

电 子 商 务 团 体 标 准

T/ZEA 005—2020

电子商务商品交易信息区块链存取证平台 服务规范

Specifications of evidence collection service platform for e-commerce
product transaction information based on blockchain

2020 - 5 - 8 发布

2020 - 5 - 8 实施

浙江省电子商务促进会 发布

目 次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 建设原则.....	2
5 平台架构和功能框架.....	3
6 功能基本要求.....	4
附录 A.....	9

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的部分内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准由浙江省商务厅提出并归口。

本标准主要起草单位：浙江省电子商务促进中心，杭州趣链科技有限公司，浙江大学区块链研究中心，浙江省区块链技术研究院，浙江省标准化研究院，浙商银行股份有限公司，浙江之江企业征信服务有限公司，杭州天谷信息科技有限公司。

本标准主要起草人：蔡亮、沈霞俊、李伟、陈晓丰、郑佩玉、施珍、周莹、谢杨洁、张帅、施进、宋士正、杨国正、臧铖、周益群。

电子商务商品交易信息区块链存取证平台服务规范

1 范围

本标准规定电子商务商品交易信息区块链存取证平台服务的建设原则，平台架构和功能框架，以及基本功能要求。

本标准适用于指导区块链服务供应商结合电子商务商品存取证业务，设计和开发基于区块链的存取证平台，同时也为需要存取证服务的用户提供选择依据和参考。

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。

3 术语和定义

以下术语和定义适用于本文件。

3.1

区块链 blockchain

区块链是一项新型的分布式技术，核心内容包括对等网络、共识机制、分布式存储、点对点传输等技术，具有去中心化、防篡改、可追溯的特性。

3.2

上链 on-chain

业务相关方向区块链系统发起一次请求，区块链节点将相关数据写入到区块链系统中。

3.3

哈希 hash

数据的“指纹”，数据经哈希算法的输出。通过哈希算法可将任意长度的输入计算成固定长度的输出，且输出具有工程意义上的唯一性和不可逆性。

3.4

校验 verify

通过对待校验的数据内容进行哈希计算，并将其与区块链系统中存储的哈希进行对比，确认数据是否与上链时一致。

3.5

私钥 private key

由系统向用户发放用于签名的一串数据。

3.6

私钥签名 private key signature

用户提供的私钥与系统保存的公钥进行匹配，匹配通过后用私钥对交易数据进行签名，系统使用对应公钥进行验签。

3.7

取证人 evidence collector

使用区块链存取证服务进行存取证的用户即取证人。

3.8

网页取证 webpage witness

对可公开访问的互联网页面进行取证。

3.9

过程取证 process witness

对用户的操作过程进行取证。技术手段上特指提供虚拟机远程桌面供用户使用，对用户的操作过程进行录屏。

3.10

清洁性 cleanability

软硬件以及网络环境安全可控，不存在上下文数据污染，不存在网络挟持，病毒注入等风险。如浏览器隐私模式。

4 建设原则

4.1 完整性

电子商务商品信息区块链存取证平台应包括商品信息的存取证功能、证据管理等，针对每个存取证过程的数据提供上链支持、区块链数据查询支持，且针对每个环节均有详细的功能支持。

4.2 安全性

电子商务商品信息区块链存取证平台应提供覆盖商品信息数据存储、传输等过程中的安全机制，确保用户数据的隐私性与安全性，针对系统中的隐私数据、敏感数据、涉及保密的数据都须进行严格加密。

4.3 可用性

电子商务商品信息区块链存取证平台应具备可用性，包括功能完整、流程科学、操作简便等。

4.4 有效性

电子商务商品信息区块链存取证平台应具备有效性，保证获得的存取证信息准确、有效、完整、不失真。

4.5 易拓展性

电子商务商品信息区块链存取证平台应具备易拓展性，包括功能模块的易拓展性与底层区块链平台的易拓展性。

4.6 清洁性

应保证电子商务商品信息区块链存取证平台具有清洁性。

5 平台架构和功能框架

5.1 参考平台架构

平台通过区块链不可篡改性对证据进行有效存证，防止抵赖，平台架构如图1所示：

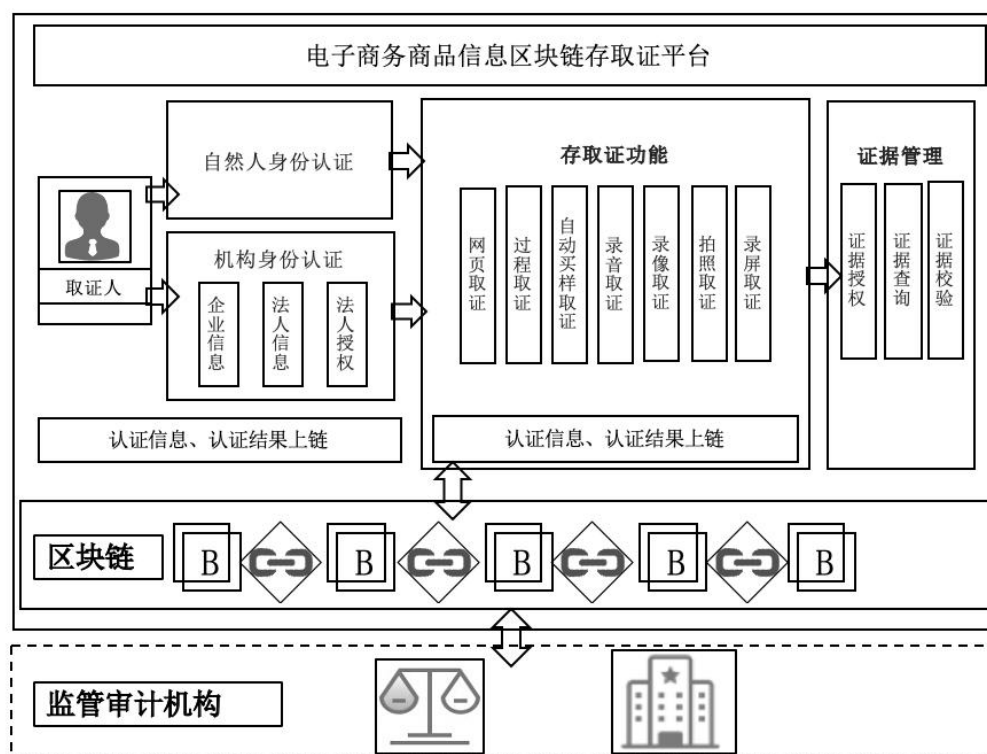


图1 电子商务商品信息区块链存取证参考平台架构

5.2 参考功能框架

电子商务商品信息区块链存取证平台所提供的服务，应针对不同的使用场景，提供不同的存取证服务功能，功能模块应包括区块链管理、用户身份管理、存取证功能、证据管理、系统维护和监管审计等功能。功能框架如图2所示：

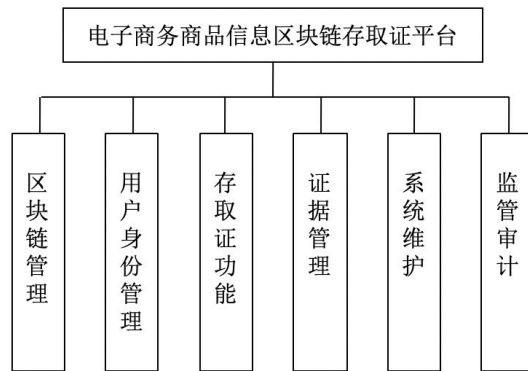


图 2 电子商务商品信息区块链存取证平台参考功能框架

6 功能基本要求

6.1 区块链管理

区块链管理的功能设计应包括区块链数据管理、区块链节点管理、区块链运行监控等。

6.1.1 区块链数据管理

a) 电子商务商品信息区块链存取证平台应支持区块数据管理，支持用户（取证人）查看区块链上区块信息、交易信息等。

6.1.2 区块链节点管理

电子商务商品信息区块链存取证平台应支持区块链节点管理。区块链节点管理功能应包括但不限于：

- a) 支持用户（平台管理人员）新增区块链节点；
- b) 支持用户（平台管理人员）删除区块链节点。

6.1.3 区块链运行监控

电子商务商品信息区块链存取证平台应支持区块链运行状态的监控。区块链运行监控功能应包括但不限于：

- a) 支持对于区块链各节点运行状态的监控，查看节点实时运行状态和所在服务器资源使用情况等；
- b) 支持对区块高度、区块交易信息的监控，使用户可通过图形化界面直观看到区块信息和交易信息。

6.2 用户身份管理

用户身份管理的功能设计应包括注册、认证、私钥发放、信息变更等。

6.2.1 注册

电子商务商品信息区块链存取证平台支持用户进行注册，注册信息上链，身份注册功能应包括但不限于：

- a) 支持对于用户（取证人）身份信息进行注册；
- b) 在用户（取证人）确认提交身份注册申请的情况下，提供对于身份注册信息的审核机制，对身份登记信息的完整性、合法性进行验证；
- c) 支持身份登记过程中上传的所有信息通过私钥签名后进行上链，并反馈给用户此次存储所在的区块以及交易信息；
- d) 支持用户（取证人）查询链上存储的身份信息。

6.2.2 认证

电子商务商品信息区块链存取证平台支持通过身份注册的用户（取证人）进行身份认证，并将认证结果上链。身份认证功能应包括但不限于：

- a) 支持个人用户使用身份证信息进行实名认证；
- b) 支持企业采用统一社会信用代码、营业执照等信息进行实名认证；
- c) 完成认证信息填写并提交时，支持对认证信息的完整性、正确性以及上传附件的格式进行自动审核，如果通过审核，应向用户（取证人）进行告知，如果认证信息及上传附件存在缺失、错误等问题，应向用户（取证人）发出警报；
- d) 支持以站内信或电子邮件等方式向用户（取证人）发送身份认证结果的通知；
- e) 对身份认证结果上链，并反馈给用户此次存储所在的区块以及交易信息；
- f) 支持用户（取证人）查询链上存储的身份认证结果。

6.2.3 私钥发放

电子商务商品信息区块链存取证平台支持通过身份认证的用户（取证人）进行私钥发放。私钥发放功能应包括但不限于：

- a) 支持对认证审核通过的用户（取证人）发放区块链私钥；
- b) 支持区块链私钥的下载，并进行下载权限校验，以确保是用户（取证人）自己进行的下载；
- c) 进行私钥下载时，须提供可靠的加密措施保证下载过程中私钥传输的安全性。

6.2.4 数字签名

电子商务商品信息区块链存取证平台支持通过身份认证且下载过私钥的用户（取证人）进行私钥上传。上传的私钥与平台保存的公钥进行匹配，匹配通过后系统用该私钥对交易进行签名，系统用对应的公钥进行验签，验证通过后可进行上链操作。

6.2.5 信息变更

电子商务商品信息区块链存取证平台支持通过身份认证的用户（取证人）进行认证信息变更。认证信息变更功能应包括但不限于：

- a) 提供对于提出变更申请的用户（取证人）进行更改申请的审核；
- b) 支持对于用户（取证人）的认证信息进行变更；
- c) 支持对于认证信息变更过程中所涉及的相关证明文件进行上传，上传文件应采用较为通用的文件存储格式；
- d) 支持以站内信或电子邮件等方式向用户（取证人）发送认证结果的通知；
- e) 支持将变更申请记录、变更上传的证明文件、以及变更审核结果上链，并反馈给用户此次存储所在的区块以及交易信息；

f) 支持查看区块链上的变更申请记录、变更上传的证明文件、以及变更审核结果。

6.3 存取证功能

存取证管理的功能设计应包括网页取证、过程取证、自动买样取证、录音取证、录像取证、拍照取证和录屏取证等。存取证功能实际应用场景详见附录A。

6.3.1 网页取证

在新增取证时，电子商务商品信息区块链存取证平台应支持网页取证的形式进行新增取证。网页取证功能包括但不限于：

- a) 支持用户（取证人）通过网页取证工具抓取某网页信息，要求网页取证生成包括证据包、截图文件等相关证据；
- b) 支持将网页取证信息通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持用户查询区块链上对应的信息。

6.3.2 过程取证

在新增取证时，电子商务商品信息区块链存取证平台应支持过程取证的形式进行新增取证。过程取证功能包括但不限于：

- a) 支持用户（取证人）远程连接虚拟机，通过虚拟机桌面进行相关操作，电子商务商品信息区块链存取证平台对整个过程进行录屏，要求形成录屏文件等相关证据；
- b) 支持将过程取证信息通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持用户查询区块链上对应的信息。

6.3.3 自动买样取证

在新增取证时，电子商务商品信息区块链存取证平台应支持自动买样取证的形式进行新增取证。自动买样取证功能包括但不限于：

- a) 支持用户（取证人）提交相关买样请求后系统执行自动化程序自动购买目标商品，购买过程进行录屏并形成相关证据；
- b) 支持将自动买样取证信息通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持用户查询区块链上对应的信息。

6.3.4 录音取证

在新增取证时，电子商务商品信息区块链存取证平台应支持录音取证的形式进行新增取证。录音取证功能包括但不限于：

- a) 支持用户（取证人）通过移动终端应用进行录音取证，形成相关证据；
- b) 支持将录音取证信息通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持用户查询区块链上对应的信息。

6.3.5 录像取证

在新增取证时，电子商务商品信息区块链存取证平台应支持录像取证的形式进行新增取证。录像取证功能包括但不限于：

- a) 支持用户（取证人）通过移动终端应用进行录像取证，形成相关证据；
- b) 支持将录像取证信息通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；

- c) 支持用户查询区块链上对应的信息。

6.3.6 拍照取证

在新增取证时，电子商务商品信息区块链存取证平台应支持录音取证的形式进行拍照取证。拍照取证功能包括但不限于：

- a) 支持用户（取证人）通过移动终端应用进行拍照取证，形成相关证据；
- b) 支持将拍照取证信息通过私钥签名上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持用户查询区块链上对应的信息。

6.3.7 录屏取证

在新增取证时，电子商务商品信息区块链存取证平台应支持录屏取证的形式进行拍照取证。录屏取证功能包括但不限于：

- a) 支持用户（取证人）通过移动终端应用进行录屏取证，形成相关证据；
- b) 支持将录屏信息通过私钥签名上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持用户查询区块链上对应的信息。

6.4 证据管理

证据管理的功能设计应包括证据查询、校验、下载等。

6.4.1 查询

电子商务商品信息区块链存取证平台应支持证据查询。证据查询功能应包括但不限于：

- a) 支持用户查询之前存储在区块链上的证据；
- b) 可查询内容应包括但不限于用户的存证数量、存证时间、存证内容、取证记录。

6.4.2 校验

电子商务商品信息区块链存取证平台应支持证据校验，以验证证据的真实性。证据校验功能应包括但不限于：

- a) 支持用户（取证人）使用存证哈希进行校验，检查证据是否和区块链上的数据一致，并告知用户（取证人）证据是否真实；
- b) 支持用户（取证人）使用证据文件进行校验，通过原文对比方式检查证据是否和区块链上的数据一致，并告知（取证人）证据文件是否真实。

6.4.3 授权

- a) 电子商务商品信息区块链存取证平台应支持用户证据授权给他人，方便他人查看。

6.4.4 下载

电子商务商品信息区块链存取证平台应支持证据下载。证据下载功能应包括但不限于：

- a) 支持将用户将存储在区块链的原文证据下载至本地；
- b) 证据下载过程中，应提供可靠的加密方法保证证据传输的安全性。

6.5 系统维护

系统维护的功能设计应包括用户管理、权限管理、日志管理、安全管理。

6.5.1 用户管理

应对使用系统的用户进行统一管理,其功能应包括但不限于:

- a) 支持对人员信息的创建、修改、删除、查询;
- b) 支持对人员信息的创建记录、修改记录、删除记录上链。

6.5.2 权限管理

为实现用户(取证人)使用系统功能的访问控制,保证有效用户正常使用的同时,防止非法用户和无权限用户对系统功能的使用及用户数据的访问,其功能应包括但不限于:

- a) 支持对用户(取证人)的权限进行新增、修改、删除和查询等操作;
- b) 支持设置不同用户(取证人)的访问和操作权限。

6.5.3 安全管理

电子商务商品信息区块链存取证平台的安全管理应遵循《信息安全等级保护管理办法》的相关行业的相关规定,建立完善的数据安全防护机制,在保障可用性的基础上为业务数据提供完整性和保密性。

6.6 监管审计

电子商务商品信息区块链存取证平台应支持监管审计,监管部门和司法部门在职权范围内可以调阅存储在区块链上的各种信息,包括证据信息、取证记录等。

附录 A

(资料性附录)

应用场景

A.1 版权保护

使用区块链对电子商务平台中涉及到的商品版权等信息进行提前登记存证，为商家提供版权保护。发生纠纷后，可以通过查询存证情况，判断原因，解决纠纷。

A.2 侵权取证

商家使用区块链取证工具，对电子商务平台中涉及到侵权的商品进行取证，并以该证据作为侵权行为发生的主要证据，申请维权。

买家用户使用区块链取证工具，对购买过程中产生的纠纷进行相关取证，并以该证据作为商家侵权行为发生的主要依据，申请维权。

A.3 市场监管/监督举报

对于电子商务平台中商家的一系列违法违规行为，例如价格违法、违禁物品出售、虚假宣传等情况，通过区块链取证工具进行取证，作为市场监督、民众举报的证据依据，依据相关固化证据展开定向管理与处罚。
