ICS 35.240.01
CCS C 07

团　体　标　准

T/CPMA 026—2023

疫苗追溯的区块链技术应用要求

Baseline for vaccine traceability blockchain application

2023 - 02 - 02 发布　　2023 - 02 - 02实施

中华预防医学会　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。

本文件由中华预防医学会健康大数据与人工智能应用专业委员会提出。

本文件由中华预防医学会归口。

本文件起草单位：中国疾病预防控制中心、中国科学院软件研究所、中国科学院大学健康医疗大数据国家研究院、国科健信(北京)科技有限公司、中科软科技股份有限公司、苏州沈苏自动化技术开发有限公司、深圳三代人科技有限公司、济南市疾病预防控制中心、苏州市伏泰信息科技股份有限公司、河北世窗信息技术股份有限公司。

本文件主要起草人：马家奇、赵自雄、梁赓、陈胜、靖瑞峰、刘大鹏、刘继增、阮师漫、刘翀、李志海、苗雪飞、杨威、石铁军、龙本超、沈健、郭龙、崔小波、崔春生、李磊。

疫苗追溯的区块链技术应用要求

1 范围

本文件规定了疫苗监测监管与追溯业务活动过程中，应用区块链技术的相关基础要求、技术要求、安全要求与应用功能要求。

本文件适用于疫苗上市许可持有人/生产企业、经营企业、使用单位、监管部门和社会参与方等协同建设、完善和规范可信疫苗信息化追溯体系的区块链技术应用。

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 15843.1 信息技术 安全技术 实体鉴别 第1部分：总则
GB/T 32918 信息安全技术SM2椭圆曲线公钥密码算法
GB/T 32905 信息安全技术SM3密码杂凑算法
GB/T 32907 信息安全技术 SM4分组密码算法
GB/T 39786 信息安全技术 信息系统密码应用基本要求
NMPAB/T 1004 疫苗追溯基本数据集
NMPAB/T 1005 疫苗追溯数据交换基本技术要求

3 术语和定义

NMPAB/T 1002—2019界定的以及下列术语和定义适用于本文件。

3.1

区块链网络 blockchain network

组网节点程序使用一致的初始配置、创世块建立和加入的对等网络。

3.2 **联盟链 consortium blockchain**

仅由一组具有利益相关的特定区块链服务客户使用，仅有授权节点可接入，接入节点可按规则参与共识和读写数据的区块链部署模型。

[来源：YD/T 3747—2020]

3.3

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。

[来源：CBD-Forum-001-2017，2.2.7]

3.4

疫苗电子凭证 electronicvaccine certificate

存证于区块链上一种由签发者担保，证明疫苗流通全程上链交易数据的标志性信息属性（具体内容可由签发者定义或达成行业共识），可离线流转在线验证的以二维码形式呈现的加密数字凭证。

3.5

疫苗信息化追溯体系 vaccine Informationization traceability system

疫苗上市许可持有人/生产企业、配送单位、疾病预防控制机构、接种单位、监管部门等疫苗追溯参与方，通过信息化手段，对疫苗生产、流通、使用等各环节的信息进行追踪、溯源的有机整体。

注：应用功能包括疫苗追溯服务中涉及的数据采集、存储、传输、处理、使用等活动。

4 缩略语

下列缩略语适用于本文件。

AEFI 预防接种不良反应（Adverse Events Following Immunization）
API 标准开放编程接口（Application Programming Interface）
BFT 拜占庭容错（Byzantine Fault Tolerance）
CFT 故障容错（Crash Fault Tolerance）
ID 身份标识号（Identity）
JSON JS对象简谱（JavaScript Object Notation）
KV 键值对数据库（Key-Value）
PKI 公钥基础设施（Public Key Infrastructure）
POW 工作量证明（Proof Of Work）
SDK 软件开发工具包（Software Development Kit）
TLS 传输层安全协议（Transport Layer Security Protocol）
XML 可扩展标记语言（Extensible Markup Language）

5 基本要求

5.1 基础链选择

以自主可控为原则，应选择国内自主设计和研发，核心功能的主要技术方法进行了专利覆盖，使用时不受第三方专利约束的基础链服务。应采用业界标准规范实现区块链通用功能，方便协议升级和模块替换。所依赖的环境、工具和库建立在开源生态上，且不存在开源许可冲突。

5.2 对等网络

网络层应支持TLS 1.3许可组网并提供组网成员的动态管理，允许单主机同时加入不少于100个组网。支持组网实时状态的可视化展示，以及以实时图形报表展示平台内部模块的实时压力、处理能力、节点运行状态、区块链账本存储等情况。

5.3 密码技术

包括且不限于数据加密技术、密钥管理技术、数字签名技术、杂凑值计算等。杂凑算法主要用于计算哈希值，对称加密主要用于业务交易数据JSON字符串或XML文本的加密。上述技术使用的算法应符合GB/T 39786第三级的相关要求。

5.4 共识算法

应采用可插拔设计，允许通过配置选择BFT或CFT共识算法，或实现自定义的共识算法。

5.5 智能合约

应支持提供集合约编辑与调试、代码版本管理、静态分析和形式化证明于一体的集成开发环境。通过调用基础链API提供SDK的交互方式，以智能合约和访问控制策略实现数据的访问权限控制。

5.6 区块数据

应实现区块数据的链式结构存储，包含时间戳、电子签名、加密业务交易数据等区块链技术中最底层的数据结构。应采用可定义的数据结构并支持数据向下兼容，签名交易数据结构中的系统字段不超过通常物联网设备的存储大小，支持接入冷链过程物联网设备的签名数据。

5.7 应用组网

5.7.1 区块链组网

可采用联盟链组网技术。以互联网为基础通过共识算法创建疫苗追溯区块链对等网络。业务参与方加入区块链网络时，应完成实名信息注册登记，确保每个交易节点在该网络中的唯一性。区块链网络应具备根据业务压力扩充处理能力的机制。

5.7.2 疫苗追溯机构隔离组网

各级承担疫苗追溯管理职责的机构，可根据业务应用实际建立与互联网逻辑隔离的网络环境，并通过网闸与区块链网络实现信息交互应用。

5.7.3 疫苗生产流通机构组网

疫苗生产企业和冷链物流企业可依托区块链组网应用，亦可独立组网与区块链网络共享疫苗配送、流通数据。

5.7.4 区块链组网共识

区块链组网下，各节点用户应达成共识，修改节点用户信息配置、修改操作权限都应通过签名交易或智能合约，并基于共识进行，发出区块时全网一致更新。

操作者的签名组合应满足相应的身份规则策略，才能够被允许执行相应操作，并对签名数据按照规则进行校验。

5.7.5 跨链互信机制

具备区块链跨链互信机制，支持同基础链建立的同构链以及不同基础链建立的异构链信息系统之间的区块数据进行交互与流通互认。跨链的机制包含且不限于公证人机制、哈希锁定机制、分布式私钥控制、侧链/中继链等。

5.7.6 工程友好

采用跨平台跨语言的API，并提供集成API接口方法说明的在线测试，提供不少于两种主流语言的SDK封装；针对平台测试与性能分析、合约开发、内容数据存储、应用实施提供技术成熟、功能完备的配套工具集。

6 功能要求

6.1 智能合约调用

6.1.1 身份认证

使用注册实体Id作为身份标识，采用基础链提供的数字证书对应的签名作为身份证明，或使用兼容公开密钥基础设施的PKI证书和电子签名，身份证书的验证介质和载体可使用USB Key或加密二维码。技术应用时应提供身份认证功能，疫苗追溯活动相关参与方加入区块链网络节点时，完成账号的注册和实名认证。经过实体认证的机构可向下级单位以及名下的设备或系统签发数字证书。

6.1.2 节点账户

采用别名机制缩短注册实体账户编码长度；采用多密钥对应分级使用机制解决密钥对丢失或被盗。组网节点通过加载初始配置文件和创世块启动或加入组网，在创世块中部署实体注册/证书管理合约，并注册初始共识节点账户及其证书。疫苗生产、销售、物流、使用等机构通过实体注册合约注册账户并申请认证，通过认证后可自行使用证书管理合约管理其账户证书。授权机构应对提交签名交易数据的各类系统、手持设备或物联网设备进行实体注册，并关联其用于签名的账户证书。公钥算法应符合GB/T 32918。

6.1.3 权限管理

基于组网共识算法和签名交易或智能合约方式实现灵活的访问权限控制，针对节点、组织、角色和用户制定不同的使用权限策略，包括获取上一节点区块、交易等数据的读操作，向区块链发起交易的写操作，以及各节点用户配置信息的管理操作等。

6.2 数据存储验证

6.2.1 区块头结构

每个区块由区块头和区块体两部分组成,每个区块头中应包含区块元信息和一个指向前一个区块头哈希值（Hash）的指针。

区块头结构由版本号、前一个区块哈希值、默克尔根（merkle root）、本区块哈希值、该区块创建的时间戳构成，格式参见附录表A.1。

6.2.2 区块头哈希值

通过对前一个区块哈希值、时间戳和默克尔根进行两次哈希计算获得。默克尔根节点即为区块中所有业务数据构成的默克尔根的哈希值。哈希值生成算法应符合GB/T 32905。

6.2.3 业务数据

区块链上的业务数据即为账本数据，包括区块数据和状态数据，区块数据使用块链式的存储模型，由包含N个随时间排序的块串联组成，主要记录疫苗生产信息、冷链物流信息、预防接种信息和AEFI监测信息等疫苗追溯管理所需信息的JSON字符串或XML文本，应符合NMPAB/T 1004。

业务数据上链应符合GB/T 39786，通过对称国密算法对JSON字符串或XML文本进行加密，同时生成该节点交易时间戳和数字签名的哈希，对称加密算法应符合GB/T 32907。各节点解析应用业务数据时，与区块链系统进行数据交互的业务信息系统或智能采集终端应具备解密JSON字符串或XML文本，对用户使用业务数据进行授权和访问控制的功能。

6.2.4 数据记录与验证

区块链节点的存储层应能支持按需扩展文件存储和KV存储容量的能力。数据记录均以签名交易或智能合约的形式写入区块中，每一区块包含前一区块所有数据记录的哈希值和业务交易数据。签名交易一旦出块，不可更新或删除，更改区块链中任何一个数据，其后所有区块的哈希值均发生变化而无法通过验证，业务数据的更新或删除只能通过追加签名交易的方式间接实现。数据写入的结果是全网一致的区块数据和KV状态数据，它们分别存储于文件系统和KV数据库中，确保验证最后一个区块的哈希值即验证了整个账本信息的交易验证、不可篡改的总账本。

6.2.5 数据格式

疫苗追溯数据根据数据标准分类，统一以键值对格式保存在KV数据库中。业务交易数据以加密JSON字符串或XML文本格式保存为单独字段。JSON格式应符合NMPAB/T 1005。

6.2.6 数据注销

上链数据应可注销。授权的区块链账号可通过智能合约注销疫苗使用、报损、报废等上链数据，并上链存证注销过程。

6.3 数据追溯服务

6.3.1 数据预处理

在业务信息系统中预处理疫苗追溯数据时应与业务操作同步,并检查疫苗追溯数据的完整性与合规性，确保追溯数据收集的及时性和一致性。

6.3.2 注册实体验证

数据追溯验证过程中,应对各参与方及其名下产生溯源数据的信息系统、设备等注册实体进行核验，并通过私钥和签名进行数据查验。

6.3.3 参与方节点验证

参与发行、流转、注销的区块链账户应进行实名认证，确保可追溯到参与主体。各参与方节点均可通过已认证系统和设备自动同步区块数据,以私钥和签名对授权区块的业务交易数据进行完整追溯存证

数据查验和比对。查验的结果可重新定向到区块链服务，向用户提供验证数据完整性及数据来源一致性的查验结果。

6.3.4 受种者数据查验

应向受种者提供查验接种疫苗追溯信息电子存证的功能。受种者可通过公开签名证书和个人身份信息查验本人或被监护人所接种疫苗的追溯信息。

6.3.5 区块交易数据解析

区块交易数据通过区块链服务的数据同步机制，经公钥解密后同步交换到业务信息系统，按业务含义拆分为结构化字段，存储至关系型数据库，提供基于业务字段的数据应用。验证服务可重定向到区块链服务，向用户验证数据完整性和数据一致性。

6.3.6 追溯信息查询

上链的疫苗全程追溯信息可通过提供应用程序API结合安全网关认证的方式开放给相关授权企业和机构，并确保疫苗电子凭证发行、流转、注销全过程的可追溯性。

6.3.7 疫苗电子凭证

疫苗电子凭证发行、变更、注销过程中的每一环节应通过签名交易或智能合约在区块链上存证，支持对已注销疫苗电子凭证的完整追溯，并可查询所有存证记录。对疫苗电子凭证进行有效性验证服务时，应当支持符合相关法律、法规要求，具备相关资质的第三方机构验证；并提供可验证的存证电子数据和基于第三方疫苗管理信息系统提供的原始数据；可根据特定且公开的算法对电子数据进行验证。

6.4 流程定制

区块链疫苗追溯应用流程定制应支持以下功能：

a) 可定制疫苗追溯所需上链数据字段；
b) 可定制冷链物流追踪流程模板；
c) 流程定制模板可关联第三方冷链物流管理信息系统中的指令；
d) 可设置流程定制中涉及到的业务数据来源。
e) 具备流程定制的审核与发布功能。

6.5 可靠性校验

疫苗追溯数据应至少有3个参与方加入节点，参与数据校验。参与方可包括疫苗生产企业、疫苗存储/运输企业、疫苗接种单位、监管机构等。在一组疫苗追溯区块链中，每个参与方应各自持有密钥，采用一致的共识算法，共同完成对顺序签名交易执行结果的计算，并对计算结果签名背书。

7 安全要求

7.1 合规性

应符合国家相关信息安全等级保护及个人隐私保护的相关要求。应用节点应保护受种者个人隐私数据，隐私数据流通应加密上链并限定在特定的范围内，应支持授权访问；链下数据应防止泄露个人隐私。

7.2 密码应用

7.2.1 国密体系产品

在数据加密存储、签名/验签、API双向身份认证等方面，允许通过配置选择符合国标的开源加密库。

7.2.2 实名注册与认证

在保护私密性的前提下支持实体的实名注册与认证，提供实体证书的管理（新增/注销、锁定与替换）与分级使用机制。在网络层与API层均采用双向身份认证的安全连接，在此基础上实现基于共识的全网一致的权限管理与授权访问。

7.3 制订合约编程规范

制订合约编程规范，避免合约非预期调用导致的安全漏洞或其他导致分布式不一致的结果，并针对编程规范提供合约静态化分析，在合约编译期予以告警。提供合约的形式化证明，以保证合约的可终止性以及对特质声明断言的正确性证明，在否定其正确性时，给出至少一个反例。

7.4 节点安全

包括节点身份认证及对异常节点的监控。区块链节点的加入应采用准入机制，可通过数字身份认证等方式验证加入节点的身份。区块链运行过程中，应配备相应的节点监控措施，能够及时发现异常运行的节点。

7.5 账本安全

区块链账本应符合区块链上存储多个全量账本，确保账本数据的完整性。

7.6 账户安全

区块链账户生成基于安全的密码学算法，且符合GB/T 39786，应配备区块链账户私钥保存和使用过程中的安全措施，具备多重签名功能，只有账户私钥持有者才能操作对应的账户，同时防止私钥丢失后无法继续使用区块链账户。

7.7 疫苗电子凭证安全

包括疫苗电子凭证本身的安全性和管理的安全性，其发行基于安全的密码学算法，确保电子凭证无法被伪造和篡改；发行机构需具备一定的资质并经过区块链系统各参与主体共同授权，电子凭证编号、发行时间、发行证明等详细信息需在区块链上存证，且支持离线流转和验证，防止私密性内容泄露。

附 录 A
（资料性）
疫苗追溯区块头结构格式

表A.1给出了疫苗追溯区块头结构格式。

表A.1 疫苗追溯区块头结构格式

字段名	类型	长度	备注
version	string	8	版本号
provider	string	128	创建者 hash
previous_block_hash	string	128	上一个区块 hash
block_hash	string	128	本区块 hash
timestamp	number	16	该区块创建的时间戳
merkle_root	string	128	Merkle 哈希（疫苗生产信息）
transaction data	string	8K	业务交易数据 hash+加密 JSON

参 考 文 献

[1] WS 375.12-2012 疾病控制基本数据集第12部分：预防接种。
[2] WS 375.19-2016 疾病控制基本数据集第19部分：疫苗管理。
[3] CBD-Forum-001-2017区块链 参考架构。
[4] NMPAB/T 1002 药品追溯码编码要求。