

团 体 标 准

T/AI 130—2024

基于区块链的视频系统可信赖要求

Trustworthiness requirements for video system based on blockchain

2024-11-29 发布

2024-11-29 实施

中关村视听产业技术创新联盟 发布

TIAI 130-2024

TIAI 130-2024



版权保护文件

版权所有归属于该标准的发布机构，除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版，影印件，或发布在互联网及内部网络等。使用许可可于发布机构获取。

TIAI 130-2024

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 缩略语	2
5 系统架构	2
6 技术要求	4
附录 A（资料性） 系统工作流程	11
附录 B（资料性） 场景应用	13
参考文献	15

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。

本文件由新一代人工智能产业技术创新战略联盟AI标准工作组提出。

本文件由中关村视听产业技术创新联盟归口。

本文件起草单位：青岛海信电子技术服务有限公司、山东大学、天津大学、美的集团(上海)有限公司、北京邮电大学、北京云天励飞科技有限公司、上海数字电视国家工程研究中心有限公司、天翼数字生活科技有限公司、上海商汤智能科技有限公司、蚂蚁金服(杭州)网络技术有限公司、海信集团控股股份有限公司、上海燧原科技股份有限公司、杭州海康威视数字技术股份有限公司、中国移动通信集团有限公司、西安电子科技大学、北京世纪好未来教育科技有限公司。

本文件主要起草人：刘微、方静、刘琚、李克秋、姚昌松、陆月明、饶雪、殷惠清、吕冠中、徐浩、孙曦、王思善、钟凯伦、秦日臻、朱辉、王婷、何晨迪、孙冀浩、刘常昱、王士宁、曹旭、刘秀龙、高雪松、蔡亚森、左金鑫、代翔、贾立鼎、张鸿伟、孟令邦、马豪、马立原、高雅、曹若菡、杨睿毅、赵奕捷、邹名伊、张维、程学军、周素雨、李玉楷、赵海英、崔晓冉。

基于区块链的视频系统可信赖要求

1 范围

本文件确立了基于区块链的视频系统可信赖框架，规定了基于区块链的视频系统数据采集、传输、处理、使用、存证，以及分布式管理、跨链互操作的可信赖技术要求。

本文件适用于可信赖的基于区块链的视频系统设计、应用及测试。

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 43572-2023 区块链和分布式记账技术 术语

3 术语和定义

GB/T 43572-2023界定的以及下列术语和定义适用于本文件。

3.1

视频系统 video system

具备音视频采集、传输、存储、处理、管理、播放功能的系统。

注：本文件中的视频系统组成中不包含对应的硬件设备。

3.2

可信赖 trustworthiness

系统满足利益相关方期望并可验证的能力。

注1：依赖于语境或行业，也依赖于具体的产品或服务、数据以及所用技术，应用不同的可信赖特征并对其进行验证，以确保利益相关方的期望能得到满足。

注2：可信赖的特征包括实时性、可备份性、安全性、可控性、隐私性、透明性、可追溯性。

注3：可信赖作为一种属性用于描述服务、产品、技术、数据和信息，在治理中也用于组织。

[来源：GB/T 41867-2022，3.4.2，有修改]

3.3

上链存证 record on-chain

将信息写入到区块链并持久化存储的过程。

3.4

跨链 cross-chain

不同区块链网络之间实现数据和资产交互和通信的能力。

注：跨链允许不同链上的节点进行安全的数据传输、共享和交互，保证数据的一致性和可信性。

3.5

跨链通信 cross-chain communication

不同区块链网络之间进行数据传输的过程，通过跨链桥或其他跨链技术实现不同链上节点之间的数据交互和共享，促进跨链互通的实现。

3.6

跨链验证 cross-chain verification

通过多个链上的节点和共识机制来验证跨链事务的有效性以及数据和交易的合法性和真实性。

3.7

跨链可追溯性 cross-chain traceability

通过区块链技术和跨链验证机制，提供对跨链操作的审计和验证能力，在跨链操作中追溯和记录数据和交易的来源和历史，确保数据的可溯源和真实性。

4 缩略语

下列缩略语适用于本文件。

AI：人工智能(Artificial Intelligence)

P2P：点对点(Peer-to-Peer)

5 系统架构

5.1 概述

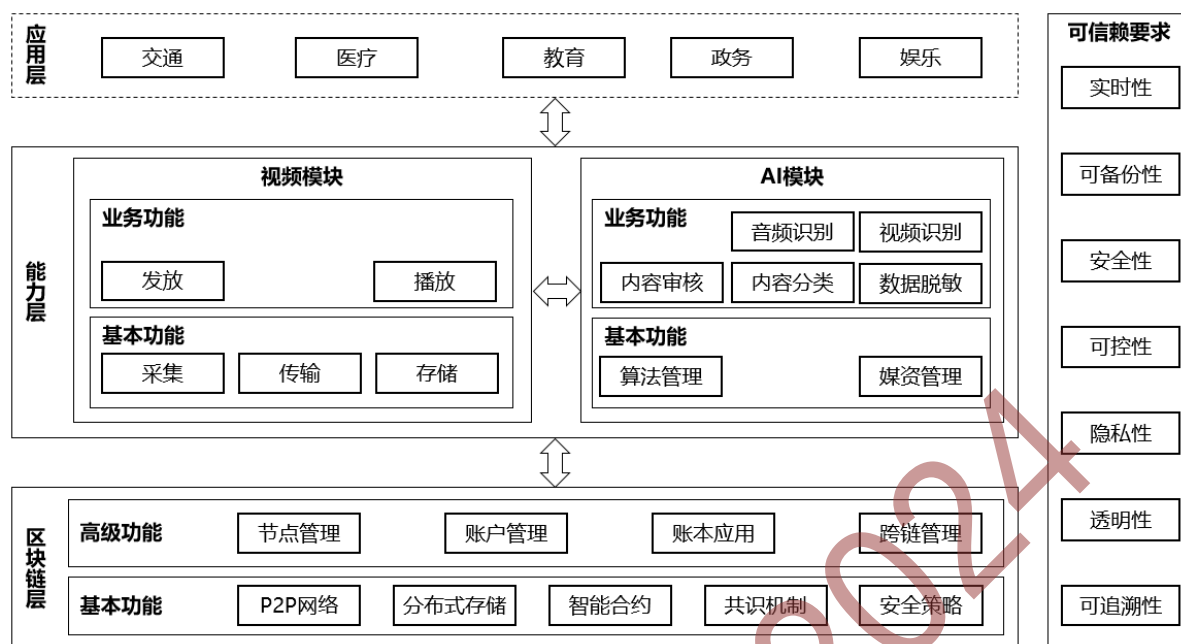
基于区块链的视频系统（以下简称“系统”）由区块链层、能力层、应用层三层组成。

- a) 区块链层为系统提供安全策略、跨链管理等功能；
- b) 能力层为系统提供正常运行所需要的音视频采集、传输、播放等功能；
- c) 应用层支撑各类应用场景的使用。

系统工作流程示例参见附录A。

5.2 系统框架

系统根据应用层的场景需求，调用能力层和区块链层的各模块功能，实现对音视频的处理、管理，并对过程进行上链存证。能力层的视频模块为系统提供了音视频采集、传输、存储、发放、播放的功能，满足系统可信赖要求的实时性、可备份性。AI模块提供了算法管理、媒资管理、内容审核、内容分类、数据脱敏、音频识别、视频识别等功能，满足系统可信赖要求的安全性、可控性、隐私性。AI模块中的业务功能可根据实际应用场景需求选择使用。区块链层对数据流转和处理过程中的重要信息进行上链存证，满足系统可信赖要求的透明性、跨链可追溯性。系统框架见图1。



注：图中实线部分对应本文件规定的范围，虚线部分仅为表明基于区块链的视频系统框架，不在本文件中规定。

图1 系统框架

5.3 区块链层

区块链层具备与能力层进行数据交互的能力。包括基本功能和高级功能，其中：

- a) 基本功能：为区块链模块提供运行的基本能力。包括：
 - 1) P2P 网络；
 - 2) 分布式存储；
 - 3) 智能合约；
 - 4) 共识机制；
 - 5) 安全策略。
- b) 高级功能：为系统的能力层提供区块链的分布式管理、跨链互操作、跨链通信、跨链验证等服务能力。包括：
 - 1) 节点管理；
 - 2) 账户管理；
 - 3) 账本应用；
 - 4) 跨链管理。

5.4 能力层

5.4.1 视频模块

视频模块为系统提供音视频数据处理能力。包括基本功能和业务功能，其中：

- a) 基本功能：采集、传输、存储；
- b) 业务功能：发放、播放。

注：音视频发放功能指的是单路音视频转发功能、多路音视频分发功能。

5.4.2 AI 模块

AI模块为音视频处理提供算法和管理能力。包括基本功能和业务功能，其中：

- a) 基本功能：为AI模块提供运行的基本能力，包括算法管理、媒资管理等；
- b) 业务功能：为系统提供音视频内容的识别、分析等能力，包括：
 - 1) 内容审核；
 - 2) 内容分类；
 - 3) 数据脱敏；
 - 4) 音频识别；
 - 5) 视频识别。

5.5 应用层

系统应用的典型场景，包含但不限于交通、医疗、教育、政务、娱乐。应用示例参见附录B。

6 技术要求

6.1 区块链层

6.1.1 P2P 网络

为保障区块链功能的使用，P2P网络应符合以下要求：

- a) 节点之间的直接通信；
- b) 有效的路由和转发机制；
- c) 数据的分发、同步和存储；
- d) 单点故障不影响整个网络的运行。

6.1.2 分布式存储

为保障系统的可备份性，通过不同节点对账本共同记录与维护。分布式存储应符合以下要求：

- a) 账本记录持久化存储；
- b) 多节点拥有完整的、一致的数据记录；
- c) 对账本中的数据进行校验，以提高防篡改能力；
- d) 向授权者提供数据记录。

6.1.3 智能合约

为系统的智能合约根据不同应用场景提供功能支持。智能合约符合以下要求：

- a) 应支持合约内容静态和动态检查；
- b) 应提供运行载体支持，并执行合约逻辑；
- c) 对于与系统外部数据进行交互的智能合约，外部数据源的影响范围应仅限于智能合约范围内，不影响区块链的整体运行；
- d) 应防止合约内容被篡改或攻击；
- e) 应支持多方共识下的合约内容升级；
- f) 应支持向账本中写入合约内容；
- g) 宜提供多种编程语言；
- h) 宜支持跨链智能合约的部署和执行。

6.1.4 共识机制

根据不同需求，选择不同的共识算法来实现共识机制。共识机制应符合以下要求：

- a) 多个节点参与共识和确认；
- b) 独立节点对区块链网络提交的上链信息进行有效性验证；
- c) 防止任何独立的共识节点未经其他共识节点确认而在区块链模块中进行信息记录或修改；
- d) 具备一定的容错性，包括但不限于：
 - 1) 节点物理或网络故障的非恶意错误；
 - 2) 节点遭受非法控制的恶意错误；
 - 3) 节点产生不确定行为的不可控错误。
- e) 所有记账节点对上链信息达成共识后，全网同步更新账本信息。

6.1.5 安全策略

6.1.5.1 密码算法

为保障系统的安全性，密码算法应符合以下要求：

- a) 支持哈希算法，如 SM3、Keccak256 等；
- b) 支持以下至少一种密码算法：
 - 1) 非对称加密算法，如 SM2、ECDSA 等；
 - 2) 对称加密算法，如 SM4、AES 等。

6.1.5.2 密钥管理

为保障系统的安全性，密钥管理应符合以下要求：

- a) 应具备密钥生成、存储的能力；
- b) 密钥存储应加密；
- c) 密钥的密码宜定期更换、使用强密码；
- d) 可支持公钥加密。

6.1.5.3 数据传输

为保障系统的安全性，数据传输应符合以下要求：

- a) 上传的数据应通过私钥进行加密处理；
- b) 传输前应进行身份验证、数字签名；
- c) 数据接收后，应通过数字验签校验数据的真实性和完整性；
- d) 为防止中间人攻击，通信过程应进行证书真实性、有效性检验；
- e) 应使用安全传输协议，确保终端用户与网络业务之间的通信安全；
- f) 宜具备反欺骗机制；
- g) 可支持加密传输。

6.1.6 节点管理

节点管理用于节点的信息查询和管理控制，应符合以下要求：

- a) 节点状态信息查询服务；
- b) 节点启动与关闭服务；
- c) 节点服务配置，包括但不限于：
 - 1) 节点准入准出；
 - 2) 节点事务处理；

- 3) 账本查询授权。
- d) 网络连接状态监控服务。

6.1.7 账户管理

为保障系统可控性、可追溯性，账户管理应符合以下要求：

- a) 用户通过账号注册使用系统；
- b) 用户使用系统账号能作为区块链账号认证的凭证，不再重复注册和登录；
- c) 注册信息生成公私钥对，私钥储存在输入终端，公钥上传至区块链网络；
- d) 具备权限管理机制：
 - 1) 用户只能访问权限允许范围内的资源，包括账户信息、账本信息、统一管理的跨链账户；
 - 2) 用户只能在权限允许范围内进行业务操作，包括上链存证、节点管理、跨链管理；
 - 3) 具备账户权限分级功能，权限包括管理员、普通账户。

6.1.8 账本应用

为保障系统的透明性、可追溯性，账本应用应符合以下要求：

- a) 应支持链上内容发行和交换；
- b) 应支持共识前的逻辑验证和共识后的结果验算；
- c) 应支持所有交易记录对有权限的用户公开可见；
- d) 应支持对系统数据流转过程中的重要信息进行上链存证，并通过索引信息对全过程进行追溯；
- e) 可对待定事务进行多签名权限控制设置；

注：多签名权限控制是一种智能合约的安全措施，可以防止单一账户或单一实体对智能合约进行未经授权的操作。它基于多个账户共同控制智能合约的原则，只有在多个账户都同意后，才能执行智能合约的操作。

6.1.9 跨链管理

为保障系统的安全性，跨链管理应符合以下要求：

- a) 具备不同区块链网络之间进行信息可信传输与交换的能力；
- b) 支持多种链间的跨链通信协议和共识机制；
- c) 具备跨链数据的映射和转换的能力以及不同区块链网络共同参与共识过程的能力；
- d) 跨链事务处理过程采取技术措施，防止恶意攻击和隐私信息泄露，包括但不限于：数据加密、身份验证；
- e) 具备节点规模和服务用户数量的可扩展性；
- f) 具备权限管理和准入控制功能；
- g) 具备解耦的跨链交互功能，满足系统在功能设计上的迭代扩展，包括但不限于：
 - 1) 底层架构；
 - 2) 数据结构；
 - 3) 接口协议。

6.2 视频模块

6.2.1 音视频采集

6.2.1.1 每秒帧数

为保障视频播放的流畅度，通过不同的输入终端采集到系统的视频每秒帧数应不小于 25 帧每秒。

6.2.1.2 分辨率

为保障视频播放的质量，通过不同的输入终端采集到系统的视频分辨率要求如下：

- a) 应至少支持 720 p；
- b) 宜支持 4K、8K 及以上。

6.2.1.3 声音采样率

为保障音频播放的质量，通过不同的输入终端采集到系统的声音采样率应不小于16 kHz。

6.2.1.4 采样位深

为保障音频播放的质量，通过不同的输入终端采集到系统的音频采样位深应不小于16 bit。

6.2.1.5 编码

为保障采集到的音视频传输、存储和播放的安全性、可控性，音视频的编码、解码格式应符合以下要求：

- a) 视频：支持 AVS1、AVS2、AVS3、MJPEG、MPEG-4、H.264、H.265、SVAC 等视频编码格式中的一种及以上；
- b) 音频：支持 AVS1、AVS2、WAV、WMA、MP3、MJPEG、MPEG-4 等音频编码格式中的一种及以上。

6.2.1.6 上链存证信息

为保障音视频来源可追溯性，符合以下要求：

- a) 上链存证信息应包含：
 - 1) 输入终端 IP；
 - 2) 输入终端唯一标识；
 - 3) 采集时间；
 - 4) 采集数据的哈希值。
- b) 上链凭证应进行结果校验；
- c) 宜包含采集地点；
- d) 宜支持音视频原始数据上链存证。

6.2.1.7 多源输入

如应用场景有需求，则系统应支持多路音视频源输入。

6.2.2 音视频传输

为保障系统音视频数据传输的实时性，音视频数据从采集终端到播放终端设备的双向传输时延应不大于500毫秒。

6.2.3 音视频存储

为保障音视频内容的可备份性、可控性和实时性，音视频存储应符合以下要求：

- a) 具备数据备份功能；
- b) 具备数据缓冲功能；
- c) 数据删除前进行身份验证；
- d) 删除的数据可恢复；

- e) 数据销毁前应有提示，销毁后不可恢复。

6.2.4 音视频发放

为保障系统具备单路音视频转发或多路音视频分发的能力，音视频发放符合以下要求：

- a) 应具备数据传输断点恢复功能；
- b) 上链存证信息应包含但不限于：
 - 1) 发放设备 IP；
 - 2) 发放设备唯一标识；
 - 3) 账户 ID，包含发放方和接受方；
 - 4) 发放时间；
 - 5) 发放内容摘要，包含名称、版本、大小、哈希值。
- c) 宜具备直播、流媒体通道创建功能；
- d) 宜具备多路音视频数据的分发功能。

6.2.5 音视频播放

6.2.5.1 分辨率

音视频播放分辨率应符合本文件6.2.1.2的规定。

6.2.5.2 解码

音视频的解码格式应符合本文件6.2.1.5的规定。

6.2.5.3 上链存证信息

6.2.5.3.1 通用要求

视频上链存证信息，包含但不限于：

- a) 应输出终端设备 IP；
- b) 应输出终端的唯一标识；
- c) 应播放内容摘要，包含名称、版本、大小、哈希值、与原始数据关联关系等；
- d) 宜输出终端账户 ID。

6.2.5.3.2 跨链

当视频数据跨链传输时，视频上链信息应包含但不限于：

- a) 中继存证链 ID；
- b) 跨链存证交易证明。

6.3 AI 模块

6.3.1 算法管理

为保障系统的安全性，算法管理应符合以下要求：

- a) 支持算法选择、升级、调用等操作；
- b) 算法模型加密存储；
- c) 模型使用前进行校验；
- d) 算法管理过程上链存证，包括但不限于：

- 1) 模型版本信息;
- 2) 处理时间。

6.3.2 媒资管理

为保障应用层业务需要，媒资管理符合以下要求：

- a) 应具备媒资数据存储管理能力，包括但不限于：
 - 1) 数据备份;
 - 2) 数据恢复;
 - 3) 数据迁移。
- b) 应采取技术手段保障媒资数据的安全，包括但不限于：
 - 1) 数据加密;
 - 2) 访问控制。
- c) 应进行数据标准化处理，实现数据的交换与共享;
- d) 应具备媒资数据索引建立和媒资数据检索的功能;
- e) 删除数据应能恢复，但销毁数据不能恢复;
- f) 数据宜定期备份。

6.3.3 内容审核

为保障播放内容安全性，根据业务需求对音视频内容中的指定信息进行审核，应符合以下要求：

- a) 具备基于内容分类信息，提取语义结构化特征的能力;
- b) 具备根据审核结果对原始媒资进行标记的能力;
- c) 具备根据审核结果对原始数据的处理方式决策推荐的能力，推荐的决策包括但不限于删除、脱敏;
- d) 上链存证信息包括但不限于：
 - 1) 审核模型版本;
 - 2) 审核的起始和终止时间;
 - 3) 审核结果。

6.3.4 内容分类

为保障用户对音视频等数据查询和管理的效率及准确性，内容分类应符合以下要求：

- a) 分类的结果至少包含重要事件语义特征、所属标签类别;
- b) 具备对音频、视频等生成摘要的能力;
- c) 具备输入查询指令的入口，用于查询摘要结果;
- d) 存储在服务器端的摘要信息根据业务需求向终端发放;
- e) 上链存证信息包括但不限于：
 - 1) 分类结果;
 - 2) 模型名称、版本;
 - 3) 处理的起始和终止时间;
 - 4) 摘要名称、摘要类型;
 - 5) 原始数据的哈希值。

6.3.5 数据脱敏

为保障系统的隐私性，防止音视频等数据中敏感信息泄露，数据脱敏应符合以下要求：

- a) 具备对多媒体数据的脱敏能力，包括但不限于：
 - 1) 音频；
 - 2) 视频；
 - 3) 图片；
 - 4) 文本。
- b) 音视频数据脱敏后，能够正常播放；
- c) 根据数据拥有方的需求对原始数据进行可选择地脱敏和存储；
- d) 上链存证信息包括但不限于：
 - 1) 模型版本；
 - 2) 处理的起始和终止时间；
 - 3) 脱敏后数据哈希值；
 - 4) 脱敏数据与原始数据的关联关系。

6.3.6 音频识别

根据业务需求对音视频内容中的音频进行指定特征识别，音频识别应符合以下要求：

- a) 具备识别指定特征的能力，指定特征包括但不限于：
 - 1) 人声特征，如呼救声、啼哭声等；
 - 2) 动物叫声特征，如猫叫声、狗叫声等；
 - 3) 环境音特征，如破碎声、施工声等。
- b) 能够配置需要识别的单个或组合的音频特征；
- c) 具备输出识别结果的接口；
- d) 上链存证信息包括但不限于：
 - 1) 识别结果；
 - 2) 特征名称、版本；
 - 3) 标记的起始和终止时间；
 - 4) 原始数据的哈希值。

6.3.7 视频识别

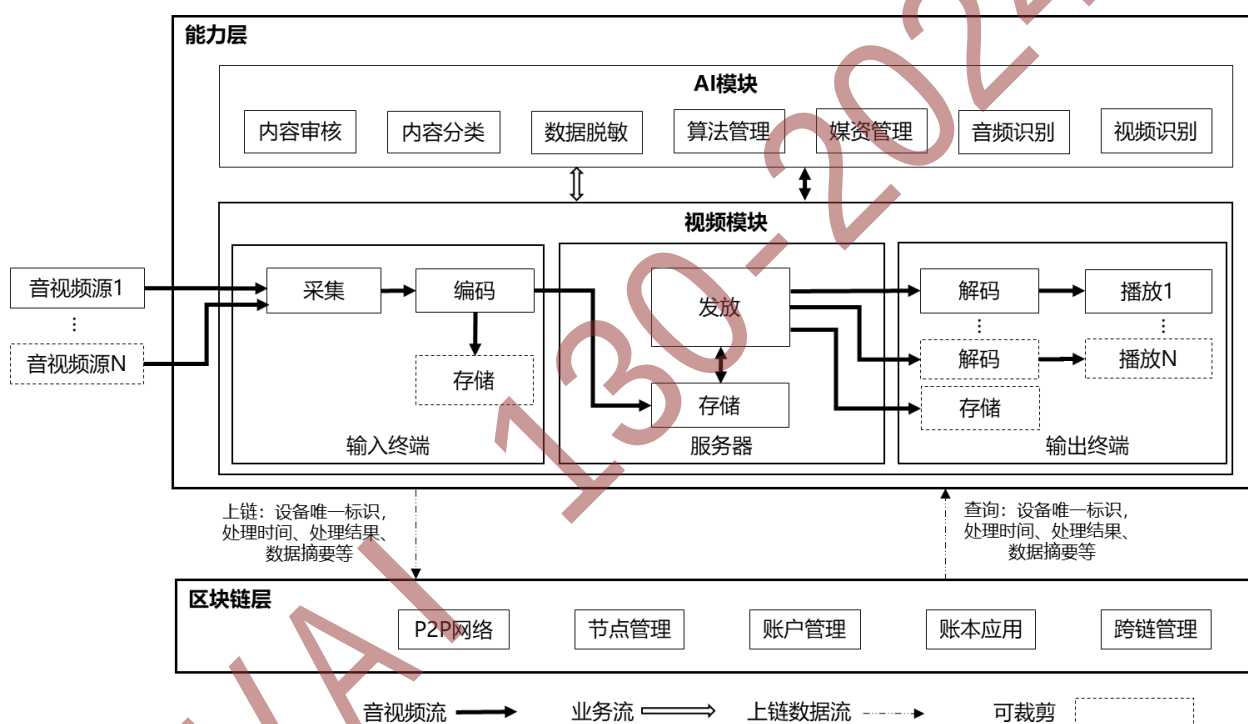
根据业务需求对音视频内容中的视频进行指定特征识别，视频识别应符合以下要求：

- a) 具备识别指定特征的能力，包括但不限于：
 - 1) 静态特征，如人脸、车号牌等；
 - 2) 动态特征，如摔倒、进食等。
- b) 能够配置需要识别的单个或组合的视频特征；
- c) 具备输出识别结果的接口；
- d) 上链存证信息包括但不限于：
 - 1) 识别结果；
 - 2) 特征名称、版本；
 - 3) 标记的起始和终止时间；
 - 4) 原始数据的哈希值。

附录 A (资料性) 系统工作流程

A.1 系统工作流程

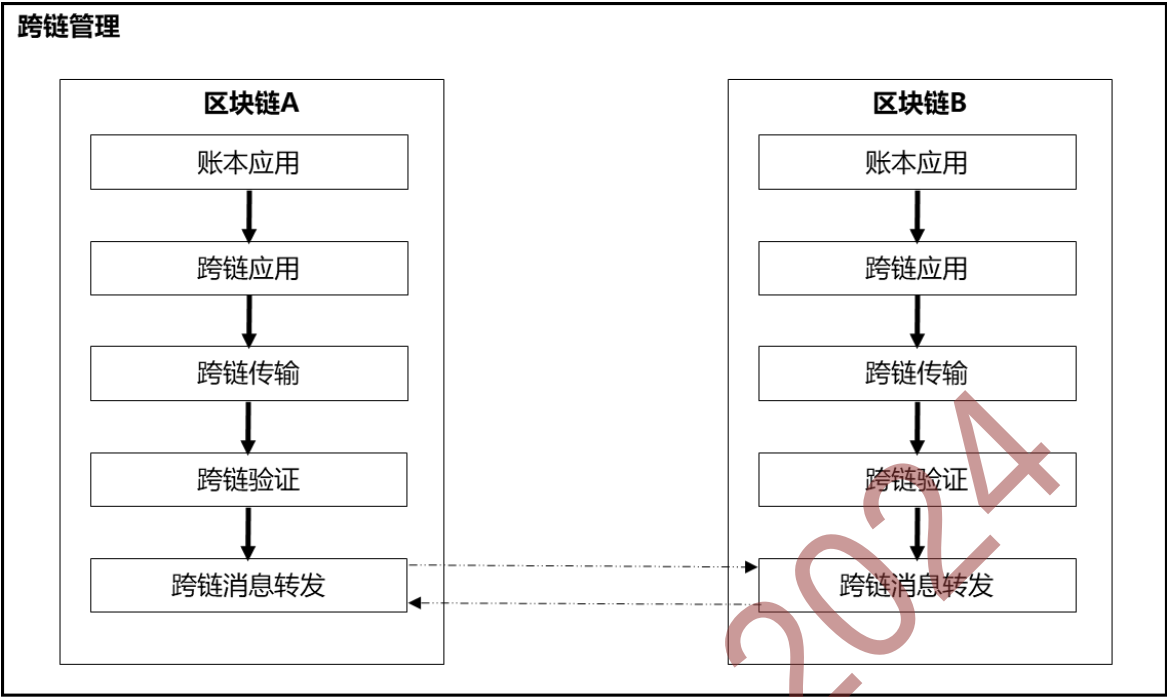
数据拥有方通过输入终端对数据进行采集、存储、发放；数据处理方根据业务需要，启用AI模块的内容分类、内容审核、数据脱敏等功能对数据进行处理，并将处理过程的信息进行上链存证；数据使用方根据业务需要发起数据调用需求，请求成功通过输出终端调用相关数据，进行播放、存储等。整个系统通过区块链进行统一账户管理，并对系统中数据全生命周期的流转信息进行上链存证；同时通过跨链管理，支持多个区块链之间的信息传递、查询、溯源等功能。系统的工作流程见图A.1。



图A.1 系统工作流程示意图

A.2 跨链工作

跨链管理用于实现对音视频资源的跨链通信与跨链验证。账本应用提供在原区块链进行媒资管理的功能，跨链应用提供了适配并实施跨链交互的能力以及跨链可追溯性能力，跨链传输提供跨链交互过程中信息可信传输的能力，跨链验证保证跨链交互过程中的信任传递，跨链消息转发保证跨链交互链上与链下可信通信。系统跨链管理框架见A.2。



图A. 2 跨链工作示意图

附录 B

(资料性)

场景应用

B.1 视频会诊系统

B.1.1 概述

目前，医联体内数据共享存在信任和协同困难等问题，主要表现为患者的健康数据、医疗档案等信息呈现碎片化分布，对患者在跨地域、跨医疗/健康机构就诊时造成不便；同时也一定程度的影响了医疗人员为患者提供准确、便捷的医疗服务。为解决以上问题，可采用基于区块链的视频会诊系统，医护通过患者提供的医疗/健康数据的摘要，在最小使用范围内向患者申请相关原始医疗健康数据的获取权限。数据传输过程加密，区块链对数据流转过程进行存证，以保证数据交换全过程的可追溯。患者可以实现细颗粒度地访问、控制权限，有效保护个人隐私，实现个人信息主体对隐私信息的完全自主控制。该系统可支撑医院之间的去中心化数据共享的实际应用需求，保证患者医疗/健康数据的完整性和安全性。视频会诊系统有效解决医疗信息资源共享应用中信任孤岛、数据所有权问题，使医疗信息资源共享在医疗联合体多元主体参与的背景下具有较强适应性。

B.1.2 视频问诊业务

患者和医护需要在各自的终端进行账户注册，患者将个人医疗/健康数据生成摘要，并对个人医疗/健康数据进行加密，生成加密数据。摘要数据上传至区块链，加密数据上传至云服务器，患者在进行视频问诊时，将个人医疗/健康数据摘要列表发送至医护终端，医护根据该列表向患者申请最小使用范围内的摘要列表。患者根据该最小使用范围内的摘要列表，从云服务器上获取加密后的医疗/健康数据到患者终端。患者使用自己的密钥进行解密，再使用医护的密钥进行加密，加密后的数据发送到医护终端，医护将接收到的数据进行解密，并通过数据摘要进行完整性、真实性校验。架构模型见图B.1。

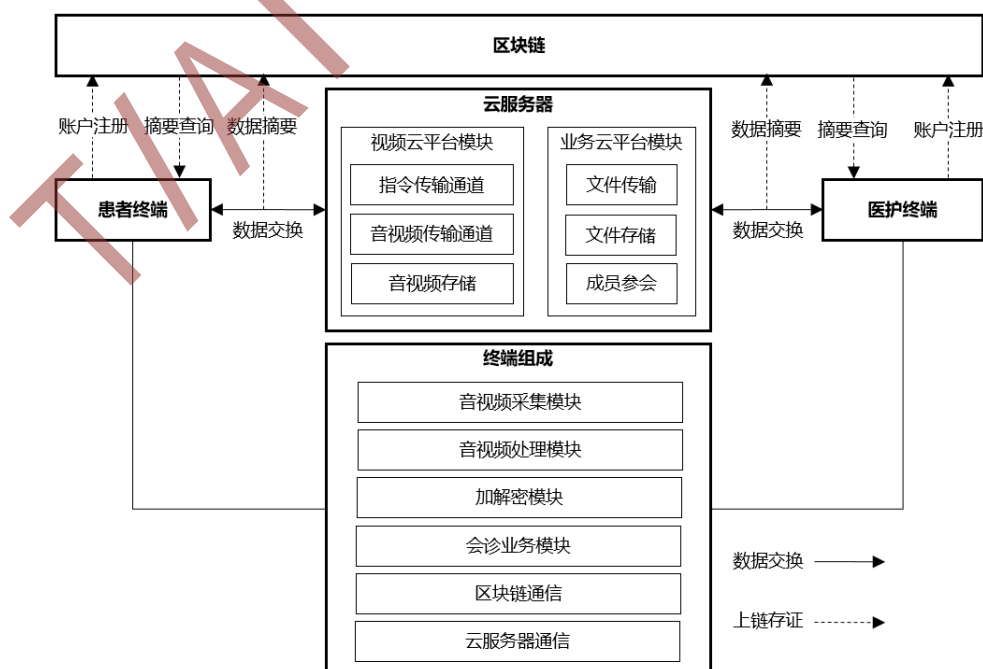


图 B.1 基于区块链的可信赖视频会诊系统架构模型

B.2 智能交通监控系统

B.2.1 概述

智能交通监控系统通过AI算法从海量的低价值原始数据中提取高价值信息,以降低服务器的数据存储压力,提高事件检索效率。通过区块链对系统中产生的重要信息进行上链存证,保证该高价值信息的不可篡改性、流转记录可追溯。

B.2.2 工作流程

智能交通监控系统由输入终端、AI模块、云服务器、区块链模块、输出终端五部分组成,视频数据流转见图B.2。

- 输入终端将采集的视频传输至 AI 模块;
- AI 模块对该视频进行处理,识别出事件后将视频片段进行唯一性命名根据需求对敏感信息进行处理;
- 视频片段上传至云服务器进行备份存储;
- 将该事件视频片段的哈希值,以及唯一性命名、时间等信息上传至区块链模块,通过共识机制完成在区块链模块上的存证操作;
- 授权用户从输出终端通过视频唯一性命名向系统发起请求,通过视频的哈希值校验,对该事件真实性进行验证,该验证操作也可通过跨链调用对跨域存储的视频进行获取及验证。系统将视频片段、校验结果、时间等信息返回给输出终端的授权用户。

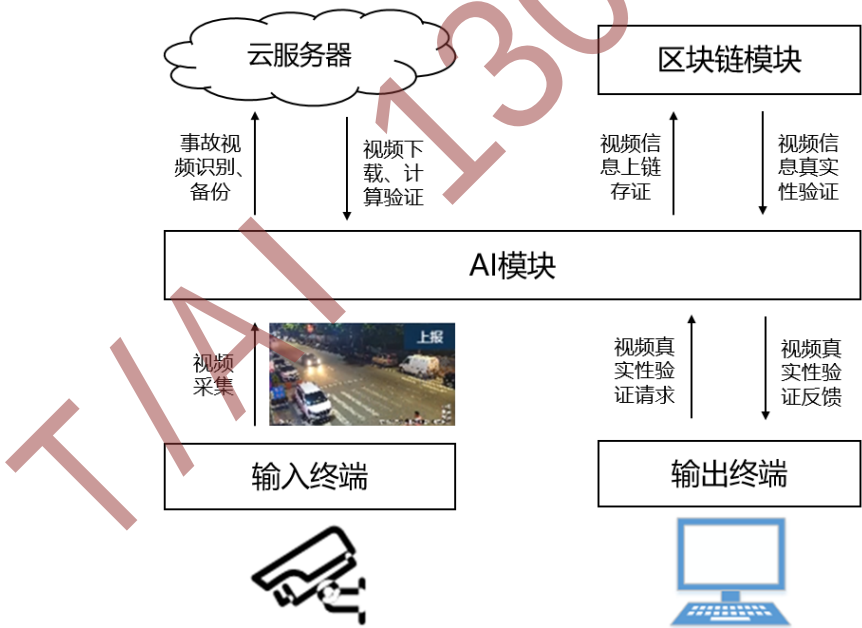


图 B.2 视频数据流转图

参 考 文 献

- [1] GB/T 41867-2022 信息技术 人工智能 术语
 - [2] T/CESA 1304-2023 人工智能 可信赖规范 第 1 部分：通则
-

T/AI 130-2024