ICS 35.240.99
CCS L 77

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX-XXXX

基于区块链技术的数据资产化可信服务平台

Data Asset Trusted Service Platform Based on Blockchain Technology

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国商业企业管理协会　　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。

本文件由武汉泰铭恒创信息技术股份有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：武汉泰铭恒创信息技术股份有限公司、.....。

本文件主要起草人：XXX、XXX、XXX.....。

基于区块链技术的数据资产化可信服务平台

1 范围

本文件规定了基于区块链技术的数据资产化可信服务平台的术语和定义、缩略语、基本要求、平台框架、技术要求、功能要求、安全要求、对接方案及应用场景、测试与运行维护。

本文件适用于基于区块链技术的数据资产化可信服务平台的设计和应用。

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 2887 计算机场地通用规范

GB/T 8567 计算机软件文档编制规范

GB/T 16680 系统与软件工程 用户文档的管理者要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 28035 软件系统验收规范

GB/T 43572 区块链和分布式记账技术 术语

GB/T 43575 区块链和分布式记账技术 系统测试规范

GB 50174 数据中心设计规范

GA/T 708 信息安全技术 信息系统安全等级保护体系框架

3 术语和定义

GB/T 43572 界定的以及下列术语和定义适用于本文件。

3.1

数据资产化 data capitalization

将数据转化为具有经济价值的资产的过程，包括数据的确权、评估、管理和运营等。

3.2

可信服务平台 trusted service platform

基于区块链技术构建的，为数据资产化提供可信服务的平台，包括数据的可信存储、共享、管理和审计等功能。

4 缩略语

下列缩略语适用于本文件：

DAG：有向无环图（Directed Acyclic Graph）

YARN：另一种资源协调者（Yet Another Resource Negotiator）
SOA：面向服务的架构（Service-Oriented Architecture）

5 基本要求

5.1 一般要求

5.1.1 平台建设应遵循整体设计、统筹建设，对接审批、优化服务，统一标准、安全可靠的原则。应易于操作、界面美观、方便用户进行浏览、搜索和交互。
5.1.2 平台中涉及涉密数据时，应符合国家和行业保密管理的规定。
5.1.3 平台运行环境应符合国家信息安全保密管理的规定，平台应对用户实行统一身份认证，实现分权 分域管理。
5.1.4 平台的密码使用和管理应符合国家密码管理的规定。
5.1.5 平台应通过验收，平台验收应符合本文件和 GB/T 28035 的有关规定。
5.1.6 平台应及时进行日常管理维护、软件维护、数据维护、运行环境维护等。
5.1.7 平台文档内容和编排应满足 GB/T 8567 的要求，平台文档管理应满足 GB/T 16680 的要求。

5.2 运行环境要求

5.2.1 上位机、分机和外设配置

5.2.1.1 上位机、分机和外设配置应根据规模和业务量来决定，应满足系统共享、兼容和高效使用的要 求，具有通用性，易于升级。
5.2.1.2 计算机机房场地应满足 GB/T 2887 的要求，机房设计应满足 GB 50174 的要求。

5.2.2 网络环境

5.2.2.1 严格按照国家有关保密政策的要求配置，应具有可靠性、安全性、开放性、便于扩充等特性。
5.2.2.2 涉密的数据只能在涉密网中运行，非涉密的数据才可在非涉密网中运行。
5.2.2.3 根据 GB/T 22239 及数据安全等级设定相应网络安全设备，建立相一致的网络环境安全管理制度。
5.2.2.4 选择大于 20 M 的网络带宽出口，以提高信息服务的访问效率。
5.2.2.5 建立较为完备的网络日常管理维护制度，对网络系统进行日常维护；宜配置网络管理软件，实现对网络资源进行管理维护，实现故障管理、配置管理、安全管理等方面的功能。

5.2.3 服务器系统

5.2.3.1 符合国家现行标准配置，应具有可靠性、安全性、开放性、便于扩充等特性。
5.2.3.2 服务器的 CPU 配置定制应可定制并满足特定要求，可根据实际需求提高服务器配置。
5.2.3.3 建立较为完备的硬件日常管理维护制度，对硬件进行日常维护。

5.2.4 基础软件环境

5.2.4.1 应配置操作系统软件、网络安全管理软件，对系统进行合理的管理。
5.2.4.2 应配置相应的数据管理软件，软件应支持空间数据与属性数据的统一管理，宜支持海量数据管理能力。
5.2.4.3 平台模块的开发应根据业务进行拆分，遵循一个业务一个服务的拆分原则，达到通用性业务服务模块的要求。各模块应可独立部署，并不受时间影响。

5.3 运行数据管理

5.3.1 管理要求

5.3.1.1 各类数据及元数据应按本文件的规定，建立数据库，且应满足平台高效运行和查询检索的需要。

5.3.1.2 数据处理完成后，应进行成果质量检查，通过后方可提交系统入库。

5.3.1.3 数据均应及时更新，并应保证其准确性与有效性；数据更新前应做历史数据的备份工作。

5.3.1.4 数据的安全保密应符合 GA/T 708 第二级基本要求的规定。

5.3.2 运行数据

5.3.2.1 平台运行数据应通过系统的维护管理功能进行定义和更新维护。

5.3.2.2 数据传输应符合以下要求：

a) 应具备纵向传输的数据加密功能；
b) 应支持数据传输的机密性和完整性保护；
c) 应具备双向身份认证功能；
d) 应支持监控信息的唯一性控制与可追溯机制；
e) 应在监控信息规定的数据范围内采集数据；
f) 应具备数据传输通道状态校验功能；
g) 应具备数据传输通道被非法入侵或专线通道串线造成误控的判定功能。

5.4 性能要求

5.4.1 一般要求

5.4.1.1 系统的存储备份应满足以下要求：

a) 基础数据库数据永久保存；
b) 业务数据库数据存储期限不少于 3 年。

5.4.1.2 应支持 32 位和 64 位的计算环境，支持多种主流操作系统。

5.4.2 可靠性

5.4.2.1 应运行稳定，准确完成多源异构数据采集、存储、管理任务，并具有容错能力。

5.4.2.2 系统软件及硬件的升级不应影响服务系统的运行及服务的提供。

5.4.3 易用性

应提供联机帮助，软件中各子系统用户界面风格应一致，应搭建统一风格的接口软件，应易学易用。

5.4.4 集成性

应具有开放式体系结构，提供多种数据接口，与其他通用应用软件及专业应用软件之间应实现集成。

5.4.5 可扩展性

结构应具有可扩展性，系统应有统一的中控系统，可实现对各个应用模块的数据维护管理。并支持通过增加服务器或换用处理能力更强的服务器的方式对系统进行扩展。组成系统的每个逻辑单元都可独立于其他单元进行升级。

6 平台框架

平台采用多层、分模块、分服务的分布式灵活搭建方式进行框架构建。共包含物理资源层、基础资源层、虚拟层、数据资源层、平台层（大数据＋区块链）、可信服务层、展示层、服务接入层八大层级结构，每一层次分模块、分应用构建组合而成，在满足可信服务应用场景需求的同时，可以进行多维度横向和纵向组合，从而具备良好的适配性和扩展性。平台总体框架如图1所示。

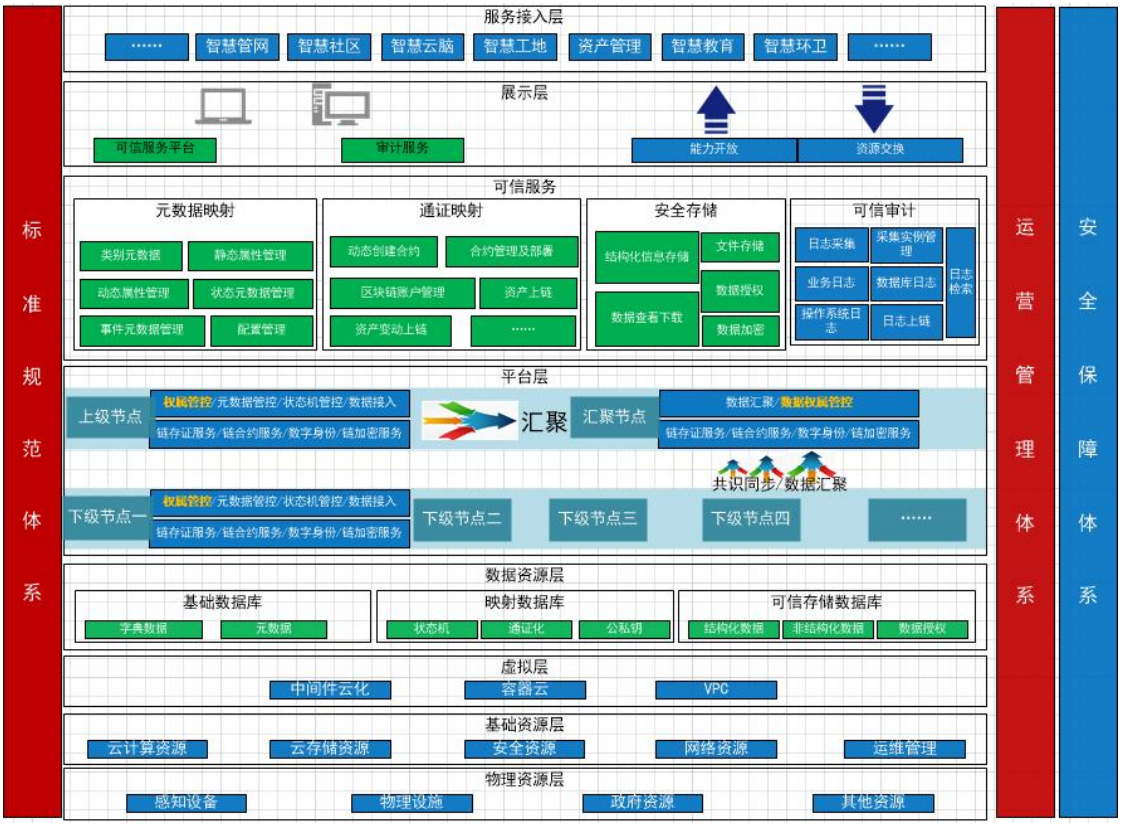

图 1 平台总体框架图

7 技术要求

7.1 区块链技术

采用DAG结构的区块链技术，支持多笔交易在互不干扰情形并行执行，提高交易并行执行能力和效率。

7.2 大数据技术

利用大数据相关技术，具备高度容错性和高吞吐量的数据效率，解决海量数据存储问题，在YARN集群服务器管理平台下，应用Hive，Spark和Druid离线数据处理技术，实现包括数据总结、查询和分析、分布式计算、大数据的分析和挖掘等功能。采用Spark Stream和Flink对平台的审计大数据进行分析和挖掘。

7.3 微服务技术

7.3.1 采用 SOA，使用 Spring cloud 的微服务体系进行研发，实现服务的模块化和灵活构建。

7.3.2 采用前后端分离的编程模式，前端框架采用 Vue＋EnlementUI，后端采用 Spring Boot＋Spring Cloud＋Mybatis-Plus 微服务框架，被拆分成的每一个小型服务均围绕着平台中的某一项或者耦合度较高的业务功能进行构建,且每个服务维护自身的数据存储、业务开发自动化测试案例以及独立部署机制。

7.4 可插拔共识机制

应支持可插拔的共识机制，允许用户在不同的应用场景中选择适合的共识算法。

8 功能要求

8.1 模块功能

应提供元数据配置中心、状态机配置中心、通证管理中心、公私钥管理中心、智能合约管理中心、协同/自办业务审计中心、业务/操作系统/数据库审计中心、资产审计中心、开放服务中心等功能核心模块。各模块功能要求为：

a) 提供元数据配置中心，为各个行业标准的基准数据提供统一管理；
b) 提供状态机配置中心，为各种数据提供动态配置服务，通过可视化机制实现节点及事件分发、流转、上链的灵活配置；
c) 提供通证管理中心，对上链资产数据进行统一管理；
d) 提供公私钥管理中心，所有进入平台的数据需有授权分配的对应公钥才可进入或查看，数据通过私钥进行加密上链，确保可信服务体系的安全；
e) 提供智能合约管理中心，每个通过可视化状态机功能动态配置的事件及属性状态机，均会自动生成特有的智能合约，数据根据生成的智能合约进行上链；
f) 提供协同/自办业务审计中心，各个自办业务或者跨系统跨部门的业务流转轨迹均可在此审计中心进行审计，轨迹一旦形成不可篡改；
g) 提供业务/操作系统/数据库日志审计中心，所有接入平台的系统，均可分别从业务日志、操作系统日志、数据库日志等维度进行日志审计；
h) 提供资产审计中心，对国有的有形资产、无形资产、文物文化等资产提供全流程的审计功能；
i) 提供开放服务中心，为系统接入提供统一标准和多种灵活接入方式，方便外围数据的接入和对接。

8.2 平台可视化功能

8.2.1 可视化态势大屏

8.2.1.1 应从服务通证维度进行态势分析，可实时从全局维度查看目前已有及最近新增的可信服务数据态势。

8.2.1.2 应支持从区块链浏览器维度实时查看链上数据情况，以及实时产生的区块详情。

8.2.1.3 应从业务角度对各个业务领域的数据进行星空图概览，每个星图可以点击查看实际的业务详情。

8.2.2 数字映射

数字映射系统应提供从元数据、状态机配置、数据采集、归集、数据质量监测、数据上链、区块链通证等整个环节的流转服务。系统功能模块包括：

a) 通证状态机管理；

b） 元数据管理；
c） 通证管理；
d） 公钥管理；
e） 标准规范；
f） 系统管理。

8.2.3 可信审计

可信审计系统应提供协同业务、自办业务、资产审计、业务日志审计、数据日志审计、系统日志审计等重要审计及上链功能。

9 安全要求

9.1 信息媒体安全

系统相关的媒体数据及媒体本身应合法、合规、安全可靠。

9.2 信息安全

应符合GB/T 20270、GB/T 20988的相关要求。

9.3 访问控制

访问控制应满足以下要求:
a） 应支持基于调度员、监控员、运维人员、审计管理员、系统管理员等角色的访问控制功能；
b） 应支持角色与权限的绑定,不同角色人员应按照工作范围、职责分工分配相应的访问控制权限；
c） 应支持角色互斥功能，禁止配置同时具有控制和维护修改权限的角色；
d） 应依据安全策略控制用户对监控信息等文件或数据库表等客体的访问。

9.4 数据完整性

数据完整性应满足以下要求：
a） 应具备对监控信息等关键数据的存储完整性保护功能；
b） 应具备对监控信息、信息点、控制命令等关键数据的传输完整性保护功能；
c） 应在检测到关键数据完整性错误时，提供必要的恢复手段。

9.5 数据安全及备份恢复

9.5.1 数据保密性

对公民身份信息、活动信息等敏感数据，应进行加密存储。

9.5.2 数据备份恢复

数据备份恢复应包括：
a） 应有数据备份机制，并对备份数据进行保护；
b） 在使用恢复的数据前应校验其可用性、完整性；
c） 日志数据、采集数据、基础数据、主题数据、业务数据和知识库数据采用每日全量备份的策略备份；

d) 采用反向代理技术实现 WEB 集群服务的负载均衡，支撑数据存储、处理、运算及应急处置的系统应保证硬件冗余，避免关键节点存在单点故障。

10 对接方案及应用场景

10.1 对接方案

可信服务平台应提供统一标准的多种对接方式，可与地理信息、物联网、资产管理、管网、交通、城管等多个部门的多套信息化系统进行对接,达到资源开放而不共享,跨部门之间数据可信的服务体系。

10.2 应用场景

可信服务平台的应用场景延展如下：

a) 城市治理：应用于城市治理的证据存储、资金监管、民事登记、政务流程监管等场景；
b) 公共服务：应用于公共服务的病人健康记录、学生教员记录、教育证书、智慧供应链等场景；
c) 数据共享：应用于数据共享的数据路径追溯、信息化日志审计等场景；
d) 数字经济：应用于数字经济领域的资产流通、征信记录、金融账本等场景。

11 测试与运行维护

11.1 软件测试

按GB/T 22239、GB/T 22240规定的安全级别确定检查和测试的项目。测试应符合GB/T 43575的规定。

11.2 测试范围

11.2.1 功能性需求测试范围

功能性需求测试的范围包括但不限于数字化与智能化应用分析模块。

11.2.2 非功能性需求测试范围

非功能性需求测试的范围包括:

a) 性能测试需求：测试系统基本且常用的功能以及对响应时间要求严格的功能模块；
b) 可靠性测试需求：运行稳定性、屏蔽用户操作错误、错误提示的准确性以及故障异常恢复能力；
c) 易用性测试需求：操作界面符合标准和规范，系统整体功能的直观性、一致性、正确性及可理解性。

11.3 测试方法

使用黑盒测试方法，Bug跟踪管理工具，定位问题抓包工具，覆盖所有功能需求对其进行等价类划分、边界值分析、错误推测等各类测试策略测试，确保功能的实现满足系统需求要求。

11.4 性能测试

使用参数化方法实现多用户的并发登录，使用虚拟用户并发来模拟实际用户对业务系统施加压力，查看各操作场景响应时间。

11.5 安装调试

现场安装调试软件、拟定培训材料，进行相应的先期培训，及时记录交付、安装过程中系统出现的问题。

11.6 运行维护

11.6.1 基本要求

11.6.1.1 系统应具有运行维护能力，主要包括运行维护能力、运维准备、运维执行、运维验收、运维改进和运维过程管理。

11.6.1.2 运行维护的过程管理应至少包含服务级别管理、报告管理、事件管理、问题管理、配置管理、变更管理、信息安全管理等内容。

11.6.2 日常维护

为保证系统安全和稳定运行，应做好日常的监控、检查和维护工作，每月进行项目文档的归档、每天监控项目运行日志，并分析可能发生的异常情况。

11.6.3 程序代码可维护

代码编写格式系统统一规范，重要代码需注释，提高程序的可读性，便于维护。采用代码版本控制软件对代码版本进行控制。

11.6.4 运行故障应急处理

对于系统运行故障，需要做好应急处理预案，确保小故障1 h内恢复，一般故障6 h内恢复，灾难性故障1 d内恢复，并详细排查故障原因，做好总结完善工作。