ICS 03.060
CCS A 11

Q/CCDC

中央国债登记结算有限责任公司企业标准

Q/CCDC 00009—2023

中债区块链数字债券发行平台规范

Specification for blockchain digital bond issuance platform of CCDC

2023-07-13 发布　　2023-07-13 实施

中央国债登记结算有限责任公司　　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。

本文件由中央国债登记结算有限责任公司提出并归口。

本文件起草单位：中央国债登记结算有限责任公司。

本文件为首次制定。

引　言

中央国债登记结算有限责任公司（以下简称“中央结算公司”）作为重要国家金融基础设施，致力于为市场提供安全、高效、专业的债券全生命周期服务。为贯彻落实新发展理念和数字化战略，向市场提供区块链数字债券发行公用平台，中央结算公司探索研发区块链数字债券发行方案，并于2022年初入围国家区块链创新应用试点。在管理部门的指导和市场机构的支持下，中央结算公司的区块链数字债券发行平台已于2022年上线应用。

区块链数字债券生态培育和高质量发展，离不开标准体系的建设。中央结算公司在探索实践中积累总结经验，提炼形成本文件。在发行业务基础上，中央结算公司还将探索区块链支持债券生命周期业务。随着区块链数字债券的探索深化和应用拓展，中央结算公司将完善本文件，并适时制定区块链数字债券系列标准。

中债区块链数字债券发行平台规范

1 范围

本文件规定了区块链数字债券发行平台的基本要求、平台架构、功能要求、数据要求、性能要求、安全要求和运维要求等内容。

本文件适用于中央结算公司通过区块链技术构建的数字债券发行平台。

2 规范性引用文件

下列文件中的内容通过文本中的规范性引用而构成本文件必不可少的条款。其中，注册日期的引用文件，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（包括所有的修订单）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

JR/T 0184—2020 金融分布式账本技术安全规范

JR/T 0193—2020 区块链技术金融应用 评估规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块链 blockchain

一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

[来源：JR/T 0193—2020，3.1]

3.2

智能合约 smart contract

一种旨在以信息化方式传播，验证或执行合同的计算机协议，其在分布式账本上体现为可自动执行的计算机程序。

[来源：JR/T 0184—2020，3.20]

3.3

共识节点 consensus node

负责账本数据一致性的节点。

[来源：JR/T 0184—2020，3.24]

3.4

记账节点　accounting node

负责账本数据完整性的节点。

[来源：JR/T 0184—2020，3.25]

3.5

联盟链　consortium blockchain

通过权限控制，对特定的组织团体开放的区块链，由联盟内部指定多个预选节点为共识节点，每个块的生成由所有共识节点共识决定，其他接入节点在权限许可的情况下可参与记账，可通过该区块链开放的接口进行交易调用及限定查询。

3.6

簿记管理人　book runner

负责实际簿记建档发行的操作者，一般由主承销商担任。

[来源：Q/CCDC 00004.1—2020，3.4]

3.7

参与者　participant

接入区块链数字债券发行平台的各类机构，包括债券市场的相关监管部门、金融机构和非金融企业。其中，金融机构和非金融企业统称为市场机构。

3.8

用户　user

参与者以发行人、承销团成员、投资人等角色开立的业务账户。

3.9

数字债券　digital bond

数字形态的债券，是以债券要素指标的标准化为基础，以数字技术为实现手段，以账户或通证为存储形式的债券。

3.10

区块链数字债券　blockchain digital bond

数字债券的一种，是应用区块链技术，具有通证形式，可支持账户松耦合的数字债券。

3.11

区块链数字债券发行平台　blockchain digital bond issuance platform

基于区块链底层技术和运维管理服务构建的数字债券发行应用系统，供监管部门、发行人、承销团成员、投资人和中央结算公司相关业务人员使用。

3.12

区块链即服务　blockchain as a service

区块链框架嵌入云计算平台，利用云服务基础设施的部署和管理优势，为开发者提供便捷、高性能的区块链生态环境和生态配套服务，支持开发者的业务拓展及运营支持的区块链开放平台。

4 缩略语

下列缩略语适用于本文件。

BaaS：区块链即服务（Blockchain As A Service）。

5 基本要求

5.1 与业务规则相协调

区块链数字债券发行平台建设以现有业务规则为基础，和现有业务规则相协调。当业务规则发生变化时，区块链数字债券发行平台应及时升级。

5.2 共建共治

中央结算公司和市场机构共建共治联盟链，共同促进区块链数字债券发行平台安全稳健运行。

共建过程中，市场机构在中央结算公司的主导组织下，积极参与区块链数字债券发行平台的方案设计、系统建设、上线应用、运行维护等全过程。

共治过程中，中央结算公司负责制定业务运行规则，编写升级智能合约，建立完善联盟治理机制。市场机构在遵守联盟制度的基础上，有序开展业务创新，提供有益反馈和合作监督。

5.3 中心化管理

中央结算公司履行法定中央托管机构职责，对区块链数字债券发行平台实施中心化管理，在关键业务环节实施裁决机制，同时接受市场机构的监督，合理采纳并及时回复市场机构的意见建议。

5.4 参与者接入方式

参与者接入区块链数字债券平台的方式，包括全节点接入、轻节点接入和无节点接入。中央结算公司通过技术文件明确各类接入方式的技术要求。

——全节点接入：既部署记账节点，又部署共识节点的接入方式。

——轻节点接入：仅部署记账节点的接入方式。

——无节点接入：不部署共识或记账节点，通过客户端形式接入。

5.5 上链机构

5.5.1 监管节点

监管部门根据业务需要，选择全节点、轻节点或者无节点方式上链。

5.5.2 上链市场机构的基本要求

上链市场机构应是银行间债券市场的参与者，上链市场机构应覆盖所有参与者类型。上链市场机构可根据自身情况向中央结算公司申请以全节点、轻节点或者无节点方式上链。

5.5.3 轻节点市场机构的选择

中央结算公司合理甄别和选择以轻节点方式上链的市场机构。以轻节点上链的市场机构应具备一定的区块链技术基础。

5.5.4 全节点市场机构的选择

中央结算公司应从业务规模、技术能力、企业属性等多方面严格甄选外部全节点机构。以全节点上链的市场机构应是债券市场的主要参与者，具有较强的区块链技术能力，具备维护节点数据安全的意愿和实力。

5.6 系统审计

5.6.1 审计依据

区块链数字债券发行平台应按照 JR/T 0193—2020，通过第三方审计机构的审计。

5.6.2 审计范围

审计范围包含区块链底层平台、运维管理平台和上层应用平台的技术标准遵循情况。

5.6.3 审计机构

审计机构应是注册成立 3 年以上、具备专门的信息科技审计团队、有固定的工作场所、商业信誉良好的专业组织。

5.7 系统评估要求

5.7.1 评估依据

区块链数字债券发行平台应根据中央结算公司相关要求，在上线前开展安全评估；按照 JR/T 0193—2020，在上线后开展专项评估。

5.7.2 评估内容

评估以系统为单位，上线前的安全评估主要包括渗透测试、代码审计评估、漏洞扫描等；上线后的专项评估主要包括区块链基础技术测评和区块链安全性测评。

5.7.3 评估机构

评估机构应具备金融机构同类项目信息安全评估经验，评估案例达 3 个以上，具有网络安全等级测评与监测评估机构服务认证证书，过去 3 年无重大违法违规行为。

5.8 备案要求

区块链数字债券发行平台应按《区块链信息服务管理规定》（国家互联网信息办公室令第 3 号）的相关要求进行首次、变更和终止备案。

6 平台架构

6.1 总体架构

区块链数字债券发行平台采用联盟链，主要架构包括：基础设施、区块链网络、区块链 BaaS 平台、业务应用系统等四大核心层级，见图 1。

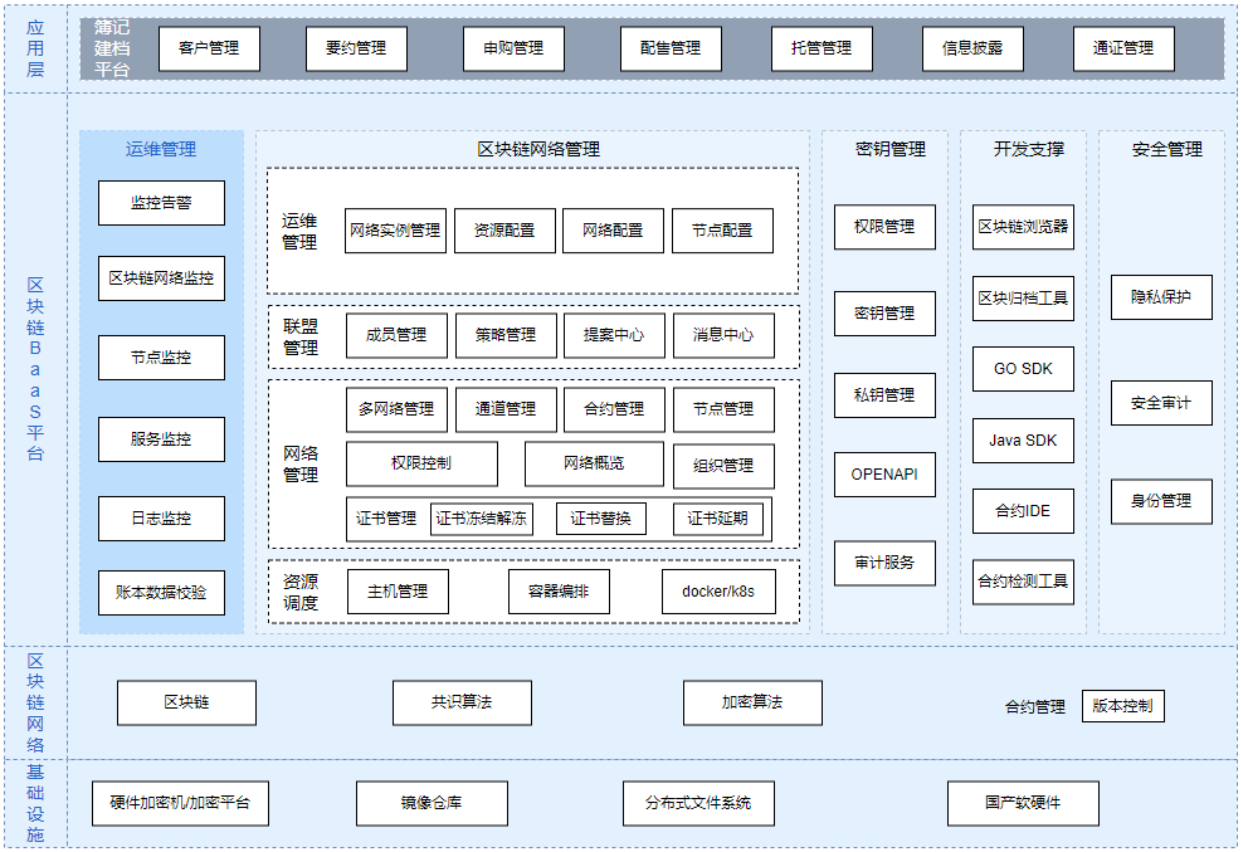

图1 区块链数字债券发行平台总体架构

6.2 基础设施

基础设施层提供平台正常运行所需的运行环境和基础组件，如硬件加密机、分布式文件系统、镜像仓库和国产软硬件等。

6.3 区块链网络

区块链网络由各参与方组成的分布式节点系统构成，具备合约管理模块、加密算法模块、共识算法模块等基础能力，在共识前提下执行交易数据读写，并对数据进行加密，实现交易数据的安全和分布式存储，为区块链应用提供运行环境。

6.4 区块链 BaaS 平台

区块链 BaaS 平台层负责提供运维管理、网络管理、密钥管理、开发支撑和安全管理功能。

6.5 业务应用系统

业务应用系统为用户提供发行服务和应用。

7 功能要求

7.1 核心功能

区块链数字债券发行平台应具备发行前信息披露文件存证、债券注册、制作申购要约、债券申购、配售、公布配售结果和生成通证等七大核心功能，见图 2。

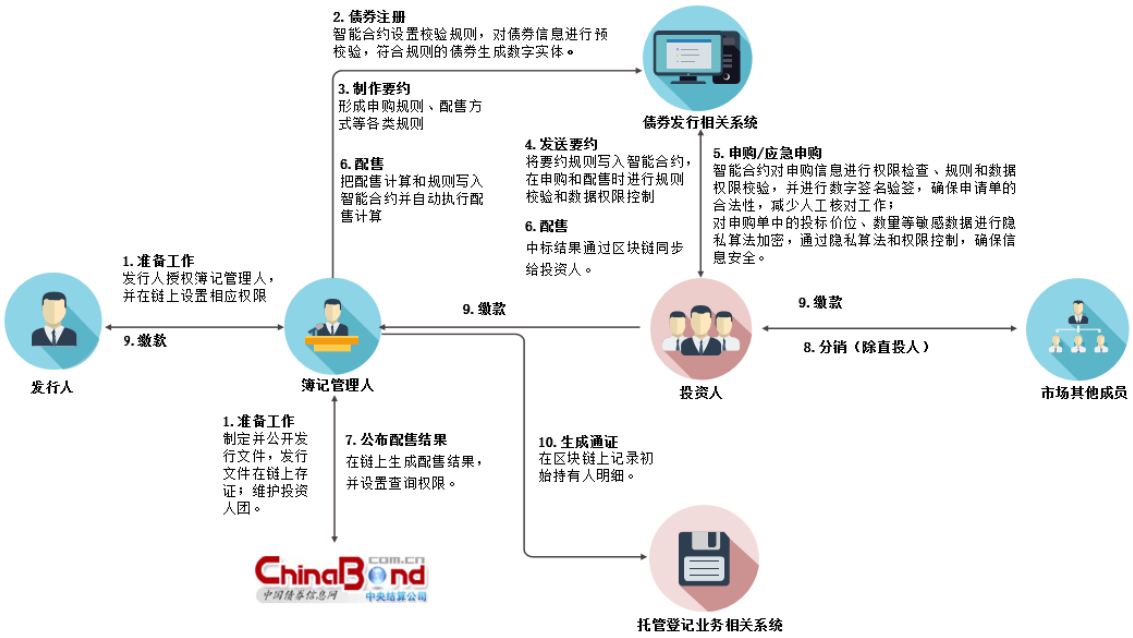

图 2 区块链数字债券发行业务流程图

7.2 发行前信息披露存证

支持信息披露文件上链存证，并支持存证查询。

7.3 债券注册

用智能合约实现债券注册模块的主要功能，在债券注册环节对数据要素等规则进行预检查和校验，符合规则的债券，上链存储，不符合规则的信息，则无法上链。

7.4 制作申购要约

在智能合约里实现要约申购、配售方式等各类规则，投资人和簿记管理人等角色在进行申购和配售时，系统根据不同角色自动校验申购数据字段规则和数据读写权限，校验通过后才可操作。

7.5 债券申购

用区块链进行规则校验、数据权限校验、申购数据的数字签名验证，确保申购数据真实、可追溯。用隐私保护算法对申购方账号、联系人、联系方式、申购价位、申购数量等申购明细信息进行加密存储。

7.6 配售

根据投资人的申购情况，调用利率簿记建档、价格簿记建档配售算法进行计算。计算完成后，对配售结果数据进行加密后上链，严格设置市场机构的操作权限和配售数据查阅权限，实现不同角色的差异化隐私保护机制。

7.7 公布配售结果

支持生成整场配售结果并导出。

7.8 生成通证

支持发行结果信息上链登记。

8 数据要求

8.1 数据格式

数据格式应符合中央结算公司的相关要求。

8.2 数据存储

发行业务数据存储采用分布式区块链技术存储。

8.3 数据权限

参与者按照各类券种业务指引、规则的要求提供并访问业务数据。

8.4 数据接口

支持通过数据接口和其他系统之间实现互操作。

中央结算公司应明确数据接口标准，通过白名单限定确保数据交互对象的真实可信，通过适当技术手段确保数据安全和不可篡改。

9 性能要求

9.1 系统容量

应支持至少 100 个参与者同时接入。

9.2 交易吞吐量

应支持至少 800TPS。

9.3 并发用户量

应支持在 200 个并发用户量下平稳运行。

9.4 响应时间

响应时间应满足如下要求：

——在网络畅通情况下，应保证业务系统与区块链系统交互的响应时间不超过 3 秒。

——在业务高峰时段网络拥堵情况下，应保证业务系统与区块链系统交互的响应时间不超过 10 秒。

9.5 节点存储规模

单节点存储规模应至少支持 100GB。

9.6 互操作性

应支持互操作，包括应用层互操作、链间互操作和链下互操作。

通过应用层互操作实现区块链数字债券发行平台业务应用和底层链的对接交互。

通过链间互操作实现区块链数字债券发行平台和其他区块链系统之间的数据互通、身份互认和治理协同。

通过链下互操作实现区块链数字债券发行平台和链下系统的安全可信交互。

10 安全要求

10.1 基础软件

应符合 GB/T22239—2019 中三级以上的主机安全、应用安全、数据安全及备份恢复相关规定。

应采用联盟链的结构，对接入节点或参与者进行一定限制的身份验证。

应采用白名单控制区块链网络节点与业务系统的相互访问。

应具备平台操作和运营日志管理功能，支持对平台历史使用情况进行追踪和审计。

10.2 节点管理

应具备节点准入控制机制，节点通过授权后才能加入或退出网络。

应采用 SSL/TLS 保障节点间通信安全。

应支持兼容环境部署，可部署于主流的 Linux 操作系统的服务器。

10.3 账本数据

10.3.1 完整性

应保证账本数据在生成、传输、存储和调用过程中的完整性，不被非法篡改。

10.3.2 一致性

应保证各节点的账本数据写入、修改、存储和调用的一致性。

参与者和中央结算公司坚持共建共治原则，共同维护账本数据的一致性。若存在不一致，中央结算公司履行系统维护管理职责，对不一致情况进行核查。

10.3.3 保密性

应通过权限控制、密码学技术保证敏感数据无法被非授权方读取。

10.3.4 授权使用

应确保数据的访问使用符合认证授权和访问控制要求，仅授权方可访问账本数据。

10.4 智能合约

智能合约应遵照 JR/T 0184—2020 中针对智能合约的相关要求。

中央结算公司根据相关业务规则编写智能合约，按参与者类型制定相应的智能合约调用权限，阻止智能合约的非法访问。

10.5 共识机制

共识协议应遵照 JR/T 0184—2020 中针对共识协议的相关要求。

参与者和中央结算公司通过智能合约高效实现业务流程中的共识形成。

10.6 裁决机制

区块链数字债券发行平台在节点增加删减、智能合约升级等关键业务环节，实施裁决机制。

实施裁决机制时，若各节点意见一致，则系统自动执行；若各节点意见不一致，中央结算公司基于职责合理判断进行裁决，并将裁决意见在链上向全节点和裁决事宜相关节点公开。

10.7 密码算法

密码算法应遵照 JR/T 0184—2020 中针对密码算法的相关要求。

业务数据通过基于国密算法构造的混合加密算法进行隐私保护和安全共享。

10.8 身份管理

10.8.1 身份鉴权

应在参与者接入网络前，颁发参与者身份凭证。

10.8.2 访问控制

参与者应在授权的前提下，凭身份凭证访问区块链网络，非授权机构不能访问区块链网络。

应采用最小权限原则，最小化参与者权限，只允许参与者在权限范围内操作和访问数据。

应支持监管机构接入，对业务有效性和发行流程合规性进行监督和审核。

10.9 隐私保护

应通过隐私保护组件为业务数据提供加解密和细颗粒度访问权限控制功能。

10.10 运维安全

运维安全应遵照 JR/T 0184—2020 中针对运维安全的相关要求。

10.11 治理机制

在中心化管理的基础上，中央结算公司和参与者共建共治。

11 可维护性要求

11.1 智能合约的可维护性

智能合约升级，应保持历史数据的可迁移性、正确性、可用性。

在满足业务规则和相关制度的前提下，市场机构参与智能合约的升级管理，并及时检测升级智能合约。

11.2 节点可维护性

增加或删减节点时，其他节点不需要停止或重启。

在满足业务规则和相关制度的前提下，市场机构参与节点的增加、删减的管理。

11.3 参与者可维护性

增加或删减参与者时，整个区块链网络的节点不需要停止或重启。

参 考 文 献

[1] Q/CCDC 00004.1—2020 中债债券业务处理规范 第1部分：发行
[2] 《关于印发国家区块链创新应用试点名单的通知》（中网办秘字〔2022〕72号文印发）.2022-1-18
[3] 中国人民银行数字货币研发工作组.中国数字人民币的研发进展白皮书[R].2021-7-16.
http://www.gov.cn/xinwen/2021-07/16/content_5625569.htm
[4] 《区块链信息服务管理规定》（国家互联网信息办公室令第3号文印发）.2019-1-10