ICS 35.240
CCS L 70

DB37

山东省地方标准

DB 37/T 4431—2021

基于区块链的企业开办可信服务平台技术规范

Technical specification for enterprise establishment trusted service platform based on blockchain

2021 - 11 - 17 发布　　2021 - 12 - 17 实施

山东省市场监督管理局　　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。

本文件由山东省工业和信息化厅提出并组织实施。

本文件由山东省信息标准化技术委员会归口。

本文件起草单位：济南高新技术产业开发区管理委员会、山大地纬软件股份有限公司、山东大学、山东省区块链金融重点实验室、中国网络安全审查技术与认证中心。

本文件主要起草人：陈波、孔兰菊、姜巧巧、杜金峰、赵强、孙德林、周永喜、崔立真、钱进、李庆忠、肖宗水、闵新平、张玉波、韩慧健、杨峰、王媛。

引　言

目前在政务服务领域中，企业开办过程存在数据跨部门传递不可信、业务难协同等现象。区块链技术具有不可篡改、公开透明、追根溯源、集体维护等优势，利用区块链技术，打造基于区块链的企业开办可信服务平台，创新区块链数据共享模式，实现企业开办数据跨部门可信传递、各部门业务在线协同办理和管控，对于推动“企业开办一次办好”等改革落地实施具有重要的应用价值和作用，对于区块链政务服务创新应用具有重要促进作用。

区块链有公有链、联盟链、私有链三种应用模式，其中联盟链是由特定的群体成立联盟组织、共同参与管理的区块链，具有高性能、多中心、安全可靠等特性。目前联盟链模式是企业开办应用的主要方向，各联盟组织在区块链技术构成的交易网络节点中进行交易，构建了可信的企业开办协同体系，实现数据跨部门可信传递，通过智能合约自动执行，优化企业开办业务办理流程。

本文件基于区块链在企业开办应用场景的成功应用实践，提出一套基于区块链的企业开办可信服务平台技术实现路径和应用模式，可为政务服务领域其他应用场景（如工程建设项目审批、出生一件事等）的区块链创新应用提供参考。

基于区块链的企业开办可信服务平台技术规范

1 范围

本文件规定了基于区块链的企业开办可信服务平台的总体框架、技术要求和安全要求等。

本文件适用于区块链在企业开办业务场景的应用，其他政务服务业务场景参考使用。

注：本文件中的区块链指联盟链。

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 31167—2014 信息安全技术 云计算服务安全指南

GB/T 34080.1—2017 基于云计算的电子政务公共平台安全规范 第1部分：总体要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

DB37/T 3481—2018 政务服务“一次办好”工作规范 第1部分：总则

3 术语和定义

DB37/T 3481—2018界定的以及下列术语和定义适用于本文件。

3.1

政务联盟链 government consortium blockchain

基于联盟链技术，由政务部门和相关机构共同搭建的区块链。

3.2

智能合约 smart contract

以数字形式定义的能够自行执行条款的程序。

注：在区块链技术领域，智能合约是基于预定事件触发、不可篡改、自动执行的计算机程序。

3.3

可信主体 trusted subject

自然人或机构等主体经过认证后，在区块链上开通账户成为可信主体。

3.4

数字资产 digital asset

数据发行到区块链上，进行确权及加解密、签名形成的有价值的数据，包括结构化数据和非结构化数据等。

3.5

可信传递 trusted delivery

数字资产在区块链上的授权传递方式，确保被授权用户得到权限内真实有效的数据信息。

3.6

联盟成员 alliance member

共同建设政务联盟链的机构和部门，提供基础设施、政务服务及业务规则等。

3.7

联盟节点 alliance node

组成政务联盟区块链的节点，提供记账、交易接入、存储等服务，可部署在政务云、公有云、私有云等设施。

3.8

共识节点 consensus node

负责账本数据一致性的节点。

3.9

交易节点 transaction node

负责交易服务接入、交易构建的节点。

3.10

存储节点 storage node

负责数字资产存储的节点。

3.11

链端节点 chain-end node

一个区块链接入端，内置可信环境，提供交易发起与查询、交易签名、加解密等服务。

3.12

数字保险箱 digital locker

基于区块链技术，为可信主体提供电子资料存储、授权、交易等服务的应用。

3.13

上链 release on the chain

将电子资料上传到可信主体的数字保险箱。

3.14

企业开办 enterprise establishment

企业设立登记以及印章刻制、社保登记、医保登记、住房公积金开户登记、银行开户、涉税办理等后续业务的办理过程。

4 缩略语

下列缩略语适用于本文件。

CA：证书颁发机构（Certificate Authority）

ISV：独立软件供应商（Independent Software Vendor）

5 应用需求

基于区块链的企业开办可信服务平台的应用需求包括：

a) 优化业务流程：需优化企业开办的业务办理流程，实现业务自动流转，缩减企业开办时间；

b) 网络互联互通：需实现电子政务外网与企业开办相关业务专网的安全连接，实现互联互通；

c) 数据可信传递：需实现企业开办业务数字资产的可信传递、共享使用；

d) 业务协同机制：需实现在多部门间构建可信的业务协同办理机制，实现企业开办业务办理的协同化、全程化和智能化；

e) 数字资产不可篡改：需实现企业开办数字资产的不可篡改、不可伪造，保证数字资产的真实可信。

6 平台框架

区块链企业开办可信服务平台(以下简称“平台”)由区块链基础设施层、数据资源层、区块链可信支撑层、业务支撑层、业务应用层组成，平台总体框架见图1。

图1 平台框架

7 平台技术要求

7.1 基本要求

平台符合以下基本要求：

a) 平台应与部门业务办理系统对接，实现数字资产在跨部门、跨领域、跨系统间的可信传递；
b) 应能实现企业开办业务办理过程产生或所需电子资料的实时签发上链；
c) 对于所需的已上链数字资产，应能实现自动从链上获取、共享共用；
d) 业务申请人应对提交资料的真实性负责，实体资料或电子资料提供方应对上链数字资产的真实性负责；
e) 应对数据存储、传输采取安全保障措施，保障数字资产的安全性、隐私性；
f) 数字资产中的数字证照应符合电子证照国家标准规范的要求。

7.2 区块链基础设施层

区块链基础设施层提供网络、计算、存储等基础支撑，符合以下要求：

a) 共识节点：基于共识算法构建区块，对数字资产、可信主体、智能合约等的状态进行记账，维护账本的一致性、不可篡改性等；
b) 交易节点：交易节点负责验证链端节点发起的交易，并将合法的交易广播给共识节点。交易节点接收共识节点构建的区块，并根据区块内容执行交易，更新数字资产、可信主体、智能合约的状态，为链端节点提供数据查询、节点路由等；
c) 存储节点：存储节点存储数字资产内容，包括但不限于结构化数据和非结构化数据，确保数字资产高可用、不可篡改。

7.3 数据资源层

数据资源层提供业务或交易数据的存储、管理等，符合以下要求：

a) 受理信息：应存储受理的企业开办业务申请信息；
b) 审批信息：应存储企业开办业务各环节的审批信息，包括审批部门、审批人员、审批时间、审批结果等，审批信息应实现上链存储；
c) 过程信息：应存储企业开办业务过程中申请材料、出件材料的流转信息；
d) 监管信息：应存储对企业开办业务办理进行监管的相关信息；
e) 可信主体信息：应存储企业或自然人的主体识别信息，包括企业基本信息、企业法定代表人信息、自然人基本信息等，可信主体信息应实现上链存储；
f) 数字资产内容：应存储企业开办业务办理过程涉及的数字资产内容，数字资产内容应实现上链存储；
g) 交易账本：应存储数字资产的发行记录、授权记录、使用记录、状态等信息，交易账本应实现上链存储。

7.4 区块链可信支撑层

7.4.1 概述

区块链可信支撑层包括区块链核心支撑、区块链开放服务和区块链应用接口。

7.4.2 区块链核心支撑

区块链核心支撑符合以下要求：

a) 成员管理：实现联盟成员的准入申请、准入审核、操作权限管理等。其中操作权限包括智能合约管理权限、节点管理权限、主体管理权限；
b) 主体管理：实现企业、自然人等可信主体管理，包括数字保险箱开户申请、许可准入、操作权限管理等；其中操作权限包括交易权限、智能合约发布权限、数字资产发行权限；
c) 节点管理：实现区块链节点的准入、准出等，包括共识节点、交易节点、存储节点、链端节点等；
d) 交易管理：实现交易构建、交易提交、交易确认、交易查询等；
e) 资产管理：实现数字资产的定义、创建、查看，以及数字资产委托、授权、转移等；
f) 安全管理：实现数字资产加密、授权使用及密钥安全托管等；
g) 运维管理：实现配置管理、版本管理、监控服务管理等。

7.4.3 区块链开放服务

区块链开放服务符合以下要求：

a) 交易服务：基于区块链核心支撑层的交易管理功能，为区块链用户提供交易发送、交易确认、交易执行验证等；
b) 密钥服务：
   1) 密钥生成：实现对称及非对称的账户密钥生成、密钥更换、密钥多方备份/找回等；
   2) 签名/验签：实现私钥签名、公钥验签；
   3) 托管服务：构建多中心的密钥安全托管区，进行密钥冷热备份，保证托管密钥安全高可用，同时提供 CA 证书、口令等多种手段保证密钥数据的访问、使用安全。
c) 加解密：实现数字资产及交易的加解密；
d) 摘要服务：实现数字资产、交易及区块的摘要计算；
e) 智能合约服务：实现智能合约的编写、审核、部署、测试、更新升级等；
f) 监控服务：
   1) 节点监控：展示当前所有节点的运行状态，提供节点信息查询服务；
   2) 交易监控：展示一定时期内平台的交易数量及变化情况；
   3) 账户监控：实现联盟成员账户、数字资产账户、智能合约账户的监控，实时监测账户数量变化情况、一定时期内账户数量的变化趋势、账户类型、创建时间等；
   4) 数字资产监控：实现各类数字资产的总量、增量、交易情况等的实时监控；
   5) 信息预警：通过分析监控数据，实时掌握政务联盟链节点异动、风险，并即时做出预警。
g) 监管服务：实现监管接口接入，监管方可查看所有具有监管权限的数字资产的内容、交易。

7.4.4 区块链应用接口

区块链应用接口符合以下要求：

a) 数字资产发行：有资产发行权限的可信主体，可将电子资料上链存储；
b) 数字资产授权：
   1) 被授权可信主体通过授权可信主体的授权，对授权可信主体的数字资产进行查看或使用；
   2) 授权可信主体将数字资产推送至被授权可信主体的数字保险箱。
c) 数字资产委托：
   1) 被委托可信主体通过委托可信主体的授权，对委托可信主体的数字资产进行查看或使用；

2) 委托可信主体将数字资产推送至被委托可信主体的数字保险箱。

d) 数字资产查询：

1) 获取数字资产最新状态：根据数字资产账户唯一标识获取数字资产的最新状态，包括可用、撤销、废除等；

2) 获取数字资产最新交易唯一标识：根据数字资产账户唯一标识获取数字资产相关的最新一笔交易的交易唯一标识；

3) 获取数字资产授权码：根据数字资产账户唯一标识获取数字资产授权码；

4) 获取数字资产内容：根据数字资产账户唯一标识和数字资产授权码，获取可信主体数字资产的内容；

5) 获取数字资产加密方式：根据数字资产账户唯一标识获取数字资产的加密方式，包括对称算法加密方式、非对称算法加密方式等；

6) 获取数字资产对称密钥：根据数字资产账户唯一标识和主体提供的账户解锁密码获取数字资产加密的对称密钥。

e) 消息管理：实现点对点通信能力，包括在线消息的发送与接收、离线消息的存储等。通信对象包括自然人、企业、机构等可信主体，应覆盖移动端、电脑端等访问渠道。

7.5 业务支撑层

业务支撑层符合以下要求：

a) 网络通：平台应以电子政务外网为基础，采用多种网络连接方式与部门业务办理系统安全连接，实现网络连通；

b) 数据通：平台应通过程序接口或前端智能交互的方式，实现业务数据的共享利用；

c) 流程定义：根据企业开办实际流程，事先将企业开办涉及的环节进行串并联设计，并固化到系统中；

d) 流程执行：企业开办业务受理后，按照事先设计的流程自动执行，实现业务办理的协同化和智能化。

7.6 业务应用层

7.6.1 综合受理

应实现企业开办业务申请的统一收件、受理，以及受理后向部门业务办理系统的自动分发。

7.6.2 数字保险箱

数字保险箱符合以下要求：

a) 数字资产展示：实现按照数字资产类型展示数字资产；

b) 数字资产查看：实现数字资产内容的查看，包括数字资产照片、数字资产信息描述、数字资产使用记录等，应支持数字资产查看与查看事由、时间关联，宜采用时间戳验证；

c) 实现电子资料上链，应支持以下上链方式：

1) 权威机构签发：对有实体资料签发权限的政府部门或权威机构，将实体资料对应的电子资料签发到可信主体的数字保险箱；

2) 出件窗口签发：经个人、企业授权后，由统一出件窗口将个人、企业的有效证照、证明材料等数字化后，签发到可信主体的区块链数字保险箱；

3) 业务办理部门签发：个人、企业在办理业务时提交的纸质证照，经个人、企业授权后，由业务办理部门将个人、企业的纸质证照验证、数字化后签发到可信主体的数字保险箱；

4) 个人、企业签发：个人、企业将纸质证照数字化后，连同其他结构化数据一起上传，经由政府部门或专门职能机构对上传证照等数据的真实性、有效性审核通过后签发到可信主体的数字保险箱；

d) 支持数字资产的授权使用；

e) 交易上链：对数字资产的签发、授权等进行记账，形成交易账本；

f) 消息提醒：如果数字资产授权没有及时处理，系统自动向用户推送提醒消息。

7.6.3 事项流程管理

事项流程管理符合以下要求：

a) 事项清单管理；应基于事项清单要素，实现事项标准化办理等。事项清单要素参见 DB37/T 3448.4—2019；

b) 管控流程管理：应实现业务办理部门审批流程环节的标准化管理，包括审批环节以及审批环节的输入信息、输出信息、共享信息、积累信息以及向服务对象推送的信息；

c) 信息设置管理：应实现部门业务办理系统的输入、输出信息的设置管理。

7.6.4 职责权限管理

应实现各相关方的职责权限管理，包括部门、岗位、人员、角色等。

7.6.5 智能合约管理

应实现智能合约按照业务定义，以及智能合约查询、修改、废止等管理。

7.6.6 业务流程监管

应实现企业开办业务流程监管，包括业务办理环节、业务办理时限、是否人工干预。

7.6.7 统一出件

应实现业务审批结果的数字化，并签发到可信主体的数字保险箱，包括电子营业执照、社保告知单、医保告知单等。

7.7 部门业务办理系统

部门业务办理系统实现企业开办办理过程中具体部门业务环节的审批、办理。应将部门业务办理系统的网络、数据打通后与平台对接，包括营业执照申领业务系统、印章刻制业务系统、社保登记业务系统、医保登记业务系统、住房公积金开户登记业务系统、银行开户在线预约业务系统、涉税办理业务系统等。

8 平台安全要求

8.1 基本要求

平台安全符合以下基本要求：

a) 平台安全应符合 GB/T 22239—2019；

b) 平台应与部署于信创云之上的业务系统相兼容，应具备身份识别、访问控制、安全审计等能力；

c) 平台应支持国密算法，使用的密码算法应符合国家标准、行业标准的相关要求；

d) 平台密码应用应符合 GB/T 39786—2021 的要求。

8.2 数据安全要求

平台数据安全符合以下要求：

a) 平台与部门业务办理系统、平台与其他政务信息系统的数据交换安全应符合 GB/T 39477—2020 的安全技术要求；
b) 平台应具备持久化存储账本记录的能力，保证数据的可追溯性；
c) 平台应具备向获得授权者提供真实数据的能力；
d) 平台应对用户、应用的数据行为和重要安全事件进行审计。

8.3 个人信息保护

应采取措施保障平台个人信息，平台个人信息应符合GB/T 35273—2020中的个人信息安全相关规定。

8.4 云平台安全要求

当部署于云平台时，云平台安全应符合GB/T 34080.1—2017的要求，基于区块链的企业开办可信服务平台运营部门应符合GB/T 31167—2014的安全要求。

区块链可信服务平台运营服务见附录A。

附 录 A
（资料性）
区块链可信服务平台运营服务

A.1 政务联盟链的创建

政务联盟链的创建流程：

a) 针对企业开办业务场景，梳理涉及部门，并对其业务办理量进行评估；
b) 根据评估结果并结合平台运维机构推荐的区块链最低要求配置，确定硬件资源需求。硬件资源需求主要包括共识节点、交易节点、存储节点，各节点间应保证网络的互联互通且稳定，并应保障交易节点对外的带宽；
c) 配置硬件资源；
d) 进行区块链底层软件的部署及调试，完成政务联盟链的创建。

A.2 联盟节点加入政务联盟链

联盟节点加入政务联盟链的流程：

a) 企业开办流程中新加入流程事项，该事项所涉及的业务部门应向联盟链建设方申请准入；
b) 联盟链建设方审核成员信息，对联盟成员进行相关信息的分配，完成准入；
c) 针对应用场景、业务并发量、联盟成员情况等，进行摸底调研；
d) 根据调研结果并结合平台运维机构推荐的区块链最低要求配置，确定硬件资源需求。硬件资源需求主要包括共识节点、交易节点、存储节点，各节点间应保证网互联互通且稳定，应保障交易节点对外的带宽；
e) 配置硬件资源；
f) 进行区块链底层软件的部署及调试。

A.3 政务联盟链的使用

政务联盟链的使用流程：

a) 联盟链建设方输出标准的接口规范文档；
b) 联盟链建设方根据系统部署情况输出测试和正式环境访问地址信息；
c) 部门业务办理系统 ISV 向联盟链建设方申请接入账户权限等信息；
d) 联盟链建设方进行部门业务办理系统 ISV 接入的审核，并协调联盟链建设方进行相应的账户权限信息分配；
e) 部门业务办理系统 ISV 按照业务需求和政务联盟链的接口交互规范，开发相应的对接系统，完成系统对接。

A.4 智能合约开发部署

智能合约开发部署流程：

a) 对要上链的实体资料或电子资料进行调研，调研内容包括但不限于资料应用场景、各种操作带来的资料状态变化、资料各相关数据字段的含义、资料生命周期、更新频率等；
b) 根据调研情况，编制智能合约规范文档；
c) 按照智能合约规范文档，创建智能合约；
d) 在测试环境进行智能合约操作的测试。测试无误后，升级为正式环境；
e) 对正式环境的智能合约再次进行测试，测试通过发布智能合约；
f) 数字资产使用过程中，持续收集数字资产的相关智能合约信息，及时更新智能合约。

A.5 数字保险箱开户

数字保险箱开户流程：

a) 业务申请人提交数字保险箱开户材料，包括法定代表人身份证、综合受理人身份证、企业基本信息等；

b) 经核准通过后完成数字保险箱的开户。

参 考 文 献

[1] GB/T 32905—2016 信息安全技术 SM3密码杂凑算法
[2] GB/T 32907—2016 信息安全技术 SM4分组密码算法
[3] GB/T 32918—2016 信息安全技术 SM2椭圆曲线公钥密码算法
[4] JR/T 0184—2020 金融分布式账本技术安全规范
[5] JR/T 0193—2020 区块链技术金融应用评估规则
[6] DB37/T 3448.4—2019 政务服务平台 第4部分：基础数据规范
[7] 山东省人民政府《关于持续深入优化营商环境的实施意见》（鲁政字〔2020〕67号）