

团 体 标 准

T/ACEF XXX-XXXX

基于区块链的生活垃圾焚烧飞灰处理系统 技术规范

Technical specification of Blockchain-based on fly-ash treatment system
of municipal solid waste incineration power plant

(征求意见稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中 华 环 保 联 合 会 发 布

目 录

- 前 言 I
- 1 范围 1
- 2 规范性引用文件 1
- 3 术语和定义 1
- 4 总体要求 2
- 5 系统功能 2
- 6 区块链平台性能 5

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。

本文件由中华环保联合会提出并归口。

本文件主要起草单位：

本文件参编单位：

本文件主要起草人：

基于区块链的生活垃圾焚烧飞灰处理系统技术规范

1 范围

本文件规定了基于区块链的生活垃圾焚烧飞灰处理系统的总体要求、系统功能和平台性能。
本文件适用于区块链技术在生活垃圾焚烧飞灰主要处理流程的环境管理应用。

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 17903	信息技术 安全技术 抗抵赖
GB/T 18485	生活垃圾焚烧污染控制标准
GB/T 32907	信息技术安全 SM4分组密码算法
GB/T 32918	信息安全技术 SM2椭圆曲线公钥密码算法
GB/T 42570	信息安全技术 区块链技术安全框架
HJ 1134	生活垃圾焚烧飞灰污染控制技术规范（试行）
YD/T 3747	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

生活垃圾焚烧飞灰 fly-ash from municipal solid waste incineration

生活垃圾焚烧设施的烟气净化系统捕集物和烟道及烟囱底部沉降的底灰。本标准中简称“飞灰”。

[来源：HJ 1134-2020, 3.1]

3.2

区块链 blockchain

将区块顺序相连,并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

[来源：GB/T 42570-2023, 3.2]

3.3

区块链技术架构 blockchain technical architecture

运行在区块链网络中的节点中,提供区块链系统功能的软件和存储实体的集合,包括基础层、核心层和接口层的密码算法、共识机制、智能合约等功能组件。

[来源: YD/T 3747—2020, 3.1.3]

3.4

联盟链 consortium blockchain

针对特定组织团体开放,节点通过管理员或管理机构授权后方可加入,所有共识节点的地址互相互知并可互相通信的区块链。

[来源: GB/T 42570-2023, 3.11]

3.5

智能合约 smart contract

由用户部署在区块链中,且执行结果记录于区块链的计算机程序。

[来源: GB/T 42570-2023, 3.12]

4 总体要求

4.1 飞灰收集、贮存及运输污染控制应符合 HJ 1134 的规定。

4.2 基于区块链的生活垃圾焚烧飞灰处理系统应对下列数据上链和数据校验:

- a) 垃圾进厂数据;
- b) 垃圾焚烧工艺设备数据;
- c) 垃圾处理量数据及飞灰产生量数据;
- d) 飞灰螯合混炼中的螯合剂添加量数据以及稳定化飞灰贮存等飞灰处理流程数据。

5 系统功能

5.1 总体架构

5.1.1 基于区块链的生活垃圾焚烧飞灰处理系统总体架构如图 1 所示。

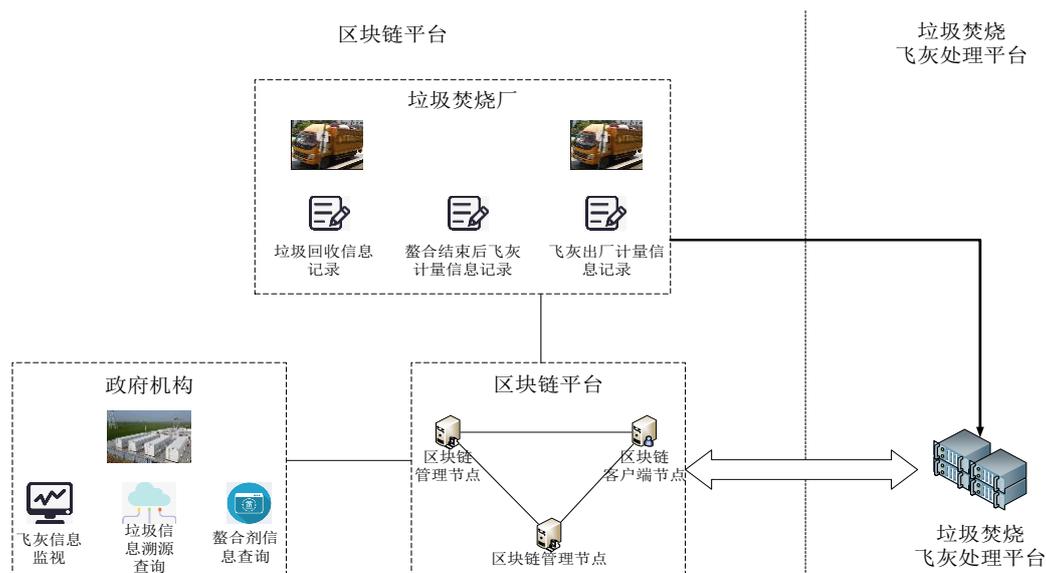


图 1 基于区块链的生活垃圾焚烧飞灰处理系统总体架构图

5.1.2 系统总体架构应满足下列要求：

- a) 区块链平台结构应根据访问角色构建，应记录生活垃圾焚烧飞灰处理平台和垃圾回收平台用户角色推送的不同类型的重要数据。生活垃圾焚烧飞灰处理平台和垃圾回收用户重要数据应直接推送到区块链平台中；
- b) 区块链平台应根据应用场景，规定上链频率；
- c) 区块链平台应对用户上链数据量作出限制，一次上链数据量不应过大；
- d) 生活垃圾焚烧飞灰处理平台应实现与区块链平台信息交互。生活垃圾焚烧飞灰处理平台应为区块链提供用户登录、生活垃圾焚烧飞灰处理信息披露、垃圾回收量信息监视和区块链监视等辅助服务；
- e) 生活垃圾焚烧飞灰处理平台应建立用于存储区块标识的关系型数据库，通过关系型数据库的高效查询，提高数据查询的效率。

5.2 技术架构

5.2.1 基于区块链的生活垃圾焚烧飞灰处理系统技术架构图如图 2 所示。

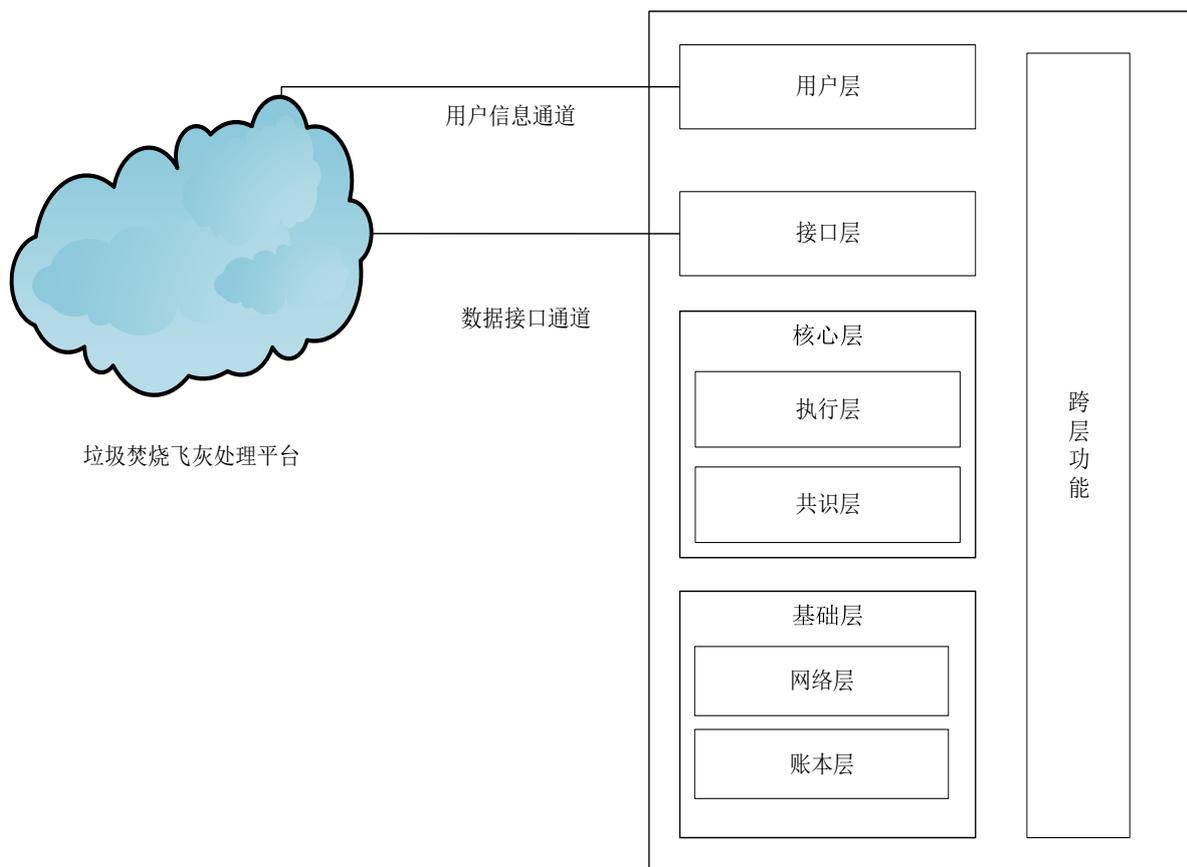


图 2 基于区块链的生活垃圾焚烧飞灰处理系统技术架构图

5.2.2 技术架构应满足下列要求：

- a) 基础层应提供区块链平台正常运行的运行环境和基础组件，应包括账本层和网络层，功能应包括存储、计算和对等网络。账本应为多通道单链结构，支持对有向无环图等新一代账本结构的可扩展支持。网络应为确定性网络；
- b) 核心层应基于基础层提供的硬件或网络基础体系实现相应功能，并为接口层提供相关功能支持服务。核心层应包括执行层和共识层，功能应包括共识机制、密码服务、账本记录、交易 / 事务处理、智能合约和成员服务等，共识层应支持 PoW/PoS/PBFT 等共识协议，可根据业务场景需要设置，并可扩展支持对新一代共识协议；
- c) 接口层应通过调用核心层功能组件，提供可靠接入服务支撑。接口层功能应包括管理接口、客户接口和外部接口。管理接口应为节点状态查询、网络状态监控和节点服务配置等功能的接口；客户接口应具备用户层对账本信息查询和事务操作处理等功能。生活垃圾焚烧飞灰处理平台应通过区块链提供的外部接口，对区块链与外部系统数据交互操作；
- d) 用户层应调用区块链平台用户层接口，对用户信息 CA 认证操作和用户登录区块链平台操作；
- e) 跨层功能应提供跨越多个功能层次能力的功能组件，应包括开发、运营、审计和安全等；
- f) 区块链平台应实现与生活垃圾焚烧飞灰处理平台的通信，应通过生活垃圾焚烧飞灰处理平台采集的飞灰处理信息，作为上链的数据支撑。

5.3 应用服务

5.3.1 进厂垃圾数据统计

生活垃圾焚烧飞灰处理平台应对每日进厂垃圾称重信息进行数据采集，并将采集信息上链，并为每日进厂垃圾称重信息提供上链凭证和数据校验功能。

5.3.2 飞灰处理螯合剂添加量信息数据上链及溯源

生活垃圾焚烧飞灰处理平台应对添加螯合剂情况以及混炼机电流量监视和采集，并将采集信息上链，并为处理飞灰添加螯合剂量提供上链凭证和数据校验功能。

5.3.3 稳定化飞灰暂存量数据上链及溯源

5.3.3.1 生活垃圾焚烧飞灰处理平台应对每批次处理完成的稳定化飞灰贮存进行监视、统计、自行检测。

5.3.3.2 对完成稳定化飞灰的检测报告上送到垃圾焚烧飞灰处理系统数据库，并生成测试报告字典，将测试报告字典上链以及提供上链凭证和数据校验功能。

5.3.3.3 将飞灰暂存信息上链，同时为稳定化飞灰暂存量提供上链凭证和数据校验功能。

5.3.4 飞灰出厂数据上链及溯源

出厂的固态飞灰重量应进行测量统计，将固态飞灰重量测量统计信息上链，并对重量信息提供上链凭证和数据校验功能。

5.3.5 飞灰处理信息披露

基于区块链的生活垃圾焚烧飞灰处理平台应按日、月、年维度对垃圾入厂情况、垃圾焚烧量、飞灰产生量和螯合剂使用量进行数据披露。

5.3.6 螯合剂信息上链共识

平台每半年到一年应对合格的螯合剂进行数据收集，并将合格的螯合剂数据上链，实现合格螯合剂信息披露。

6 区块链平台性能

6.1 区块链结构

区块链平台宜采用联盟链。

6.2 上链数据结构

- 6.2.1 基于区块链的生活垃圾焚烧飞灰处理服务平台应对垃圾焚烧量 and 处理飞灰的螯合剂使用量等关键信息上链管理。
- 6.2.2 生活垃圾焚烧飞灰处理流程应包括垃圾进入焚烧厂前称重,飞灰螯合过程,飞灰螯合稳定化暂存,飞灰出厂前称重等流程。
- 6.2.3 垃圾进厂数据上链应对每日进入垃圾焚烧厂的信息上链,上链数据结构应包括进厂垃圾车车牌号,进厂时间,重车重量和轻车重量等数据。
- 6.2.4 飞灰处理螯合剂添加量信息数据上链应对飞灰螯合过程中的数据上链,上链数据结构应包括螯合时间,螯合剂品牌,螯合剂添加量、水的添加量以及混炼机电流量等数据。
- 6.2.5 稳定化飞灰暂存量数据上链应对已完成稳定化贮存飞灰的信息上链,上链数据应包括飞灰贮存批次,飞灰取样时间以及飞灰测试报告字典等数据。
- 6.2.6 飞灰出厂数据上链应对飞灰出厂时相关数据上链,上链数据应包括出厂垃圾车车牌号,出厂时间,重车重量和轻车重量等数据。
- 6.2.7 螯合剂信息上链应对螯合剂相关信息上链,上链数据应包括产品编码,产品名称,生产厂家以及使用剂量等数据。

6.3 上链频率要求

- 6.3.1 生活垃圾焚烧飞灰处理流程应包括垃圾进入焚烧厂前称重,飞灰螯合过程,飞灰螯合稳定化暂存,飞灰出厂前称重等流程。
- 6.3.2 数据上链频率应根据数据来源及数据应用目的确定。并应符合下列规定:
 - a) 垃圾进入焚烧厂前称重统计信息应将每日采集的信息汇总后上链;
 - b) 垃圾焚烧厂应对飞灰螯合、稳定化飞灰暂存检测和飞灰出厂称重数据采集,并将每批次采集信息上链;
 - c) 平台应按每半年至一年对螯合剂数据收集,并将收集到的合格的螯合剂数据上链。

6.4 访问用户授权

- 6.4.1 访问区块链的用户应根据业务需求提供认证和身份管理机制,建立身份管理策略。
- 6.4.2 对于区块链平台准入的用户,应根据业务需求提供权限管理功能。
- 6.4.3 平台应遵循最小化授权原则,设定权限控制。

6.5 区块链平台

- 6.5.1 上链区块文件容量不应超过 64 M,一个账本保存的最大数据量宜为 61 TB。
- 6.5.2 区块链平台性能应符合下列规定:

- a) 区块链平台应实现秒级出块；
- b) 区块链平台吞吐量应保证 TPS 为 200~300。

6.5.3 区块链平台审计应满足下列要求：

- a) 区块链平台应对每日上链次数统计；
- b) 区块链平台应对每日下链次数统计；
- c) 区块链平台应对查链次数统计。

6.5.4 区块链平台扩展能力应满足下列要求：

- a) 区块链平台应支持新型账本结构的可扩展能力，允许用户经过共识扩容，增加/删除等管理节点，允许新增节点按业务需求同步更新账本，删除节点具备账本数据自毁功能，并取消已删除节点账本的同步功能；
- b) 区块链平台应支持新型共识算法的可扩展能力，支持用户通过共识达成共识算法的更新；
- c) 区块链平台应支持区块链浏览器，通过区块链浏览器，对区块链平台运行情况监视；
- d) 区块链平台应支持 BaaS 服务。

6.6 区块链安全

6.6.1 密码应用安全应符合下列规定：

- a) 密码算法和密码技术应符合 GB/T 17903、GB/T 32907、GB/T 32918 的规定；
- b) 密码产品与密码模块应通过国家密码管理部门核准；
- c) 密码服务应通过国家密码管理部门许可。

6.6.2 共识机制安全应满足下列要求：

- a) 区块链平台应选择证明安全的共识机制；
- b) 共识机制应具有符合业务需求的容错性，容错性应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等的容错性；
- c) 共识机制应满足应用场景的强一致性、最终一致性等一致性要求。最终一致性算法，应具备满足业务需求的收敛速度和确认时间；
- d) 共识机制应具备分叉管理能力；
- e) 共识机制应保证公平。

6.6.3 智能合约安全应满足下列要求：

- a) 智能合约应具备防篡改和抗抵赖性，智能合约应针对合约约定条件和事项，按规则强制执行；
- b) 智能合约编程语言宜采用最新稳定版本，应避免使用存在安全问题的版本，编程语言的编译器应确保一致性，智能合约源码在编译成字节码后前后逻辑应一致；
- c) 合约代码应满足代码书写规范、逻辑要求等规范性要求，可对合约代码进行完整性测试和形式化验证；

- d) 智能合约应具备合约创建、部署、升级、触发、执行、废止等生命周期管理功能。合约每次修改应为独立版本，合约升级操作应采用接口调用方式，升级操作应记录在区块中，升级后应保留前一版本；
- e) 智能合约宜具备可终止性，宜对其支配的资源限制。合约虚拟机应具有合规性检测，在处理非合规代码时应向用户提示；
- f) 合约代码应在沙盒中运行，沙盒选择或设计应避免出现沙盒逃逸等问题，对于与区块链平台外部数据交互的智能合约，外部数据源影响范围应仅限于智能合约范围内，不应影响区块链平台运行；
- g) 区块链平台应支持智能合约应急响应机制，在发现合约漏洞后，区块链平台应及时检查和修复。

6.6.4 成员服务安全应满足下列要求：

- a) 对于联盟链和私有链，应根据业务需求提供认证和身份管理机制，支持建立身份管理的策略，支持利用身份认证方法支撑身份管理策略，支持在身份认证的基础上建立用户身份管理机制；
 - b) 对于联盟链和私有链，应根据业务需求提供权限管理功能；
 - c) 应根据业务需求提供隐私保护功能，应支持通过认证机构代理用户在区块链上进行事务处理，应支持将数据传输限制在特定授权节点间，应支持用加解密方法对用户数据访问采用权限控制，应支持对事务发起方 / 接收方的信息及事务信息隐藏；
 - d) 应遵循最小化授权原则，设定权限控制；
 - e) 远程管理时，应采取使用 TLS 加密传输技术，防止鉴别信息在网络传输过程中被窃听的措施；
 - f) 系统应提供可扩展的成员安全功能。
-