

ICS 35.240.40

CCS A 11

团 体 标 准

T/NIFA 25—2023

金融分布式账本技术资金管理应用 技术要求

Fund management application of financial
distributed ledger technology—Technical
requirements

2023-11-10 发布

2023-11-10 实施

中国互联网金融协会 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语与定义	1
4 缩略语	5
5 总体要求	5
5.1 对等合作	5
5.2 安全透明	6
5.3 数据可追溯	6
5.4 开放共享	6
5.5 分层部署	6
6 资金管理技术参考架构	6
7 基础设施层	7
7.1 总体要求	7
7.2 机房要求	7
7.3 服务器要求	8
7.4 网络要求	9
7.5 基础软件要求	10
7.6 运维要求	11
8 金融分布式账本平台层	12
8.1 总体原则	12
8.2 参考架构	13
8.3 功能要求	14
8.4 性能和安全	20
9 资金管理服务层	20
9.1 总体原则	20
9.2 参考架构	21
9.3 功能要求	21
参考文献	24

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》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

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。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、中国工商银行股份有限公司、深圳前海微众银行股份有限公司、京东科技控股股份有限公司、博雅正链（北京）科技有限公司、华为技术有限公司、中国人民保险集团股份有限公司、北京银行股份有限公司、交通银行股份有限公司、上海浦东发展银行股份有限公司。

本文件主要起草人：单强、陆书春、朱勇、王新华、刘朝伟、夏琼、陈法山、姚新亮、郭晓磊、周婧、张薇、余纬中、马文杰、傅华崧、温沛霖、杨立峰、武国峰、邸明杰、刘燕青、高玉翔、王海龙、王飞、张小军、张亮亮、杨猛、李赫、刘朋辉、王光中、钱菲、高扬。

引 言

金融分布式账本技术是密码算法、共识机制、点对点通讯协议、分布式存储等多种核心技术体系高度融合形成的一种分布式基础架构与计算范式。资金管理是金融领域的重要应用场景，金融分布式账本技术可提升资金管理的安全性、可信性、公开性。金融分布式账本资金管理应用技术要求旨在提供基于金融分布式账本技术的资金管理所需的基础设施、平台、服务和应用的技术指标。

金融分布式账本技术资金管理应用技术要求

1 范围

本文件确立了基于金融分布式账本技术的资金管理系统的的原则，明确了系统的参考架构，规定了系统的功能要求。

本文件适用于金融分布式账本资金管理系统研发、部署、运营、检测等。

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 32905—2016 信息安全技术 SM3密码杂凑算法
GB/T 32907—2016 信息安全技术 SM4分组密码算法
GB/T 32918.2—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法
GB/T 32918.4—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法
GB/T 37092—2018 信息安全技术 密码模块安全要求
GB 50174—2017 数据中心设计规范
GM/T 0045—2016 金融数据密码机技术规范
GM/T 0054—2018 信息系统密码应用基本要求
GM/T 0104—2021 云服务器密码机技术规范
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
ISO/IEC 14888—2:2008 信息技术 安全技术 带附录的数字签名 第2部分：基于整数分解的机制
ISO/IEC 14888—3:2018 信息技术 安全技术 带附录的数字签名 第3部分：基于离散对数的机制
ISO/IEC 18033—2:2006 信息技术 安全技术 加密算法 第2部分：非对称密码
ISO/IEC 18033—3:2010 信息技术 安全技术 加密算法 第3部分：分组密码

3 术语与定义

下列术语和定义适用于本文件。

3.1

金融分布式账本 financial distributed ledger

分布式账本 distributed ledger

由一组金融分布式账本节点（3.2）共享，并使用共识机制（3.3）在分布式账本技术节点之间同步的分户账（3.4）。

[来源：ISO 22739:2020, 3.22, 有修改]

3.2

节点 node

金融分布式账本节点 financial distributed ledger node

参与网络并存储分户账记录（3.5）的完整或部分副本的设备或过程。

[来源：ISO 22739:2020, 3.27, 有修改]

3.3

共识协议 consensus protocol

共识机制 consensus mechanism

达成共识（3.6）的规则和程序。

[来源：ISO 22739:2020, 3.12, 有修改]

3.4

分户账 ledger

保存最终的、确定的和不可变更（3.7）的交易（3.8）记录（3.9）的信息存储。

[来源：ISO 22739:2020, 3.43, 有修改]

3.5

分户账记录 ledger record

包含交易记录（3.10）、交易记录的哈希值（3.11）或交易记录（3.10）在金融分布式账本（3.1）上引用的记录（3.9）。

[来源：ISO 22739:2020, 3.44, 有修改]

3.6

共识 consensus

金融分布式账本节点（3.2）之间的约定，一是一个交易（3.8）是已确认的（3.12），二是金融分布式账本（3.1）包含已确认的（3.12）交易（3.8）排列的一致集合。

[来源：ISO 22739:2020, 3.11, 有修改]

3.7

不可变更性 immutability

一旦添加到金融分布式账本（3.1）中，分户账记录（3.5）就不能修改或删除的属性。

[来源：ISO 22739:2020, 3.40, 有修改]

3.8

交易 transaction

工作过程的最小单元，它是产生符合治理规则的结果所需的一个或多个活动序列。

[来源：ISO 22739:2020, 3.77, 有修改]

3.9

记录 record

一个组织或个人在履行法律义务或在业务交易中（3.8）作为证据和资产（3.13）创建、接收和维护的信息。

[来源：ISO 22739:2020, 3.67, 有修改]

3.10

交易记录 transaction record

记载任何类型的交易（3.8）的记录（3.9）。

[来源：ISO 22739:2020, 3.79, 有修改]

3.11

哈希值 hash value

一个密码哈希函数（3.14）的输出位串。

[来源：ISO 22739:2020, 3.39, 有修改]

3.12

已确认的 validated

当实体（3.15）所需的完整性条件已被检查后的状态。

[来源：ISO 22739:2020, 3.81, 有修改]

3.13

资产 asset

任何对干系人有价值的东西。

[来源：ISO 22739:2020, 3.1, 有修改]

3.14

密码哈希函数 cryptographic hash function

函数将任意长度的二进制字符串映射到固定长度的二进制字符串，这样在给定的输出中寻找一个映射到输出的输入在计算上成本很高，在给定的输入中寻找第二个映射到相同输出的输入在计算上不可行，且在计算上寻找任何两个不同的输入映射到相同的输出也不可行。

[来源：ISO 22739:2020, 3.15, 有修改]

3.15

实体 entity

在信息和通信技术系统内部或外部的项，如人、组织、设备、子系统，或能被清晰地识别出来的由多个项构成的项组。

[来源：ISO 22739:2020, 3.34, 有修改]

3.16

智能合约 smart contract

存储在金融分布式账本系统（3.19）中的计算机程序，该程序的任何执行结果都被记录在金融分布式账本（3.1）上。

[来源：ISO 22739:2020, 3.72, 有修改]

3.17

金融分布式账本系统 financial distributed ledger system

实现金融分布式账本（3.1）的系统。

[来源：ISO 22739:2020, 3.30, 有修改]

3.18

金融分布式账本平台 financial distributed ledger platform

一组处理、存储和通信的实体（3.15），它们共同提供每个节点（3.2）上金融分布式账本系统（3.17）的能力。

[来源：ISO 22739:2020, 3.29, 有修改]

3.19

区块 block

由区块数据（3.20）和区块头（3.21）组成的结构化数据。

[来源：ISO 22739:2020, 3.2, 有修改]

3.20

区块数据 block data

包含零到多个交易记录（3.10）或交易记录引用的结构化数据。

[来源：ISO 22739:2020, 3.3, 有修改]

3.21

区块头 block header

包含到前一个区块（3.19）密码链接（3.22）的结构化数据，除非没有前一个区块。

[来源：ISO 22739:2020, 3.4, 有修改]

3.22

密码链接 cryptographic link

使用密码哈希函数（3.14）技术构造的指向数据的引用。

[来源：ISO 22739:2020, 3.16, 有修改]

3.23

预言机 oracle

通过金融分布式账本系统（3.17）以外的数据更新金融分布式账本（3.1）的服务。

[来源：ISO 22739:2020, 3.28, 有修改]

3.24

共识节点 consensus node

负责金融分布式账本数据一致性的节点。

[JR/T 0184—2020, 定义3.24, 有修改]

3.25

记账节点 accounting node

负责金融分布式账本数据完整性的节点。

[JR/T 0184—2020, 定义3.25, 有修改]

3.26

跨链 inter-blockchain

在多个分布式账本之间传递价值和信息的技术方案。

3.27

数据归档 data archiving

将金融分布式账本中不经常使用的历史数据迁移到一个单独的存储设备来进行长期保持的技术方案。

3.28

可编程支付 programmable payment

根据预先设定的条件和规则进行自动支付的技术方案。

3.29

隐私信息 private information

特定自然人的标识信息及其在特定系统中的活动信息。

[JR/T 0184—2020, 定义3.41]

3.30

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[JR/T 0184—2020, 定义3.42, 有修改]

3.31

局部聚集系数 local clustering coefficient

网络分析中的一个概念，用于衡量一个节点的邻居节点之间连接的紧密程度。

3.32

联盟 consortium

联盟链 consortium blockchain

由两个以上机构共同运营的金融分布式账本系统（3.17），其中每一个机构控制一个或多个节点（3.2）。

4 缩略语

下列缩略语适用于本文件。

CA: 认证机构 (Certificate Authority)

ID: 身份标识符 (Identification)

5 总体要求

5.1 对等合作

资金管理应用应由参与机构平等共同维护，不应由一个或部分机构控制资金管理的全流程，应通过金融分布式账本技术实现资金的协同管理。

资金管理应用的金融分布式账本应由多个对等节点组成，由上述参与方平等地共同建设、管理和运营，参与方对其所建设、管理和运营的节点享有全部权利。

5.2 安全透明

资金管理应用应通过金融分布式账本技术实现资金的安全、透明全流程管理。

金融分布式账本存储的数据，除确需保密的管理、运营相关数据外，所有业务数据应毫无保留地向任何参与节点公开，管理运营节点对此类数据的查询权限，应与其他任何参与节点一致。

5.3 数据可追溯

资金管理应用应将资金流转、审核流程等信息存储于金融分布式账本，支持信息可回溯。

金融分布式账本应如实存储资金管理应用的操作历史，确保系统投入运营后，任意用户在任意时间发生的资金管理操作均可查询。

5.4 开放共享

资金管理应用应支持第三方数据接入、系统对接，支持金融分布式账本上的信息共享和权限查询、调用等，应支持多银行机构基于金融分布式账本技术形成联盟链，通过金融分布式账本传递交易信息和反馈结果等。

5.5 分层部署

资金管理应用可根据资金管理的不同层级，支持分层部署，如基础设施层、金融分布式账本平台层、资金管理服务层、业务应用层。

6 资金管理技术参考架构

基于金融分布式账本技术的资金管理服务从底层到顶层可划分为基础设施层、金融分布式账本平台层、资金管理服务层、业务应用层等四个边界清晰、高度内聚、有机统一的主要功能层。

- 基础设施层包含机房、服务器、网络设备等基础软硬件设施，为上层提供安全可靠的运行环境；
- 金融分布式账本平台层包含金融分布式账本节点及其内部的通讯、共识、合约、存储等关键模块，为上层提供业务无关的核心金融分布式账本技术能力；
- 资金管理服务层包含基础服务、金融服务、运营管理等服务组件，为上层提供资金管理必须的核心业务中间件；
- 业务应用层包含建工、预付、政务等应用场景，为资金管理应用的最终用户提供丰富、完整、友好的资金管理服务。

注：业务应用层内容见T/NIFA 24—2023《金融分布式账本技术资金管理应用业务要求》。

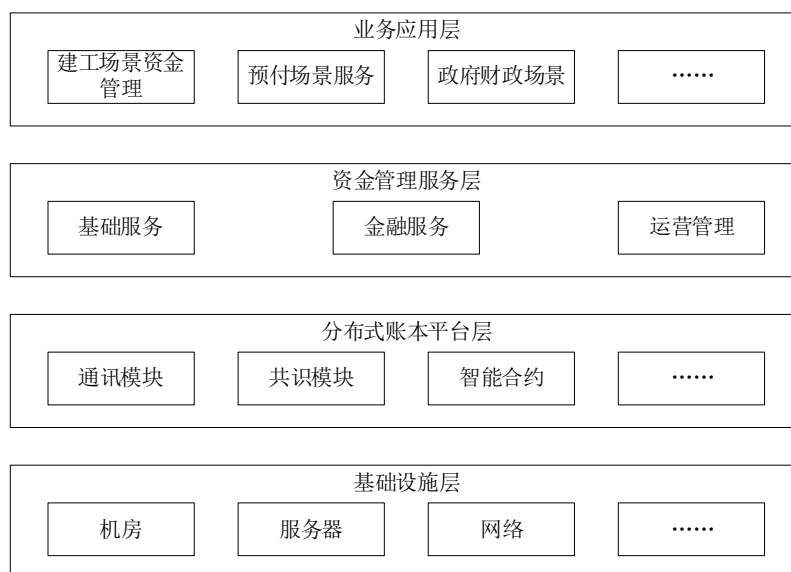


图1 金融分布式账本资金管理应用的参考架构

7 基础设施层

7.1 总体要求

基础设施层是指金融分布式账本技术资金管理应用的基础硬件设施与设备，以及基础软件，分为物理机房、硬件服务器、网络设备、操作系统等基础设施，为金融分布式账本技术资金管理应用的业务系统提供基础支撑环境。基础设施层应使用安全可控、体系架构开放的硬件进行构建，保障安全性、可用性和可靠性。

金融分布式账本技术资金管理应用基础设施层应满足国家及金融行业相关标准中对基础设施层的要求。

7.2 机房要求

7.2.1 物理机房要求

物理机房在选址与设备布置、环境要求、建筑结构、供配电、照明、空气调节、电磁屏蔽、网络与布线、环境与设备监控、消防与安全等方面应达到GB 50174—2017中B级及以上标准。此外，部署的物理机房及附属设施应符合以下要求：

- 对于云端部署模式，应保证用金融分布式账本技术资金管理系统的运行环境位于高安全区域；
- 对于金融分布式账本技术资金管理系统中承担共识节点或记账节点功能的系统节点，宜保证使用者业务运行、数据存储和处理的物理设备位于中国境内；
- 物理数据中心应具备一定的防自然灾害能力，应防水、防潮、防雷击、防火、防静电、防风、防沙，并进行温湿度控制。

7.2.2 安全及管理要求

机房出入人员和物品应进行安全管理，包括但不限于以下要求：

- 机房内应严禁存放易燃、易爆、易碎、易污染、强磁场、腐蚀性物品；
- 机房内的各类设备、资料、磁介质未经批准不得私自带出；
- 机房内设备或主要部件应放置牢固，并设置明显的不易除去的标记；

- d) 应严禁外来人员携带手机、照相、摄像、录音以及其他记录设备等无关物品进出机房；
- e) 外来人员在机房进行维修、维护活动期间，接待部门必须专人全程陪同，并监督、审核全部操作内容。

7.2.3 高可用部署要求

机房的规划和部署应满足对业务高可用、灾备演练、自动主备切换等要求，保障在特殊异常情况下可正常对外提供硬件服务器、网络、基础软件等服务：

- a) 机房应至少进行双园区部署，满足灾备演练以及断电、火灾、地震等特殊异常情况的主备机房切换要求。可选择但不限于同城异地模式，两地多中心等模式；
- b) 金融分布式账本节点设备应部署在不同机构各自的所属机房内，各机构对节点所在的设备应具备全权管理能力；
- c) 金融分布式账本节点应避免出现集中托管或运行于同一物理环境的情况。如存在集中托管情况应具备多园区机房的备份能力。

7.2.4 监控要求

针对机房内环境和设备的监控应具备但不限于以下要求：

- a) 监测和控制机房内的温度，应确保环境满足机房内设备的运行要求；
- b) 机房专用空调、发电机、不间断电源系统等设备应配带监控系统，监控的参数宜纳入设备监控系统；
- c) 宜支持对设备进行智能化故障诊断和健康检查功能；
- d) 可支持基于 RFID 的设备资产管理功能；
- e) 可支持基于 ZigBee 通讯的电池监控管理功能；
- f) 可支持基于智能 PDU 的电能监测等监控功能。

7.3 服务器要求

7.3.1 硬件设备要求

对于金融分布式账本技术资金管理系统中硬件设备主要包括系统部署的服务机，虚拟机归属的物理服务机，云上节点的宿主机，外部存储等。设备指标和基本功能应满足但不限于以下要求：

- a) 应确保设备和存储介质在重用、报废或更换时，能对其承载的数据进行清除且不可恢复；
- b) 应保证不同节点使用的硬件设备具备异构性；
- c) 对于云端部署模式，应在云端环境服务方的配合下，保证云端环境具备一定的异构性；
- d) 应保证设备运行状态或资源使用情况异常时能发出警告；
- e) 对于云上部署的金融分布式账本系统，宜满足以下配置条件：
 - 1) 共识节点部署的服务器或虚拟机，CPU 宜不小于 16C，内存宜不小于 32G、外部存储宜不小于 500G；
 - 2) 记账节点的服务器或虚拟机，CPU 宜不小于 4C，内存宜不小于 8G，外部存储宜不小于 600G；
 - 3) 单个共识节点容器，CPU 配置应大于 1C，内存配置应大于 1024M。

7.3.2 硬件加密设备安全要求

对于使用硬件加密设备完成密码运算和密钥存储的金融分布式账本技术资金管理系统，所用硬件加密设备应满足以下要求：

- a) 硬件加密设备应符合 GM/T 0045—2016 的要求；
- b) 云服务器加密设备应符合 GM/T 0104—2021 的要求。

7.3.3 节点部署要求

对于金融分布式账本技术资金管理系统中节点部署的安全及监控功能应满足但不限于以下要求：

- a) 应保证系统关键节点冗余部署，保证操作系统可用性；
- b) 应保证系统承担共识或记账的节点部署在不同机房内；
- c) 应保证带有不适合共享数据的节点放置于机构内部或受保护区域；
- d) 应保证节点的硬件设备存储容量可扩展，避免因容量达到上限而无法同步账本；
- e) 应在支持物理机、虚拟机、云技术等节点部署方式；
- f) 应具备节点状态展现和信息查询等功能；
- g) 应具备节点日志自动收集和统一查询等功能。

7.3.4 存储功能要求

对于金融分布式账本技术资金管理系统使用的存储设备资源在功能、安全性和高可用等方面满足但不限于以下要求：

- a) 应支持在每个对等网络节点上部署并使用；
- b) 应支持高效、安全、稳定地提供数据写入及查询服务；
- c) 对于采取分库分表的数据存储方案，存储功能组件应支持数据的分片及路由处理能力；
- d) 能够对写入数据做到持久化处理，随账本节点可持续；
- e) 宜支持对存储数据进行高效备份；
- f) 宜支持在存储节点故障后进行快速自检与恢复；
- g) 宜支持对数据的局部或全局进行加密；
- h) 宜提供扩容支持；
- i) 应支持数据备份与恢复功能；
- j) 应支持分布式账本资金管理系统数据的导出功能，支持将分布式账本系统数据导入到其他数据库或者文件系统中；
- k) 宜支持归档存储功能。

7.4 网络要求

7.4.1 网络安全要求

支撑金融分布式账本技术资金管理系统的基础设施在网络架构的安全和通讯传输安全等方面满足但不限于以下要求：

- a) 在网络拓扑中，应防止单个节点故障而形成网络隔离；
- b) 应保证每个重要节点具有较大的局部聚集系数；
- c) 对于金融行业里高敏感度的金融业务，应通过金融专用网或端到端加密的方式与公网隔离；
- d) 应在金融分布式账本各节点间实现信源加密和网络通道加密，信源加密使用加密算法将数据明文转换为密文，网络通道加密可采用 SSL/TLS 协议、SSH 协议、VPN 技术等措施在网络传输过程中对数据进行保护，保证数据机密性、完整性与可用性；
- e) 应对金融分布式账本数据传输实现访问控制，包括但不限于身份认证、权限限制、端口开放限制等技术手段；
- f) 应对数据和信息采取相应的防护措施，保证其能抵抗篡改、重放等主动或被动攻击；
- g) 应增加防火墙设置，避免非法用户访问；
- h) 互联网接入应符合多运营商链路接入，如条件具备，可要求各运营商提供二路由接入机房；
- i) 应提供通信线路、关键网络设备的硬件冗余，保证网络可用性；

- j) 应能对非授权设备私自联到内部网络的行为进行检查或限制;
- k) 应对主机攻击行为可溯源,可还原攻击过程;
- l) 应能检测到对重要节点进行入侵的行为,并且在发生严重入侵事件时提供报警。

7.4.2 节点访问要求

支撑金融分布式账本技术资金管理系统的基础网络设施应满足对金融分布式账本系统组网、内部通讯、外部请求访问等功能的基本要求。

- a) 各节点应支持基于网络通信协议和对等网络进行通信和数据互换;
- b) 通信控制功能应分布在各节点上,且任一节点均至少与其他两个节点建立通信连接;
- c) 保证共识节点或记账节点之间能直接进行网络通信或能间接进行消息传递;
- d) 支持上层服务应用通过域名访问金融分布式账本节点;
- e) 对于负责接入访问金融分布式账本节点的网关应支持负载均衡功能;
- f) 支持对网关设备的自动健康检查功能,对于异常网关能够自动实施隔离措施,并发起报警;
- g) 支持网络故障快速切换功能。

7.4.3 网络监控要求

对于金融分布式账本技术资金管理系统中基础网络的监控功能应满足但不限于以下要求:

- a) 应支持网络故障报警功能;
- b) 应支持网络关键设备或资源的状态可视。

7.5 基础软件要求

7.5.1 安全要求

基础软件环境应遵循GB/T 22239—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要求,同时还应包括以下对访问控制、入侵防范、恶意代码防范等方面的要求:

- a) 应由授权主体配置访问控制策略,访问控制策略规定主体对客体的访问规则;
- b) 访问控制的粒度应达到主体为用户级或进程级,客体为文件级、数据库表级;
- c) 应对重要主体和客体设置安全标记,并控制主体对有安全标记信息资源的访问;
- d) 应遵循最小安装的原则,仅安装需要的组件和应用程序;
- e) 应关闭不需要的系统服务、默认共享和高危端口;
- f) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;
- g) 应提供数据有效性检验功能,保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;
- h) 应能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞;
- i) 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为,并将其有效阻断。

7.5.2 操作系统要求

系统应有针对不同操作系统的软件版本,宜支持至少三种操作系统或系统版本。

示例1: Ubuntu、SUSE、麒麟Neokylin 是三种操作系统。

示例2: Ubuntu 18.04.6 LTS、Ubuntu 16.04.7 LTS、Ubuntu 14.04.6 LTS 是同一种操作系统的三种不同系统版本。

7.5.3 软件部署要求

应支持针对物理机、虚拟机、云上节点等服务器使用的操作系统、数据库、JAVA 等基础软件及其版

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/407012023150006050>