团体标准

**区块链应用 商品及其流通信息可追溯性要求**

**Block chain application：Requirements of commodity and its circulation information traceability**

(工作组讨论稿)

目  次

前  言

本标准根据GB/T 1.1-2009给出的规则编写。

本标准由中国商业联合会零售供货商专业委员会提出。

本标准由商业联合会归口。

本标准起草单位：

本标准主要起草人：

本标准为首次发布。

区块链应用 商品及其流通信息可追溯性要求

1. 范围

本标准规定了区块链技术在商品流通信息可追溯体系中应用的要求，包括应遵循的原则、应用框架、数据要求、应用支持等内容。

本标准适用于企业的商品信息追溯体系建设，也适用于市场监管部门的监管平台建设。

1. 标准性引用文件

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。

GB/T 36061-2018 电子商务交易产品可追溯性通用规范

CBD-FORUM-001-2017 区块链 参考架构

CBD-Forum-002-2017 区块链数据格式规范

1. 术语定义

下列术语定义适用于本文件。

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，以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]

可追溯性 traceability

对于商品的历史、应用情况或位置情况可以回溯，包括原材料或零部件的来源、生产或加工的历史、物流与销售的情况，以及交付后的分布或所处位置等内容。

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，其实质是基于预定事件触发、不可篡改、自动执行的计算机程序。

数据元 data element

通过定义、标识、表示和允许值等一系列属性描述的一个数据单元。

标识符 identifier

数据元的唯一标识。

对等网络 peer to peer network

一种仅包含对控制和操作能力等效的节点的计算机网络。

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。

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。

活动 action

是指一组特定任务的集合。

1. 应用原则
   1. 合规性原则
      1. 应用区块链技术或提供区块链服务的各方，应遵守国家相关法律法规的要求。
   2. 安全性原则
      1. 区块链技术的应用过程中，应保证信息追溯系统的数据安全和运行安全。
   3. 唯一性原则
      1. 追溯信息的编码和标识应采用国际通用的编码标识技术，或采用已发布的国家标准和行业标准，并具有唯一性。
   4. 网络信任原则
      1. 强调信任源自于商品信息追溯体系的整体，分布于所有的体系参与者。
   5. 隐私性原则
      1. 可以自主决定哪些信息在什么时候、以何种方式、透露多少给其他人。
   6. 权利保护原则
      1. 所有权公开透明且可执行，个体自由是可以被承认和尊重的。
2. 应用框架
   1. 区块链应用于商品信息可追溯体系的基本架构如下：
   2. 数据层
      1. 所需追溯的信息，应以数据的形式存储与数据层。
      2. 所存储数据以数据块的形式，并且建立相互间的链接关系。
      3. 支持链式和图式两类数据存储结构。对于性能要求较高的溯源系统，建议采用图式存储结构。
   3. 网络层
      1. 网络层的主要作用是实现数据交换功能。
      2. 网络层不设中心服务器，通过点对点技术实现各节点的连接和通讯。
   4. 共识层
      1. 共识层的主要作用是实现全网所有节点的数据达成一致，其算法称为共识机制。
      2. 根据算法不同，可以形成不同的共识机制，以适应不同的场景。
   5. 应用层
      1. 通过在智能合约上添加能够与用户交互的前台界面，形成去中心化的应用。
3. 架构视图
   1. 基于区块链的溯源系统采用用户视图、功能视图、实现视图和部署视图等四个不同的视图进行描述。

功能视图

用户视图

部署视图

实现视图

图1 不同架构视图之间的转换

* 1. 用户视图
     1. 用户视图涉及以下内容：活动、角色和子角色、相关方。
     2. 活动需要有一个目标，并能交付一个或多个结果，通过功能组件来实现。
     3. 角色是一组具有共同目标的区块链活动的集合，子角色是某个指定角色的区块链活动的子集。某个角色的区块链活动能被该角色下的不同的子角色所共享。
     4. 相关方是一个或一组自然人或者法人构成的追溯系统的利益相关者。在某个给定时间点，一个相关方可承担多个角色，也可承担某个角色活动的指定子集。
  2. 功能视图
     1. 功能视图是构建溯源系统所需功能的技术中立的视图，描述了支持溯源活动所需功能的分布。
     2. 功能架构定义了功能之间的依赖关系。

图 2 展示了功能、层和**功能组件**的概念.

跨层

功能组件

跨层

层

功能组件

层

功能组件

层

功能组件

* + 1. 功能组件是参与某一活动所需的功能构件，它定义了追溯系统的能力。
    2. 功能架构可部分层次化，即包含多个层和一组跨层功能。
    3. 跨层功能可进行分组。已定义的跨层功能子集包括：开发、运营、安全、监管和审计。
  1. 实现视图
  2. 部署视图
     1. 区块链部署模型是根据对分布式账本的控制和共享方式对区块链进行的分类。
     2. 区块链部署模型包括公有链、联盟链、专有链。

1. 数据要求
   1. 数据运算
      1. 所有数据分析运算可以由网络上的全部节点验证
      2. 不同领域的场景数据生产都能在系统上运作起来
   2. 数据权益保证
      1. 数据作为一种资产，需要有明确的数据所有权、处置权和交易权。
      2. 数据包具有唯一的哈希值，能验证数据的真实性，确认其原始所有权。
      3. 保证数据资产的流通路径公开透明，以及可追溯性。
   3. 数据价值认可
      1. 贡献数据并被应用认可
      2. 贡献数据存储并被网络认可
      3. 贡献数据运算成果并被模型和场景认可
   4. 数据激励机制
      1. 数据交易都记录在分布式账本上，并提供可追溯路径和评价体系。
      2. 评价已完成的数据交易，通过智能合约保护数据贡献者，从经济上确保数据生产和运算质量。
   5. 数据安全分级
      1. 应用多种安全和隐私保护技术。
      2. 根据数据的来源、类型和应用需求，定义不同的数据安全分级模型。
      3. 数据所有者可以根据应用需要方便的定义数据安全等级。
2. 应用支持
   1. 区块链技术服务商
      1. 取得区块链技术服务的相应资质。
      2. 能做到诚信经营。
      3. 专业能力强，包括设计、开发、测试、运维等方面的技术能力。
      4. 综合能力全面，包括商务能力、项目管理能力等。
   2. 区块链平台运营商
      1. 提供区块链平台运营服务的，应当符合下列条件：

* 取得相应的行政许可或资质。
* 有与从事的业务和规模相适应的硬件设施；
* 有保障交易正常运营的网络及信息系统和安全环境；
* 有与平台经营规模相适应的管理人员、技术人员和客户服务人员。
  + 1. 平台经营者应制订和实施平台运营管理制度，并定期检查各方执行情况，并根据结果采取改善措施。
  1. 区块链运营监管方
     1. 对基于区块链的追溯系统及相应的服务商进行必要的行业管理。
     2. 对区块链技术提供培训服务，和职业资质评定。

参 考 文 献

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_