智能合约管理、数据安全存储的内容，数据上链流程，以及区块链存证数据的验证、鉴定等。。

本文件适用于采用区块链技术对电子数据进行存证，及对区块链存证数据进行司法鉴定和审验的系统可靠性测试和证明力验证。

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，仅所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。

SF／T 0076-2020　　电子数据存证技术规范

GB／T 25069-2022　　信息安全技术 术语

GB/ T 35285-2017　　信息安全技术公钥基础设施基于数字证书的可靠电子签名生成及验证技术要求

GB/T 42752-2023　　区块链和分布式记账技术参考架构

GB/T 22239—2019　　信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子数据 Electronic Data

通过电子邮件、电子数据交换、网上聊天记录、博客、微博客、手机短信、电子签名、域名等形成或者存储在电子介质中的信息。

[来源：《最高人民法院关于适用<中华人民共和国民事诉讼法>的解释》第一百一十六条]。

3.2

电子签名 Electronic Signature

电子数据中以电子形式所含、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。

[来源：GB/T 25069-2022 ，3.119]

3.3

可信时间标识 Trusted Timestamp

基于可信时间源的唯一地标识某一刻客观时间的字符序列。

3.4

电子数据固定 Electronic Data Preservation

为防止电子数据被篡改或者破坏，使用散列算法等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值

［来源：《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》］

3.5

区块链 Blockchain

一种将数据区块顺序相连，并通过共识协议、数字签名、散列算法等密码学方式保证的抗篡改和不可伪造的分布式账本。

［来源：信息安全技术 区块链技术安全框架（征求意见稿），3.2，有修改］

3.6

节点 Node

具有特定功能的区块链组件，可独立运行的单元。

3.7

共识 Consensus

在分布式节点间达成区块数据一致性的认可。

［来源：信息安全技术 区块链技术安全框架（征求意见稿），3.7］

3.8

共识协议 Consensus Protocol

区块链中通过数学算法实现不同节点之间对记账内容达成一致的方法，是区块链确认世界状态，节点间建立信任、协同合作的基础。

［来源：信息安全技术 区块链技术安全框架（征求意见稿），3.9］

3.9

拜占庭容错 Byzantine Fault Tolerance

通过使用拜占庭将军一致性共识协议，恶意或失效节点的数量不超过总结点数量的三分之一，区块链系统仍然可以维持一致性。

［来源：区块链共识安全技术测评标准］

3.10

智能合约 Smart Contracts

智能合约是代码存储、部署、并且执行在区块链系统上，其执行结果记录在区块链系统内。

3.11

区块链司法存证 Blockchain Evidence Preservation

为保证信息的完整性和真实性，实现司法证明力，采用区块链技术实现多节点共识的电子数据存证。

3.12

区块链司法存证服务提供者 Blockchain Electronic Evidence Preservation Service Provider

提供区块链电子数据存证服务的机构或组织。

3.13

区块链司法存证服务使用者 Blockchain Electronic Evidence Preservation Service Users

使用区块链电子数据存证（验证）服务的组织或个人。

3.14

区块链司法存证平台 Blockchain Electronic Evidence Preservation Platform

由区块链电子数据存证服务提供者向其使用者以网站、应用程序和编程接口等形式提供区块链电子数据存证服务的软件或系统。

3.15

区块链浏览器 Blockchain Browser

区块链浏览器是链上数据可视化的主要窗口。它可以记录和统计区块链网络的每个区块、每笔交易以及地址等信息。

3.16

代码坏味道 Code Smells

低质量代码的典型特性，例如重复代码(duplicated code)、长函数(long method)、过大的类（large class）。代码有坏味道，代表代码质量可能有问题。

3.17

检材数据 Evident Data

作为司法鉴定检材提交的电子数据。

4 缩略语

下列缩略语适用于本文件。

API	应用程序接口	Application Programming Interface
SDK	认证机构	Software Development Kit

5 总体系统功能与应用逻辑要求

5.1 区块链司法存证系统框架

区块链司法存证系统主要包括五层：资源层、区块链底层平台、中间层、业务层以及用户层，具体如下图1所示。

图1 区块链司法存证系统框架

区块链司法存证系统每层需包含的功能或服务：

a)资源层应为系统提供网络资源、存储资源以及计算资源；

b)区块链底层平台应包括共识算法、加密算法、节点管理、区块链浏览器、智能合约、合约管理以及权限管理等功能；

c)中间层应为区块链底层平台和业务应用层之间或为其他系统提供必要的API接口、数据上链SDK以及RPC指令封装控制等；

d)业务层应支持数据采集、数据存储、数据管理、账户管理、监管审计、数据查询、数据核验等功能，宜支持数据电文保存、数据电文原件固定等功能；

用户层应支持不同类型用户的使用，如法院、仲裁机构、鉴定机构、律师事务所等；

e)区块链的具体技术架构应满足GB/T 42752-2023的要求。

5.2 应用逻辑框架

电子数据原件在固定、传输并存证到司法区块链存证平台上，用户在平台上可查询已授权的数据，也可以通过核验电子数据原件的散列值，来确定数据的存在性，以及是否被篡改。应用逻辑框架如下图2所示。

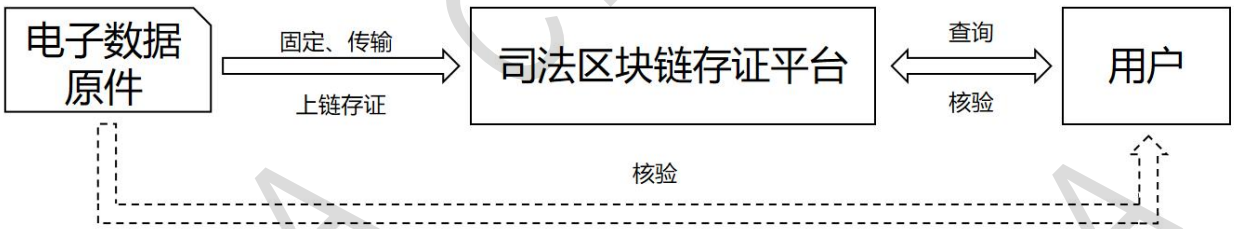

图2 应用逻辑框架

6 区块链电子数据上链前要求

6.1 电子数据原件的保存

6.1.1 通常性要求

电子数据在进行区块链电子数据存证前，其生成、收集、传输、存储电子数据的软、硬件及网络环境应满足以下条件：

a) 生成、收集、传输、存储电子数据的软、硬件及网络环境安全、可靠且处于正常运行状态；

b) 生成、收集、传输、存储电子数据的软、硬件及网络环境应有制定相关的管理制度并由专人管理。

6.1.2 电子数据的形态

电子数据可为用户注册数据、身份认证数据、意愿认证数据、合同签署数据、电子交易记录、日志操作数据、多媒体图片音频视频数据等，包括但不限于：

a) 用户注册数据：包括但不限于账户名称、密码、注册时间等；

b) 身份认证数据：包括但不限于姓名、企业名称、身份证号、统一社会信用代码、银行卡号、手机号、验证码等；

c) 意愿授权数据：包括但不限于意愿授权方式、授权人名称、授权人证件号码、授权时间、IP地址、意愿授权结果等；

d) 合同签署数据：包括但不限于签署人信息、签署时间、IP地址、数字证书信息、签署的文件等；

e) 电子交易记录：包括但不限于交易人信息、交易金额、交易时间、交易流水号等；

日志操作类数据：包括但不限于系统日志、应用程序日志、数据库日志、登陆日志、操作日志、安全日志、接口日志等；

f) 多媒体图片音频视频数据：包括但不限于文本、图片、音频、视频、数字证书、计算机程序等；

其他数据：包括但不限于完整性校验值、取证记录等信息。

6.1.3 电子数据的生成

电子数据在进行区块链电子数据存证前，对于电子数据的生成应满足：

a) 电子数据应以物理隔离的形式脱离原业务系统存储，同时具备冗余存储机制；

b) 由具备电子数据司法鉴定资质的第三方检测机构对电子数据生成环境的安全性和业务合规性进行检测评估，并出具检测报告。

6.1.4 电子数据的收集

在提供区块链电子数据存证服务前，区块链电子数据存证服务提供者应验证该服务使用者的身份。在使用区块链电子数据存证服务前，区块链电子数据存证服务使用者收集电子数据的内容及方式应符合相关法律法规，同时满足合法、正当、必要、诚信原则，且应当限于实现处理目的最小范围，此外，对于电子数据的收集还应满足：

a) 收集电子数据时应使用可靠的电子签名；

b) 收集电子数据时应使用权威的可信时间标识。

6.1.5 电子数据的传输

电子数据在进行区块链电子数据存证前，对于电子数据的传输应满足：

a) 在传输电子数据前，应鉴别电子数据收集者（或发送者）、电子数据存储者（或接收者）身份；

b) 在传输电子数据前，应对电子数据明文进行加密处理，在传输时应使用双向TLS协议进行加密通讯；

c) 在传输电子数据时，应记录电子数据收集者（或发送者）、电子数据存储者（或接收者）信息；

d) 在传输电子数据后，应将电子数据加密或散列值计算后实时推送至区块链系统。

6.1.6 电子数据的存储

电子数据在进行区块链电子数据存证前，电子数据的存储，应包含以下信息：

a) 电子数据的唯一标识码；

b) 电子数据对应的完整性校验值和完整性校验算法，当需要进行原文存证的，还需要包含电子数据原文；

c) 电子签名、可信时间标识的信息；

d) 操作日志、访问日志、系统间交互日志等；

e) 电子数据存储的硬件设备信息、软件系统信息、网络信息及其他过程信息，并计算相关信息的完整性校验值；

此外，电子数据的存储还应满足如下要求：

f) 存储电子数据的同时，应存储电子数据收集者（或发送者）、电子数据存储者（或接收者）的身份信息；

g) 对于经权威第三方数据服务提供者鉴别、校验或验证的电子数据，应存储该第三方数据服务提供者信息，验证结果，验证时间等；

电子数据的存储宜在司法机关、司法鉴定中心、公证处、电子认证服务机构等权威机构进行备份。

6.2 电子数据原件的固定

6.2.1 电子数据固定方法

电子数据在进行区块链电子数据存证前，应对电子数据进行固定，其固定方法应满足以下要求：

a) 使用可信时间标识；

b) 使用可靠的电子签名及获取用于校验数据完整性的数据值。

6.2.2 电子数据固定要求

对电子数据进行固定的要求包括以下：

a) 对电子数据原件及涉及电子数据生成、收集、传输、存储的关键节点数据，相关主体应使用可靠的电子签名进行固定；

b)所固定的电子数据应能组成完整的证据链，其中包含的可靠的电子签名应可被验证。

6.2.3 可信时间标识

可信时间标识应满足以下要求：

a)可信时间标识应能标记电子数据固定时的客观准确时间；

b)可信时间标识所采用的时间应溯源于国家认可的法定授时机构；

c)可信时间标识所采用的时间应使用国家法定授时机构认可的硬件和方法获得；

d)可信时间标识对密钥的使用应遵照国家密码管理主管部门有关规范执行；

e)用于电子数据固定的可信时间标识，在算法及密钥长度上还应满足：

—— 所使用的摘要算法应为符合相关国际、国家标准；

—— 所使用的非对称加密算法应为符合相关国际、国家标准的RSA、SM2或ECC算法；其中，RSA算法密钥长度应不低于2048位，SM2、ECC算法密钥长度应不低于256位。

6.2.4 电子签名

用于电子数据固定的电子签名应满足以下要求：

a)使用具有资质的电子认证服务机构颁发的数字证书进行签名；

b)数字证书属电子签名人专有，且仅由电子签名人控制；

c)电子签名由数字证书的持有者所签署，且签名者的身份能被鉴别；

d)签名时所使用的数字证书在有效期内，且未处于冻结或吊销状态；

e)签名后对该电子数据原件和电子签名未进行任何形式的改动，且任何形式的改动都能被发现。

具备资质的电子认证服务机构，应满足以下条件：

—— 具有国务院信息产业主管部门颁发的电子认证服务许可证；

—— 具有国家密码管理主管部门颁发的电子认证服务使用密码许可证；

—— 企业正常经营，相关资质处于有效期内；

—— 法律、行政法规规定的其他条件。

用于电子签名的数字证书，在算法及密钥长度上还应满足：

—— 所使用的摘要算法应为符合相关国际、国家标准的SHA256、SHA512、SM3算法；

—— 所使用的非对称加密算法应为符合相关国际、国家标准的RSA、SM2或ECC算法；其中，RSA算法密钥长度应不低于2048位，SM2、ECC算法密钥长度应不低于256位。

6.2.5 可信时间标识的验证

对于电子数据固定中使用的可信时间标识，对其合法性、有效性的验证应还包括以下内容：

a)可信标识可以被验证采用的时间源来自可信时间源；

b)验证可信时间标识所使用的摘要算法、非对称加密算法及密钥长度，满足5.2.3 之要求；

c)法律、法规规定的其他要求。

6.2.6 电子签名的验证

用于电子数据固定的电子签名的验证流程应遵循GB/T 35285-2017的规定，包含签名人文件的完整性验证过程、验证数据的签名策略符合性验证过程、相关证书及验证数据的有效性验证过程以及验证结果输出过程。

对于电子数据固定中使用的电子签名，对其合法性、有效性的验证应还包括以下内容：

a)验证电子签名所使用的数字证书，由具有资质的电子认证服务机构颁发；

b)验证电子签名所使用的数字证书，其摘要算法、非对称加密算法及密钥长度，满足5.2.4之要求；

c)验证电子数据中所附的电子签名是否被改动；

d)验证电子数据的内容及形式是否被改动；

e)法律、法规规定的其他要求。

7 司法区块链系统与存证平台技术要求

7.1 司法区块链系统技术要求

7.1.1 共识协议

共识协议需满足如下功能：

a)在共识流程中所有的通信过程都需要使用加密解密技术并通过数字签名技术进行签名并验签，节点间通信使用的加密协议应参考TLS协议，即节点间的通信信息使用对称加密算法进行计算，对称加密算法的秘钥使用非对称加密算法进行加密传输。

b)各参与节点应对区块链网络提交的所有信息进行有效性验证（描述数据遵循预定的语法规则的程度，是否符合其定义，比如数据的类型、格式、取值范围等），只有通过验证的信息数据才能继续进行其他区块链步骤。没有通过的信息数据将被系统拒绝；

c)各参与节点应对区块链系统提交的所有信息数据进行拜占庭将军共识协议检验。只有通过拜占庭将军协议一致性验证的信息数据才可写入区块链系统内；

d)具有公信力机构加入到共识或验证节点，维护系统的公信力；

e)支持至少一种满足拜占庭容错的共识协议；

f)使用满足拜占庭容错的共识协议来维持每个节点的数据一致性，使用的协议必须至少有3个阶段以及两轮投票[1]。

7.1.2 合约管理

合约管理需满足如下功能：

a)智能合约应经电子数据司法鉴定机构验证后部署到区块链上。该智能合约验证测试结果记录在区块链系统上；

b)应支持对智能合约的全生命周期的管理，如创建、编译、测试、部署、升级、冻结、解冻、废止等；

c)应支持智能合约安全审计，如智能合约漏洞分析、静态分析（智能合约代码分析）、软件测试技术等；

d)智能合约计算结果经共识后上链存证。

7.1.3 加密算法

加密算法支持如下功能：

a)应支持国际主流加密算法，如AES256、RSA（最低2048位）、ECC（256）、SHA256等，其中RSA的密钥长度不低于2048比特，ECC的密钥长度不低于256比特，SHA256摘要长度不小于256比特。

b)应支持我国商密算法，如SM2、SM3、SM4等；

c)应具备明确的密钥管理方案；

d)应至少有一种保护密钥存储安全的机制；

---

1) 例如 PBFT 协议为 3 阶段协议，CBFT 协议为 4 阶段共识协议，Tendermint 协议为 3 阶段协议，Hotstuff 协议为 4 阶段共识协议。少于 3 阶段投票的共识算法只能维持数据库一致性，不能支持拜占庭容错机制，安全性差，不能使用在司法区块链系统内。

e)共识过程中加密算法选择，其中对称加密算法应选择SM1或SM4等国密算法。非对称加密算法应选择SM2国密算法。数字（摘要）使用SM3国密算法。

7.1.4 节点管理

节点管理功能需满足如下要求：

a)应支持增加、删除、更新节点；

b)应支持节点的权限分配；

c)应支持对节点的资源配置；

d)应支持节点网联状态监控。

7.1.5 区块链性能

区块链的性能应满足如下要求：

a)区块链交易延迟应小于2秒；

b)区块链交易处理的吞吐量应大于1000交易/秒。

7.1.6 唯一性标记与追溯

应支持通过唯一性协议对具有唯一特性的非同质化权益数据进行标记和追溯。

7.1.7 区块链网络

应至少由4个节点组成。

7.2 存证平台技术要求

7.2.1 基础功能

存证平台应具有如下基础功能：

a)应确保链上数据不可篡改、伪造，保证数据的完整性、真实性；

b)应支持存证数据的查询、管理数据的查询；

c)应支持平台数据、链上数据以及日志的监管审计；

d)应支持多方存证、取证和相互验证；

e)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。

7.2.2 数据管理能力

区块链司法存证平台应具备链上数据管理能力，包括但不限于于以下内容：

a)应支持对数据的权限控制能力；

b)支持基于目录、关键词、区跨链地址的检索查询；

c)应支持根用户链上数据遍历能力；

d)在数据传输过程中，应支持数据的完整性、保密性以及真实性；

e)应支持对数据全生命周期的审计，包括存储、申请、审批、授权等；

f)支持链上数据批量导出。

7.2.3 账户管理能力

区块链司法存证平台应具备链上账户管理能力，包括但不限于于以下内容：

a)支持创建、冻结、解冻账户等功能；

b)支持为用户设置不同的权限，且按照权限最小化、相互制约原则为账户分配访问权限；

c)支持用户身份标识唯一和鉴别信息复杂度校验功能；

d)使用符合国家密码管理规定的非对称加密算法公钥进行身份认证。

8 上链存证与查询核验技术要求

8.1 上链流程

上链前准备：系统收到任何数据后，有相关人员或系统先进行电子数据真实性验证，验证人员需要签名，记录验证方式，验证得到的结果。验证结果不论通过没有都将相关数据上链。

上链过程：任何数据上链时，都要经过区块链系统的数据加密/解密，签名验证，拜占庭将军协议共识，数据存在区块链系统内，在一般情形下，数据自动加密然后分片，存在不同容错服务器上，保障数据安全。

8.2 区块链系统验证

a)区块链共识机制验证，具备拜占庭将军协议，不只是数据库一致性协议；

b)系统不存在中心节点，轮流移除少量部分节点（所有少量节点组合都要覆盖到），区块链系统也不瘫痪[2]；

c)司法数据区块链系统上链过程应支持数据保密处理、身份验证。

d)区块链系统内数据没有被篡改；

e)静态分析区块链系统的软件代码，软件源代码检验，BUG（软件错误）为零，代码漏洞为零，坏味道可以包容。BUG和代码漏洞必须移除后才能使用。

8.3 查询与权限管理方式

a)所有查询流程：发起请求，提供请求人身份信息以及权限，司法区块链平台核验请求，包括验证用户身份和权限，返回符合权限的数据；

b)查询数据应包括原始数据、散列值、时间戳等数据；

c)区块链系统应当提供存证数据的统一查询验证接口、在线查询验证功能页面及区块链浏览器，以供查询或是验证相关上链信息；

d)区块链电子数据存证服务使用者仅可查询或验证其权限内的相关数据。

9 区块链司法鉴定数据检材要求

9.1 基本原则

区块链存证以司法鉴定实施做为整个服务的闭环，通过标准的司法鉴定程序将商业化存证数据转化为具有法律效力的电子证据。从证据审查角度，应遵循如下基本原则：

a)真实性： 保证鉴定实施数据来源可信，且经过鉴定证明数据在存证未发生篡改。

b)合法性： 整个鉴定实施过程必须按照法定程序操作，强调对过程的依法依规管理。

c)关联性： 对数据内容的解析，强调同权属方、责任方的权利义务关系。

9.2 实施要求

2) 如果瘫痪，表示有中心节点存在。即使系统提供方认为没有，而实际系统却显示中心化设计。

检材数据指为开展司法鉴定工作，经由区块链存证系统中导出并提交至司法鉴定中心的相关电子数据。

a)检材数据的取得和提交应按照标准的程序规范，符合《司法鉴定程序通则》规范性引用文件所要求的相关法定条件。

b)检材数据应当按照特定场景或系统事前评估所确定的字段、格式等要求进行导出和封存，并按照标准鉴定程序提交至鉴定中心。

c)鉴定中心对封存提交的检材数据，在核验数据来源的基础上，可通过时序分析和比对验证等方式对数据的原始性、完整性进行检验，并出具相应鉴定报告。

d)鉴定报告中应当对检材数据的真实性、完整性形成明确意见，并基于对来源和内容的检验，明确数据的关联性和对应的权属关系。

10 平台信息数据安全

10.1 系统安全

存证服务提供平台应达到GB/T 22239—2019信息安全技术 网络安全等级保护基本要求 的第三级基本要求，应具备以下要素：

a)所使用的物理设备及环境有完善的监控体系，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应具有防护措施和应急预案；

c)定期检测评估，防止网络攻击、病毒和非法网络代理的使用。

d)应遵循《区块链信息服务管理规定》具备应急处置方案和能力。

10.2 存储安全

存证服务提供平台存储服务确保存储安全，应具备以下要素：

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)支持敏感信息加密存储，并具备访问控制措施；

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)支持高效、安全、稳定地提供数据写入、持久化及查询服务；

e)支持数据隔离存储；

f)支持防止数据被篡改、伪造。

10.3 传输安全

存证服务提供平台应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，应具备以下要素：

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，只有预期接受者才能读取数据；

c)支持数据传输过程不可篡改、删除、伪造、丢失，确保数据的完整性；

d)接口及系统配置应安全可靠，避免系统代码被反编译或篡改；

e)防止中间人攻击，通信过程进行证书真实性、有效性检验。

附 录 A

附 录 B（资料性）

附 录 C附录名称

参 考 文 献

[1] GB/T 39321-2020 电子合同取证流程规范
[2] 20173824-T-469 信息技术 区块链和分布式账本技术 参考架构（征求意见稿）
[3] 20210991-T-469 信息安全技术 区块链信息服务安全规范（征求意见稿）
[4] 20210998-T-469 信息安全技术 区块链技术安全框架（征求意见稿）
[5] 《人民法院在线诉讼规则》 2021.6 最高人民法院
[6] 《最高人民法院关于互联网法院审理案件若干问题的规定》 2018.9 最高人民法院
[7] 《中华人民共和国电子签名法》 2004.8 全国人民代表大会常务委员会
[8] 《最高人民法院关于适用<中华人民共和国民事诉讼法>的解释》 2022.4 最高人民法院
[9] 《最高人民法院关于加强区块链司法应用的意见》 2022.5 最高人民法院
[10] 《区块链信息服务管理规定》 2019.1 国家互联网信息办公室
[11] 《北京互联网法院天平链应用接入技术规范》 2019.12 北京互联网法院
[12] 《北京互联网法院天平链应用接入管理规范》 2019.12 北京互联网法院