ICS 33.050
CCS M 30

团　体　标　准

T/TAF 101.5-2021

冷链物流可信溯源服务技术要求　第5部分：基于区块链技术实现可信溯源服务的要求

Trusted and traceable service technical requirement for the cold chain logistics—Part 5: Blockchain technology based traceable service requirement

2021-12-13 发布　　2021-12-13 实施

电信终端产业协会　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》的规定起草。

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专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、百度在线网络技术（北京）有限公司、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、四川长虹电子控股集团有限公司。

本文件主要起草人：国炜、徐晓娜、王海棠、吴月升、王婧琦、李汝鑫、陈飞飞、刘献伦、刘为华、康亮、唐博、邓密密、黄德俊。

引　言

当前形势下，冷链物流成为社会关注的焦点，提高其信息化、数字化水平，建立健全其可追溯体系，成为冷链物流发展的新要求。与此同时，区块链技术的发展正在深刻影响着各行业变革，其去/弱中心化、不可篡改的分布式帐本和共识机制的特点，奠定了坚实的“信任”基础和可靠的“合作”机制。基于区块链的以上特点，可将区块链技术与冷链物流全链条安全场景进行有效结合，以提升冷链物流在作业人员、单证/票据、车辆、行为、设备等一系列数据的可信性、防篡改性和可追溯性，为实现冷链物流的数字化、高效化、智能化监管提供强有力的技术支撑与保障。

本文件作为冷链可信溯源服务技术系列规范的一部分，旨在对区块链技术与冷链物流全链条安全场景的结合进行描述，并对区块链技术在输入接入、存储、访问、跨链对接等方面进行技术规范。

冷链物流可信溯源服务技术规范　第5部分：基于区块链技术实现可信溯源服务的要求

1　范围

本文件描述了区块链技术与冷链物流全链条安全场景的结合，并对区块链技术在输入接入、存储、访问、跨链对接等方面进行技术规范。

本文件适用于区块链技术在冷链物流可信溯源服务中的应用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239-2019　信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020　信息安全技术 个人信息安全规范

YD/T 3747-2020　区块链技术架构安全要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

溯源　tracing

从产品追溯到产品的生产流通的各个环节的信息。

3.2

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、防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。

3.3

共识算法　consensus algorithm

区块链系统中各分布的节点对事务或状态的验证、记录、修改等行为达成一致确认的方法。

3.4

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。

3.5

预言机　oracle

连接链上和链下的桥梁。区块链通过预言机来获得所需链下的数据和时间通知。

3.6

上链　cochain

用户向区块链网络发起一次事务请求，将数据存储到区块链网络中。

4　基于区块链技术的冷链物流可信服务

4.1　场景

利用区块链的不可篡改、数据完整追溯以及时间戳等功能，可为冷链物流全链条提供可信溯源服务。典型的结合场景有：

——关键环节采集数据上链：物流关键环节的关键信息可通过终端设备实现自动采集，从而实现物流流程的数字化，提高数据收集效率并减少人为错误。因此，为确保采集设备本身的可信性，将设备出厂的参数信息、质检报告、批次批号以及采集的关键信息上传的区块链上，可增强设备及设备采集数据的信服度。

——作业人员信息上链：作业人员信息将作为合规性的重要一环可以选择上传到区块链，实现作业人员情况的公示与共享，同时可以通过人脸识别等人工智能技术手段校验人员相符，借助电子地图技术验证位置，从而减少不必要的重复审核，加快信息流转速度与可信度，提升流程效率。

——单证、票据信息上链：单证、票据通常包括参与物流作业的人员、公司相关资质的证件信息的备案与存档，对于逾期的证件及时进行识别、提醒与更替，作业票据的留痕与归档等操作，在引入区块链技术后将加速这些单证的流转与追溯效率。

——冷链物流全链条流程溯源：作业流程涉及库内作业与运输作业，可以通过使用区块链技术将作业过程中核心的时间、地点、操作人员、操作行为、操作结果、操作过程等进行统一管理，从而做到流程可追溯、过程可追查的全面覆盖。

4.2　流程

基于区块链技术的冷链物流可信溯源服务流程图如图1所示。

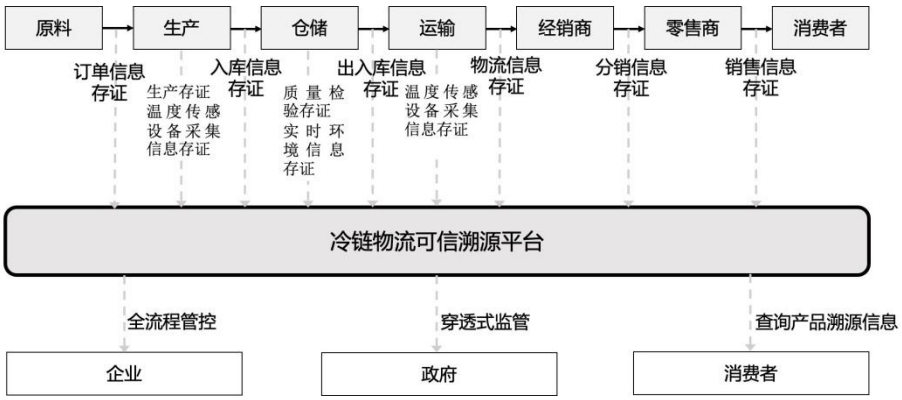

图 1　基于区块链技术的冷链物流可信溯源服务流程图

基于区块链技术的冷链物流可信溯源服务主要包括以下功能：

可信采集：在终端设备部署可信数据上链能力，从根源防范数据安全风险，对经过区块链模组的终端数据进行加密，并与终端设备唯一数字身份绑定，实现数据上链、终端设备统一身份认证和终端设备数据绑定，保障传输过程中数据安全可靠、不可篡改、不可抵赖。

可信存证：冷链物流可信溯源服务打造冷链溯源生态体系，实现原料、生产、仓储、运输、批发、零售等各个环节的生产数据、产品数据、卫星定位数据、冷链物流数据、物流运输过程中温度、湿度、光线等数据、销售信息等经哈希后上链存证，打造可信存证基础设施平台，为溯源提供可信数据支撑。

可信溯源：政府、企业与消费者等可通过冷链物流可信溯源服务查看产品从生产到销售全生命周期信息，同时可与链上存储凭证进行对比，保证信息真实性、有效性。通过冷链全流程数据上链，可有效降低窜货、假冒伪劣等风险，同时提升消费者信任度；通过穿透式的溯源追踪，可打破信息孤岛，帮助企业沉淀全流程数据，便于管理，同时也能提升政府监管效率。

4.3 数据上链要求

4.3.1 上链数据分类

上链数据包括两类：终端设备采集数据和非终端设备采集信息。

a) 终端设备采集数据包括：
   1) 传感设备采集的温湿度等环境信息、车辆地理位置、行驶路线、时间信息等；
   2) 监控设备采集的作业人员人脸、视频等信息；
   3) 作业人员通过终端输入的身份认证相关信息；
   4) 终端设备自身数据。
b) 非终端设备采集数据主要为冷链物流涉及到的单证/票据等信息：
   1) 作业人员资质信息；
   2) 冷链公司营业执照等信息；
   3) 运输工具许可证、行驶证等信息；
   4) 仓储信息；
   5) 商品仓单、检验检疫证、运单、清关单据等单证/票据信息。

4.3.2 数据上链基本要求

冷链物流各参与方将各关键环节的关键信息通过终端设备经哈希后上链。对区块链上智能合约而言，终端设备通过数据上链的过程，扮演了区块链预言机（oracle）的角色。上链的数据既可在合约中存储下来用于后续可信验真，也可以作为合约逻辑输入条件或运算的输入参数等。数据上链应遵循如下基本功能要求：

a) 用于数据上链的终端设备应当能够产生区块链私钥，或者能够在生产时向物联网终端注入区块链私钥；
b) 区块链私钥应当能够在受控条件下销毁或更新；
c) 用于数据上链的终端设备应当能够配置和/或感知区块链节点或网关的必要参数；
d) 用于数据上链的终端设备应当能够按照约定接口和协议，组装区块链智能合约调用报文或其他远程过程调用报文，并解析其响应；
e) 如果数据同时上云和上链，终端应建立两者的关联。

4.3.3 数据原文上链要求

数据原文上链，指终端设备上链的数据中，包含了终端设备所采集的原始数据，或者经端侧清洗处理且仍反映原始信息的数据。通常，若链上智能合约包含对具体数据内容的处理（例如根据数据的值进行特定的逻辑处理），则上链数据中应包含相应的原始数据或能反映原始信息的数据。

数据原文上链，应满足以下功能要求：

a） 应遵循最小必要原则，控制上链的数据量和上链频度，避免区块链网络拥塞；

b） 若上链数据涉及需授权访问的信息，应对数据内容进行加密，并通过密钥分发体系向被授权方分发访问密钥；

c） 若上链数据涉及个人信息，应根据需要按最小必要上链。

4.3.4 数据特征值上链要求

数据特征值上链，指终端设备上链的数据，是反映终端所采集的原始数据特征的摘要。这些摘要不直接反映原始信息，但能够验证原始数据的完整性。通常，若通过区块链实现数据验真，则可以采取原始数据上云，数据特征值上链的方式组合进行。

数据特征值上链，应满足以下功能要求：

a） 数据特征值可采用杂凑算法计算获取；

b） 被计算特征值的数据，可以是原始数据，也可以是经过端侧清洗处理且仍包含原始信息的数据；

c） 数据特征值上链一般与数据上云结合使用，链上的数据特征值用于在事后验证云上数据的完整性；

d） 上链的数据特征值可以与上云的数据一一对应，也可将若干组上云数据的特征值组合起来（例如以默克尔树的形式组合），计算特征值组合的特征值，将该特征值组合的特征值（例如默克尔树根）上链，以降低数据上链的频度和数量；

e） 若上链的数据特征值与上云的数据一一对应，上链信息和/或上云信息中应包含能够关联两者的标识；若上链的数据特征值与一组上云数据对应，则上链信息中应包含能够关联该链上数据特征值与云上数据组的信息。

5 技术要求

5.1 分层框架

基于区块链技术的冷链物流可信溯源服务分层框架包括基础层、核心层、接入层、用户层以及跨越各层的通用功能集合。各层由特定类型的功能组件构成，相邻层次的组件之间通过接口进行交互，其分层框架如图2所示。

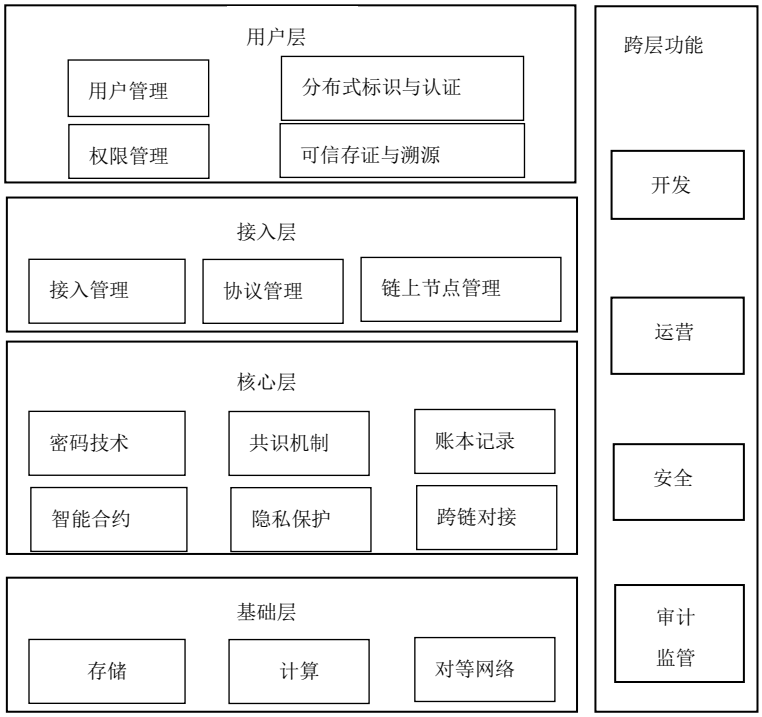

图 2　基于区块链技术的冷链物流可信溯源服务分层框架

基础层可视作全系统的基础支撑，提供冷链物流可信溯源服务系统正常运行所需要的运行环境和基础组件，主要包括存储、计算和对等网络。

核心层基于基础层提供的硬件和网络基础实现相应技术，是冷链物流可信溯源服务系统的核心功能层。主要包括：节点间的共识机制，以及在此共识机制之上的账本记录、隐私保护、密码技术等模块，保证系统的安全合规与防篡改；此外，根据应用场景的不同，可以有选择地添加能自动执行预设逻辑的智能合约，溯源场景下应包括基础的身份认证合约、存证与溯源合约。

接入层通过封装核心层功能组件为用户层或终端设备提供高效、可靠、通用的访问，包括：区块链输入接入管理，提供数据直接从终端设备上链的功能；节点管理，对接入区块链的节点进行身份认证和访问控制。

用户层是面向用户的入口。冷链物流可信溯源服务的使用方可通过该入口和服务进行交互，执行相关管理功能。用户层功能组件包括用户管理、权限管理、分布式标识与认证、可信存证与溯源等模块。

跨层功能提供跨越多个层次的功能组件，包括开发、运营、安全、监管和审计。

5.2　基础要求

基于区块链技术的冷链物流可信溯源服务应满足以下基础要求：

a)　应符合GB/T 22239-2019的要求；

b)　应采取必要的安全手段，保障链上资产和交易等信息的安全，防范攻击；

c)　应具备节点管理、加入、退出机制，保证上链节点的安全；

d)　链上、链下存取的数据应保证一致性，区块链各个节点之间的数据也应保持一致性；

e)　应保障链上信息安全，防止泄露用户信息。

5.3 基础层

5.3.1 存储

存储功能组件应满足以下要求：

a) 点对点网络中，能够被每个节点部署并使用；
b) 能够高效、安全、稳定地提供数据写入及查询服务；
c) 账本数据应区分数据对象的类别（如账户数据、区块数据、交易数据、配置数据以及账本元数据），并分别存储、分别管理、分别操作；
d) 对于敏感信息应当加密存储；
e) 对于冷链物流可信溯源系统，应当有数据访问等权限的控制和管理。同时节点CA证书的存储应当私密管理，防止泄露。

5.3.2 计算

计算功能组件应满足以下要求：

a) 计算功能组件提供区块链系统运行中的计算能力支持，包括但不限于容器技术、虚拟机技术和云计算技术等；
b) 对区块链系统提供运行环境支持；
c) 点对点网络中，能够被每个节点采用。

5.3.3 对等网络

区块链系统运行的底层拓扑结构是分布式对等网络，采用对等网络协议组织区块链中的各个网 络节点。各个节点间通常使用点对点通信协议完成信息交换以支撑上层功能。

网络传输功能组件应满足以下要求：

a) 能够进行点对点之间的高效安全通信；
b) 能够提供点对点通信基础上的多播能力；
c) 支持对节点的动态添加、减少的识别。

5.4 核心层

5.4.1 共识算法

共识算法应满足以下要求：

a) 支持多个节点参与共识和确认；
b) 支持独立节点对区块链网络提交的相关信息进行有效性验证；
c) 应具备一定的容错性，包括节点物理或网络故障的非恶意错误、节点遭受非法控制的恶意错误， 以及节点产生不确定行为的不可控错误，任意不超过理论值的节点数故障，整个系统正常工作；
d) 共识机制应保证公平，不存在后门以便特殊人员为特殊目的干扰共识机制达成逻辑；
e) 单次共识过程和系统运行的整个共识历史都应可审计、可监管。

5.4.2 账本记录

账本记录应满足以下要求：

a) 应支持持久化存储账本记录；
b) 应支持多节点拥有完整的数据记录；

c） 应支持向获得授权者提供真实的数据记录；
d） 应确保有相同账本记录的各节点的数据一致性；
e） 任何一条记录被人为修改后都可以通过历史区块回溯快速检验出来；
f） 应保证账本数据在生成、传输、存储、调用等操作不可被非授权方式更改或破坏；
g） 应保证账本数据在所有节点中具有冗余性，防止因单个节点失效而造成总账本数据的丢失。

5.4.3 智能合约

智能合约应满足以下要求：
h） 智能合约应支持图灵完备语言，应能够处理异常调用等；
i） 智能合约不应存在溢出漏洞；
j） 关键逻辑判断不应依赖区块链系统的变量（区块哈希、时间戳等）；
k） 应支持多方共识下的合约内容升级；
l） 应确保智能合约与外部应用的交互安全。

5.4.4 隐私保护

隐私保护方面应满足以下要求：
a） 对用户数据的访问采用权限控制，持有密钥的访问者才能解密和访问数据；
b） 信息采集时应明示用户，并经用户授权同意；
c） 信息采集时应对客户和采集的信息进行匹配认证，并对完整性进行校验；
d） 信息采集时应明确告知收集信息的目的和处理方式、存储期限、智能合约逻辑内容；
e） 信息传输时应对信息进行全量加密，加密的密钥和证书不能采用信息传输的同一传输通路进行传递；
f） 信息存储时应对客户信息进行全量加密；
g） 信息展示时应对客户身份标识信息进行部分隐藏，可额外提供全显示手段。非密文展示应采取去标识化措施；
h） 信息使用时，应明确记录使用者、使用内容、使用时间、使用频率；
i） 信息对外部扩散时，应告知用 户并获得授权，并提供给用户随时中断扩散传递的手段；
j） 应对用户提供信息备份和导出的手段，备份和导出的信息应加密处理，并给用户提供解密手段；
k） 应对客户提供信息的删除销毁的手段，信息删除销毁时应获得客户认证和授权。

5.4.5 加密

密码算法、密钥等应满足以下要求：
a） 所使用的密码算法应符合国家密码管理部门的要求；
b） 密钥管理包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程；
c） 除公钥外，所有密钥不能以明文形式存储或传输。

5.4.6 跨链对接

宜支持不同区块链系统的跨链交互，可以采用的主流技术有：公证人机制、侧链/中继、哈希锁定、分布式私钥控制等。

5.5 接入层

5.5.1 接入管理

接入管理功能组件应满足以下要求：

a) 接入管理功能组件提供跨进程调用功能，为终端应用及用户层提供核心层接入服务；
b) 接入管理功能组件宜具备接口服务能力管理，如支持接口调用频度设置和事务操作及账本查询缓存设置；
c) 接入管理功能组件应具备接口访问权限管理，如针对不同的用户配置不同的访问权限；
d) 应确保接口的通讯安全，如对通讯报文进行加密。

5.5.2 协议管理

协议是连入网络的设备都要遵循的一定的技术规范,应包含关于硬件、软件、端口等的技术规范。

5.5.3 节点管理

节点是区块链的载体，由安装了特定区块链软件、可连接互联网、具有可访问的 IP 地址、且能对外提供服务的物理服务器或虚拟服务器组成。节点管理功能组件应满足以下要求：

a) 支持对冷链物流可信溯源服务区块链节点的信息查询和管理控制；
b) 节点加入区块链网络之前，应由授权机构给予唯一的身份标识，并提供与之对应的身份鉴别信息和身份凭证，授权机构应在凭证中指定节点角色；
c) 身份凭证由授权机构确保其完整性和真实性，应符合密码算法对完整性和真实性的要求；
d) 身份鉴别信息应具有不易仿冒的特性，并设定更换期限，在期限到来之前进行更换；
e) 在传递及存储身份鉴别信息之前，应采用符合密码算法要求的机密性及完整性保护；
f) 节点之间建立数据通信连接之间，应先通过身份鉴别信息实现双向身份认证，并建立一条安全的数据通信信道，该过程应符合密码算法要求对机密性和完整性的要求；
g) 应具有节点身份认证失败时的处理机制，可采取结束通信、限制认证失败次数和超时自动结束等措施；
h) 应具备节点退出机制。

5.6 用户层

5.6.1 用户管理

用户管理组件应满足以下要求：

a) 应为使用方用户提供身份认证接口，为区块链业务提供者提供管理接口；
b) 身份认证接口应使用密码技术保证数据传输的完整性、保密性和不可否认性，对敏感数据应设计额外的保护机制；
c) 应具备用户交互界面，可以是命令行界面或图形用户接口以及应用程序接口等形式；
d) 应具备将冷链物流可信溯源区块链服务的使用方的特定事务请求（查询、更新）提交到冷链物流可信溯源区块链网络的功能。

5.6.2 权限管理

权限管理组件应满足以下要求：

a) 应具备权限管理机制，不同的用户只能访问、操作用户层不同的资源；
b) 账户对用户层的读写权限应做分级，如普通账户、管理员账户。

5.6.3 分布式标识与认证

应支持为设备或用户颁发唯一身份标识，并验证该设备/用户身份，保证上链数据的可信性。

5.6.4 可信存证与溯源

应支持冷链物流中采集的有效信息存证到区块链上，同时支持用户向冷链物流可信溯源服务使用方提供溯源查询、事后审计等功能。

a) 用户管理：用户登陆验证等功能；
b) 权限管理：系统访问控制策略配置与执行；
c) 分布式标识与认证：区块链为设备或用户颁发身份标识，同时验证该设备/用户身份，保证上链数据的可信性；
d) 可信存证与溯源：支持冷链物流中采集的有效信息存证到区块链上，同时支持用户向冷链物流可信溯源服务使用方提供溯源查询、事后审计等功能。

参 考 文 献

[1] 中国通信标准化协会《物联网+区块链”应用与发展白皮书（2019）》

电信终端产业协会团体标准

冷链物流可信溯源服务技术要求　第5部分：基于区块链技术实现可信溯源服务的要求

T/TAF 101.5-2021

*

电信终端产业协会印发
地址：北京市西城区新街口外大街28号
电话：010-82052809
电子版发行网址：www.taf.org.cn