ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0184—2020

金融分布式账本技术安全规范

Financial distributed ledger technology security specification

2020－02－05 发布　　2020－02－05 实施

中国人民银行　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国人民银行数字货币研究所提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行数字货币研究所。

本标准参加起草单位：中国人民银行科技司、中国工商银行、中国农业银行、中国银行、中国建设银行、国家开发银行、平安银行、招商银行、深圳前海微众银行股份有限公司、浙江网商银行股份有限公司、清华大学、上海交通大学、南京大学、浙江大学、中钞杭州区块链技术研究院、中国信息通信研究院、中金国盛认证有限公司、银行卡检测中心、京东数字科技控股有限公司、百度在线网络技术（北京）有限公司、成都卫士通信息产业股份有限公司。

本标准主要起草人：穆长春、李伟、狄刚、姚前、杨富玉、李兴锋、曲维民、赵新宇、钱友才、张红波、施展、张宏慧、崔沛东、王彦博、林华、陈钟、张大伟、周子衡、苏恒、王鹏、肖遥、王维强、范媛媛、吴炜斯、张育明、李斌、左敏、于潇、陆海宁、仲盛、蔡亮、练娜、魏凯、温昱晖、陈聪、曹鹏、肖伟、吴波。

引　言

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。在分布式账本技术形态尚具可塑性的阶段，有必要制定关键技术的安全规范，以便金融机构按照合适的安全要求进行系统部署和维护，避免出现安全短板，为分布式账本技术大规模应用提供业务保障能力和信息安全风险约束能力，对产业应用形成良性的促进作用。

为落实《中国金融业信息技术“十三五”发展规划》（银发〔2017〕140号文印发）和《金融科技(FinTech)发展规划（2019-2021年）》（银发〔2019〕209号文印发）的要求，规范分布式账本技术在金融领域的应用，提升分布式账本技术的信息安全保障能力，特编制本标准。

金融分布式账本技术安全规范

1 范围

本标准规定了金融分布式账本技术的安全体系，包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面。

本标准适用于在金融领域从事分布式账本系统建设或服务运营的机构。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2016（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35273—2017 信息安全技术 个人信息安全规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

GM/T 0006—2012 密码应用标识规范

GM/T 0009—2012 SM2密码算法使用规范

GM/T 0010—2012 SM2密码算法加密签名消息语法规范

GM/T 0015—2012 基于SM2密码算法的数字证书格式规范

GM/T 0028—2014 密码模块安全技术要求

GM/T 0039—2015 密码模块安全检测要求

GM/T 0044—2016（所有部分） SM9标识密码算法

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[GB/T 25069—2010，定义2.2.2.176]

3.2

散列/杂凑函数 hash function

将比特串映射为固定长度的比特串的函数，该函数满足下列两特性：

——对于给定输出，找出映射为该输出的输入，在计算上是不可行的；

——对于给定输入，找出映射为同一输出的第二个输入，在计算上是不可行的。

注：计算上的可行性取决于特定安全要求和环境。

[GB/T 25069—2010，定义2.2.2.166]

3.3

对称密码 symmetric cipher

一种在加密和解密算法中都使用相同的秘密密钥的密码技术。

[GB/T 25069—2010，定义2.2.2.26]

3.4

非对称密码 asymmetric cipher

基于非对称密码技术的体制，公开变换用于加密，私有变换用于解密。反之，亦然。

[GB/T 25069—2010，定义2.2.2.30]

3.5

随机数 random number

其值不可预测的时变参数。

[GB/T 25069—2010，定义2.2.2.182]

3.6

证书 certificate

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

[GB/T 25069—2010，定义2.2.2.218]

3.7

CA证书 CA-certificate

由一个CA颁发给另一个CA的证书。

[GB/T 25069—2010，定义2.2.2.219]

3.8

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

[GB/T 25069—2010，定义2.2.1.42]

3.9

零知识证明 zero-knowledge proof

用以验证某示证者知道某项秘密而不泄露该秘密及其有关信息的方法。

3.10

群签名 group signature

一个群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名。

3.11

环签名 ring signature

签名者指定了一个可能签名者的集合(或环)，并对某消息进行签名。验证者能够确信签名确实由环中的某个成员生成，但是无法指出真实签名人。

3.12

隐私保护 privacy protection

为保护隐私而采取的措施。例如：对个人数据的收集、处理和使用加以限制。

[GB/T 25069—2010，定义2.2.1.122]

3.13

标识密码算法 identity-based cryptographic algorithm

通过用户的身份标识来生成用户的公、私密钥对，主要用于数字签名、数据加密、密钥交换以及身份认证等。

3.14

同态加密 homomorphic encryption

一种加密形式，利用特定代数运算对加密数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密数据得到的输出结果一致。

3.15

秘密共享 secret sharing

一种将秘密（密钥）分割存储的密码技术，可通过将拆分的部分组合在一起来拼凑这个秘密。

3.16

对等网络 peer-to-peer network

一种仅包含对控制和操作能力等效的节点的计算机网络。

3.17

共识协议 consensus protocol

分布式账本系统中各节点间为达成一致采用的计算方法。

3.18

分布式账本 distributed ledger

可以在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的数据库。

3.19

分布式账本技术 distributed ledger technology

实现分布式账本的技术的集合，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。

3.20

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。

3.21

拒绝服务 denial of service

一种使系统失去可用性的攻击。

[GB/T 25069—2010，定义2.2.1.75]

3.22

节点 node

提供分布式账本的所有功能或者部分功能的实体。

3.23

交易验证节点 transaction validation node

负责对提交的交易数据进行验证的节点。

3.24

共识节点 consensus node

负责账本数据一致性的节点。

3.25

记账节点 accounting node

负责账本数据完整性的节点。

3.26

鉴别码 authentication code

由消息鉴别码算法输出的比特串。

注：消息鉴别码有时称为密码校验值。

[GB/T 25069—2010，定义2.2.2.65]

3.27

数据完整性 data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

[GB/T 25069—2010，定义2.1.36]

3.28

保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069—2010，定义2.1.1]

3.29

不可链接性 unlinkability

同一用户在多次交易过程中出示的匿名身份标识，不能够被还原为同一用户。

3.30

一致性 consistency

在某一系统或构件中，各文档或各部分之间统一的、标准化的和无矛盾的程度。

[GB/T 25069—2010，定义2.1.62]

3.31

终局性 finality

交易一旦确认，就不会被回滚（Rollback）或者撤销。

3.32

激励相容 incentive compatibility

一种制度安排，使行为人追求个体利益的行为，正好与整体实现价值最大化的目标相吻合。

3.33

局部广播 local broadcast

通过只向经过授权的相关方节点发送信息的方式避免信息在整个分布式账本上传播。

3.34

混淆技术 mixing

通过割裂交易双方之间的关系令交易流向难于被分析和跟踪，以保护交易细节。

3.35

局部聚集系数 local clustering coefficient

表示一个图形中单个节点聚集程度的系数。

3.36

原子性 atomicity

智能合约在执行过程中发生错误，会被回滚到智能合约开始前的状态。

3.37

图灵完备 Turing complete

在可计算性理论中，一系列操作数据的规则（如指令集、编程语言、细胞自动机）可以用来模拟单带图灵机。

3.38

不可否认性 non-repudiation

也称抗抵赖性，证明一个已经发生的操作行为无法否认的性质。

[GM/Z 0001—2013，定义2.46]

3.39

标识信息 identity information

能够单独或者与其他信息组合以识别、追踪到特定自然人身份或反映特定自然人活动情况的信息。

3.40

隐私 privacy

与公共利益无关，除了只能公开用于有保密义务的一方之外，当事人不愿第三方知道的个人信息及当事人不愿第三方侵入的个人领域。

注：隐私保护的三条要素：

——隐私的主体是自然人；

——隐私的客体是自然人的个人信息和个人领域；

——隐私的内容指特定个人对其信息或领域秘而不宣、不愿他人探知或干涉的事实或行为。

3.41

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。

3.42

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。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

[GB/T 35273—2017，定义3.1]

3.43

控制者 controller

单独或与他人共同确定处理个人信息的目的和方式的自然人、法人或其他机构。

3.44

干预机制 intervention mechanism

禁止或限制参与金融分布式账本系统的特定角色的特定行为，是为异常情况提供的紧急制动措施。

3.45

块/分组密码 block cipher

所用密码算法对明文块（即定义了长度的比特串）进行运算，以产生的密文块的对称密码。

[GB/T 25069—2010，定义2.2.2.82]

3.46

流/序列密码 stream cipher

具有如下性质的对称密码体制：其加密算法利用某一可逆函数将明文符号序列与密钥流符号序列一次一个符号地组合起来进行变换。它可分为两种类型：同步流/序列密码和自同步流/序列密码。

[GB/T 25069—2010，定义2.2.2.85]

3.47

密钥交换 key exchange

在通信实体之间安全地建立一个共享密钥的协商过程。

[GB/T 25069—2010，定义2.2.2.119]

4 缩略语

下列缩略语适用于本文件。

CA：认证机构（Certificate Authority）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DoS：拒绝服务（Denial of Service）

KYC：了解你的客户（Know Your Customer）

MAC：消息鉴别码（Message Authentication Code）

SE：安全单元（Secure Element）

SSL：安全套接层（Secure Sockets Layer）

TEE：可信执行环境（Trusted Execution Environment）

TLS：传输层安全（Transport Layer Security）

5 安全体系框架

金融分布式账本技术安全体系包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面。金融分布式账本技术安全体系框架见图1。

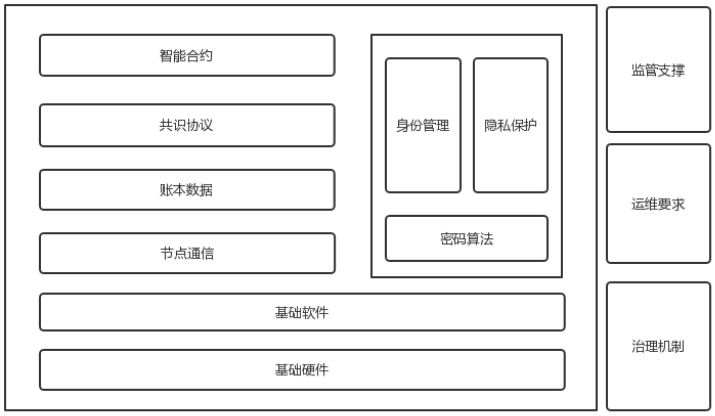

图1 金融分布式账本技术安全体系框架

本标准依照图1，分别提出以下安全要求：

——基础硬件：网络、通信传输、硬件加密设备等硬件设备的安全要求；

——基础软件：节点运行所需的操作系统、运行环境等的安全要求；

——密码算法：所采用的各类算法的安全要求；

——节点通信：节点之间通信传输的安全要求；

——账本数据：节点账本数据在完整性、保密性、一致性等安全要求；

——共识协议：共识协议技术的安全要求；

——智能合约：智能合约的执行环境以及智能合约的安全要求；

——身份管理：用户身份管理的安全要求；

——隐私保护：隐私保护的安全要求；

——监管支撑：为监管功能及特性提供的技术支撑要求；

——运维要求：为保障安全运行所应支持的运维要求；

——治理机制：治理结构以及相关的管理机制。

6 基础硬件

6.1 基本要求

基本硬件环境应遵循GB/T 22239—2019中三级及以上的物理和网络相关要求。

6.2 物理安全

6.2.1 场地安全

部署的物理数据中心及附属设施符合以下要求：

——对于云端部署模式，应保证用于金融行业数据中心运行环境位于高安全区域；

——对于承担共识节点或记账节点功能的系统节点，宜保证金融分布式账本使用者业务运行、数据存储和处理的物理设备位于中国境内。

6.2.2 硬件设备

应对设备运行状态、资源使用情况等进行监控，能在发生异常情况时发出告警。

应保证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。

应保证不同节点使用的硬件设备具备一定的异构性。

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。

6.2.3 节点部署安全

应保证关键节点冗余部署，保证系统可用性。

应避免将所有承担共识或记账的节点部署在同一机房内，应能在单一机房节点不可用时保证系统整体的可用性。

应保证将带有不宜共享数据的分布式账本节点放置于机构内部或受保护区域。

应保证部署节点的硬件设备存储容量可扩展，避免因数据容量达到上限而无法同步账本。

6.2.4 硬件加密设备安全

对于使用硬件加密设备完成密码运算和密钥存储的分布式账本系统，所用硬件加密设备应满足如下要求：

——使用的加密机设备应符合国家密码管理部门颁布的GM/T 0045—2016的要求；

——使用的个人密码设备（如UKey、加密卡、带SE或TEE的移动终端等）应符合行业主管部门和国家密码管理部门的要求。

6.3 网络安全

6.3.1 网络架构安全

应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。

在网络拓扑中，应防止单个节点故障而形成网络隔离。

应保证每个重要节点具有较大的局部聚集系数。

6.3.2 通信传输安全

应在参与分布式账本的节点之间建立安全传输通道，保证数据传输的完整性和不可篡改性。

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。

应采用密码技术保证节点间通信过程中敏感信息字段或整个报文的保密性，应确保信息在存储、传输过程中不被非授权用户读取和篡改。

可采用有权限的网络访问控制，在参与分布式账本节点之间构建虚拟专用网络（VPN），降低网络攻击造成的危害。

7 基础软件

7.1 基本要求

基本软件环境应遵循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，还应包括账本结构、共识模块、分布式组网、数据存储、智能合约、接口设计、数据传输、时间同步和操作系统等方面的要求。

7.2 账本结构

账本结构应具有防篡改性。账本结构宜使用块链式或近似块链式的存储结构，应使用哈希嵌套保证数据难以被篡改。

账本应具有数据校验功能。任何一条记录被非法篡改后都可通过历史账本数据回溯以快速检验出。

7.3 共识模块

共识模块应能协调各系统参与方有序参与数据打包和共识过程，并保证各参与方的数据一致性。

系统无故障节点或欺诈节点时，应能在规定时间内达成一致的、正确的共识，输出正确结果。

在故障节点和欺诈节点的总数量不超过理论值的情况下，系统应能正常工作。

7.4 分布式组网

系统参与方节点应在物理部署上进行分离，各节点基于网络通信协议和对等网络进行通信和数据互换。

各节点应独立存储具有一致性的账本数据，且保证任意单个节点故障都不影响整个系统的正常工作。

系统由分布在不同地点的节点互连而成，网络中可无中心节点。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。

7.5 数据存储

账本数据应根据数据对象的类别独立存储，账户数据、交易数据、配置数据以及账本元数据等，应分别存储、分别管理、分别操作。

敏感信息应加密存储，并应有数据访问等权限的控制和管理。

节点CA证书及其私钥的存储应私密管理。

数据存储可选用结构化数据库、非结构化数据库或混合选用。数据库应选用安全高效并经过检验的主流稳定版本。

7.6 智能合约

智能合约宜在可信的软件/硬件支持的环境中执行。

智能合约代码存储和运行时，系统应具备相应的安全保护能力，不应允许未授权实体明文读取合约代码和状态。

智能合约应具备数据前向兼容的能力，版本迭代时，旧版本的合约应及时停用，并存档数据，新版本合约应能调用历史数据。

智能合约的运行机制宜有前向兼容的能力，当系统版本升级后，智能合约应能正常执行。

系统应通过有效的智能合约审核以确保合约代码所表达的逻辑无漏洞。智能合约的发布应引入相关方联合审核机制，审核流程应高效、严谨。

7.7 接口设计

应设计良好的接口，隐藏底层账本的细节，为应用层提供简洁的调用方法。

接口的设计原则应简洁明了，提供完整的功能，能完成交易和维护分布式账本数据，并且有完善的权限管理机制。

接口设计应考虑扩展性和兼容性。

7.8 数据传输

传输数据过程中，应使用对称或非对称国密算法对数据进行加密，防止数据在传输过程中被窃取。

7.9 时间同步

应保证节点之间的时间戳误差维持在共识协议允许的范围内。

可使用经过认证的中心化时间同步源进行节点间的时间同步。

7.10 操作系统

系统宜有针对不同操作系统的软件版本，宜支持三种及以上的操作系统或系统版本。

8 密码算法

8.1 基本要求

分布式账本系统中的密码算法主要用于数据安全，即保护数据的保密性、完整性、真实性和不可否认性，包括分组密码算法、流密码算法、非对称密码算法、密钥交换算法、密码杂凑算法和标识密码算法等。分布式账本系统所使用的具体密码算法应符合GB/T 32905—2016、GB/T 32907—2016、GB/T 32918—2016等相关国家标准以及GM/T 0006—2012、GM/T 0009—2012、GM/T 0010—2012、GM/T 0015—2012、GM/T 0044—2016等相关行业标准。分布式账本系统应使用符合GB/T 37092—2018等相关国家标准以及GM/T 0028—2014、GM/T 0039—2015等相关行业标准的密码模块进行密码算法运算和密钥存储。

8.2 保密性

保密性指信息不被泄露给非授权的用户和进程等实体的一种性质。

保密性通过密码加密功能实现，其算法包括对称密码算法和非对称密码算法。

通信双方在交换敏感信息时，应在建立连接之前，使用密码技术进行会话初始化，通过密钥交换算法协商会话密钥。在通信过程中，应使用会话密钥对敏感信息或整个报文进行加密，并在加密时采取随机数填充等技术，避免相同的明文数据在加密后生成相同的密文。

在存储敏感的业务数据、身份鉴别数据和密钥数据之前，应采用密码技术进行加密。

8.3 完整性

完整性指数据没有受到未授权的更改，分布式账本中的完整性应用场景包括业务数据和密钥的完整性保护。

应保障关键数据在传输和存储中的完整性，并在对数据处理前检验其完整性。

数据完整性可通过消息鉴别码（MAC）或数字签名保障。

8.4 真实性

真实性指一个实体是其所声称实体的特性。

应使用非对称加密、动态口令或数字签名等方式保障真实性。

分布式账本中真实性的应用场景包括：

——进入重要物理区域人员的身份鉴别；

——节点通讯双方的身份鉴别；

——网络设备接入时的身份鉴别；

——登录操作系统和数据库系统的用户身份鉴别；

——应用系统的用户身份鉴别。

8.5 不可否认性

可使用数字签名等密码技术生成可靠的电子签名来保障实体行为的不可否认性，系统中所需的具有不可否认性的行为包括发送、接收、审批、创建、修改、删除、添加和配置等操作。

不可否认性的应用场景包括：

——实体行为的确认；

——背书方对实体行为的背书。

8.6 随机性

密码算法执行过程中需要使用随机数时，应按照国家密码管理部门的要求生成随机序列，并符合GB/T 32915—2016对随机性的要求。

8.7 密钥管理

密钥管理包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程。分布式账本系统应根据信息系统等级保护等级，满足GM/T 0054—2018中对密钥管理的要求。

可通过秘密共享算法将密钥分解为多个子密钥分别存储或传输。

9 节点通信

9.1 基本要求

分布式账本系统采取节点授权准入的原则，在节点通信过程中应保证数据的完整性、保密性。

9.2 节点身份验证

应使用符合第13章“身份管理”中要求的身份认证机制控制节点的接入。

采用密码技术对节点通信双方的身份进行验证。

9.3 通信完整性

使用符合国家密码标准的消息鉴别码算法、数字签名等密码技术来提供通信中数据的完整性保护和校验。

节点间通信协议应具备应对通信延时、中断等情况的处理机制。

当检测到数据的完整性遭到破坏时，接收节点可以采取措施从发送节点处重新获取数据。

9.4 通信保密性

在通信节点建立连接之前，应使用符合国家密码标准的密钥交换技术来产生双方共享的工作密钥，并进行双向身份认证，确保通信节点是信息的真实授权方。

通信节点应使用工作密钥对通信过程中的整个报文或会话进行加密处理。

应使用符合国家密码标准的技术来建立安全通信通道，避免因传输协议受到攻击而出现的保密性破坏。

10 账本数据

10.1 完整性

应保证账本数据的生成、传输、存储、调用等操作不可被非授权方式更改或破坏。

10.2 一致性

分布式账本中记账节点的账本数据应保持一致。对账本数据的写入和修改，须经各节点达成共识，以确保各节点的数据一致性。当出现数据分叉时，应存在可用规则进行数据选择。

10.3 保密性

应采用密码技术保证账本数据中的敏感数据在传输和存储过程中的保密性。

账本数据中敏感数据的保护密钥和账本数据本身应分开保存，并且保护密钥应支持存放在安全的密码模块中。

10.4 有效性

各记账节点的账本数据应符合第 11 章“共识协议”中要求的共识协议保证账本数据的有效性，且满足以下有效性要求：

——应能对节点存储的账本数据的有效性进行校验；

——当某个节点的账本数据失效时，应使用符合第 11 章“共识协议”中要求共识协议保证账本数据的有效性。

10.5 账本数据冗余

应保证账本数据在系统中具有冗余性，防止因单个节点失效而造成总账本数据的丢失。

10.6 访问与使用

分布式账本应确保账本数据不被未授权的第三方获取，数据访问和操作应符合第 14 章“隐私保护”中对认证授权、访问控制等方面的技术要求。

10.7 安全审计

记账节点对账本数据的操作应满足以下安全审计要求：

——账本数据的访问应提供安全审计功能，审计记录包括访问的日期、时间、用户标识、数据内容等审计相关信息；

——数据变更应提供审计功能，审计记录不仅包括数据变更成功的记录，还应包括数据变更失败的记录；

——节点有效性校验失败、一致性校验失败等情况下同步账本数据，应提供安全审计功能，审计记录包括事件类型、原因、账本数据同步的节点、账本数据校验值等审计相关信息；

——审计记录可由记账节点自行记录，不必写入账本。

11 共识协议

11.1 基本要求

应根据业务特点选用适宜的共识协议，包括但不限于工作量证明、权益证明、授权股权证明、拜占庭容错等，应满足不同共识协议安全运行所必需的前提要求，且业务激励规则和技术运维安全上的机制设计应保障其自身安全。

11.2 合法性

应确保参与共识过程的节点经过验证，保证节点共识过程的加入和退出的合法性，以及节点ID与节点实体的一一对应，以形成可信节点。

11.3 正确性

共识协议依据的算法理论应公开或经过安全评估，如有修改应经过同行评议。

协议算法的测试应全面完整，宜应用形式化验证或进行代码审计以确保算法实现的正确性。

可信节点应为协议算法的运行提供安全可信的硬件软件（如服务器、操作系统等）基础，确保协议算法运行环境的安全性与可靠性。

11.4 终局性

算法应在可接受的有限时间内具有终局性。

所有参与共识的可信节点，经过一段可接受时间内的交互，应最终达成一致性结果。

11.5 一致性

所有参与共识的可信节点得到的计算结果应是相同的，且符合共识协议。

11.6 不可伪造性

系统中恶意节点占比不超过共识协议容错率时（如采用工作量证明时该比例约为1/2），任何对系统当前状态进行恶意构造以欺骗其他可信节点所需要的时间，应不少于可接受范围。

11.7 可用性

协议应具备抗DDoS攻击、处理恶意报文、识别恶意节点的能力，且应采取不转发、拒绝连接、黑名单等措施缩小影响，使系统获得一定的主动防御能力，提高系统的可用性。

系统能始终在正常时间内对客户端的请求进行响应。

11.8 健壮性

数据在遭受恶意攻击后被污染时，被攻击节点应通过与系统中其他可信节点交互等方式来检测出攻击及数据污染。

系统中的节点如遇到网络故障等情况与系统断开连接，可能会出现与系统中其他节点状态不一致的情况。在恢复连接后，通过与系统中其他可信节点交互等干预方法，保证节点数据恢复正常状态且受攻击前的数据不会丢失，并保持与正常节点间数据的一致性。

11.9 容错性

系统中恶意节点占比不超过共识协议的容错率时，系统应保证正常运作，且保持数据一致性。

11.10 可监管性

单次共识过程和系统运行的整个共识历史都应可审计、可监管，该历史应不可被篡改。

11.11 低延迟

共识协议应保持低响应延迟，满足金融系统对于数据同步的时间要求。

11.12 激励相容

应采用激励机制保障系统安全，计算系统可承载的价值上限，并对其上的应用进行检查，避免超过安全阈值。

11.13 可拓展性

协议应具备动态拓展能力，可允许在系统保持正常服务的前提下动态或静态增删节点。

12 智能合约

12.1 基本要求

可支持非图灵完备智能合约和图灵完备智能合约，两者都应符合本章安全要求。

12.2 版本控制

应在源代码中通过金融分布式账本指定的方式定义版本号。

应在配置文件中定义版本号，该配置文件应与智能合约代码一同部署。

应在部署或升级操作时定义版本号。

智能合约升级后，应在金融分布式账本中保留前一版本。

交易信息中应明确调用的智能合约版本。

12.3 访问控制

应有相应的机制控制用户对智能合约的访问。

应有相应机制在支持智能合约之间相互访问的条件下，限制错误智能合约的感染。

应有相应机制控制智能合约对外部环境的访问。

宜针对智能合约提供隔离的执行环境。

12.4 复杂度限制

宜从合约源代码总长度、资源消耗和执行时间等方面限制合约代码的复杂度。

12.5 原子性

智能合约的执行应有原子性，支持执行过程中发生错误时的回滚操作。

一旦出现异常，所有的执行应被回撤，以避免中间态导致数据不一致。

12.6 一致性

智能合约执行应具备一致性，合约在所有金融分布式账本网络节点上的执行结果应完全相同。

多个节点同时实现合约时，应保证数据的完整性且数据同步不相互干扰。

12.7 安全审计

智能合约的安全审计和评估对象应包括智能合约设计与业务逻辑安全、源代码安全审计、编译环境审计及相关的应急响应机制等。

智能合约应经过相关专业技术人员的审计，并保留审计记录。

12.8 生命周期管理

从部署到废止的生命周期满足以下要求：

——应有相应机制控制智能合约的部署行为，防止恶意部署智能合约；

——应提供智能合约的冻结功能，防止智能合约的漏洞持续影响系统；

——应提供智能合约升级方案和机制以修复智能合约的漏洞；

——应提供智能合约的废止功能；

——应支持权限可控的智能合约升级方法；

——应支持从金融分布式账本中获取与合约相关的原始数据来解析智能合约在金融分布式账本上的业务数据；

——应在合约更新升级、重新部署后，能安全地将原合约数据迁移至新合约。

12.9 攻击防范

应有相应机制保证系统能对抗由智能合约引起的DDoS攻击，防止其长时间占用资源。

应有相应机制保障在系统遭受DDoS攻击、服务受到影响时，智能合约的运行可被干预。

应有相应机制防止隔离执行环境中的智能合约访问其执行环境之外的资源。

12.10 安全验证

应基于智能合约安全规则库和问题合约模式库实现智能合约的漏洞检测，可从合约源码和字节码两方面进行安全扫描。

应实现基于安全规则和配置信息自动生成安全智能合约模板的机制。

宜通过形式化方法验证智能合约代码的正确性。

13 身份管理

13.1 基本要求

应实现有效的用户身份管理，主要功能包括身份注册、身份核实、账户管理、凭证生命周期管理、身份鉴别、节点标识管理、身份更新和撤销等。同时，应保障身份信息的安全性，并对身份进行监管审计。

13.2 身份定义

身份是指涉及自然人及法人等实体的属性的集合。在金融分布式账本系统中，身份可以进行数字化标识（简称数字标识）。

账户是身份的一个属性集合，分为系统用户账户和应用账户。系统用户账户包括普通成员账户、系统管理员账户和其他特定权限的系统用户账户，其中系统管理员账户具有最高权限（如部署智能合约）。在金融分布式账本系统中，一个身份可对应多个账户。每个账户应关联一个身份标识，即身份凭证。身份凭证是用户实体通过身份鉴别后，由鉴别者为用户出具的一种可信任的电子凭据，包括但不限于数字证书和公私钥对等，不同的鉴别及验证方式应遵循金融业的业务及监管要求。

注1：身份定义的实体范围为自然人和法人等，不包括设备实体。

注2：身份注册是指自然人及法人等实体向注册机构提供权威机构发行的法定身份证件等身份证明材料，申请获取账户和身份凭证。

注3：身份核实是指注册机构向身份信息权威机构核验注册者提供的身份证明材料是否与注册实体一致。

注4：账户授权是指身份注册机构对注册实体的账户进行权限分配的过程。

注5：凭证签发是指完成身份核实后，身份注册机构向注册实体的账户发行身份凭证。

注6：身份鉴别是指自然人及法人在使用分布式账本服务/活动过程中，对注册实体的凭证和属性进行鉴别的过程。

13.3 身份注册

身份注册机构应建立健全身份生命周期的管理规章制度和信息系统，并确保身份生命周期管理过程中无信息泄露等安全问题。同时，身份注册机构应接受监管部门的紧急干预和审计追踪。

注册机构对注册实体信息的收集、使用、存储、传输、销毁等过程应符合国内外相关法律法规。

注册机构对注册实体信息的收集应符合最小化要求。

注册机构对注册实体信息的收集应取得信息主体的明示同意。

注册机构对注册实体信息的保存时间应符合最小化要求。

注册实体应按照注册机构的要求提供实名登记信息和身份核实所需材料，并确保其真实有效。

注册过程中，注册机构应避免注册主体重复注册，并保证注册主体提交信息的传输安全和存储安全。

13.4 身份核实

注册机构应核实注册实体身份，确保参与主体的身份真实可信。

注册机构应完善核实管理制度，增强核实系统能力。

核实过程应避免单人完成操作。

核实过程应避免主观臆测，应具备材料核验的技术手段。

核实过程应能接受监管审计。

在身份核实阶段不应弄虚作假、核实操作员不应渎职不作为、核实过程应严谨。身份核实错误导致的系统损失由身份注册机构承担。

存在隐私保护需求的金融分布式账本系统可使用匿名身份认证。但应遵循“前台自愿、后台实名”的原则，前台使用匿名标识，后台应能还原注册实体的实名身份。

13.5 账户管理

13.5.1 账户创建

应具备账户管理功能。

每个账户应关联一个身份标识，并在交易数据中携带发送方的账户身份标识。

账户的身份标识应在该分布式账本系统中具有全局唯一性，且不易被冒用。

对于存在隐私保护需求的系统，应支持账户标识的匿名化处理。

应设置普通用户账户、管理员账户和其他具有特定权限的系统账户。管理员账户应具有冻结和解冻其他账户的权限。

系统应提供上述三类账户相应的注册、授权、变更和注销功能。

13.5.2 账户授权

授权应由身份注册机构完成或发起。

普通权限可由身份注册机构独立完成授权。

监管等特殊权限的授权，应由身份注册机构发起，并按照定义好的共识策略，由各个参与方共同决定，达成共识后完成授权。共识策略由身份注册机构制定，各参与方应知晓并认同该策略。

13.5.3 凭证签发

用户在获取其身份凭证时，凭证签发机构应通过权威机构对实名登记信息进行核验后，方可颁发身份凭证。

系统为不同的用户分配不同的身份标识，标识应具有不易被冒用的特点。

13.5.4 账户冻结和解冻

账户冻结应由注册机构发起，经共识后修改账户状态为冻结。冻结的账户不能进行交易。

账户解冻应由注册机构发起，达成共识解冻后的账户可继续进行交易。

13.5.5 账户锁定和恢复

为防止恶意的私钥重置，系统应设置一个重置私钥的锁定窗口期。

在锁定窗口期内，用户无法进行账户资产操作，但用户可通过原有的私钥来解除重置并恢复账户状态。

窗口期结束后，如果没有发生解除重置，用户才可执行公私钥对的重置操作。

重置私钥的锁定窗口期可通过系统治理参数进行设置。

13.5.6 账户注销

账户应设定使用期限，过期账户应被注销。

应提供注销申请功能。实体申请注销或因法律和监管等要求而强制注销账户时，应能及时注销。

应定期发布公开和可查询的账户注销列表。

若私钥丢失，应能在不修改账户身份标识的情况下重置公私钥对，保证账户的资产不丢失。

对于已注销账户，在取消其登录和操作权限的同时，应长期或永久保留其登记信息，并永久保留其身份标识，避免重复分配。

13.6 凭证生命周期管理

13.6.1 基本要求

金融分布式账本的凭证管理应包括凭证的产生、存储、使用、撤销、终止整个过程的管理。

对不同金融业务所需凭证中包含的信息、数据格式和加解密规则，应编写专门的文档加以说明。

应明确用户身份凭证类型和内容，如数字证书、认证口令、生物特征等。

应记录用户身份凭证建立、更改、授权、禁用、终止等操作日志，确保用户身份凭证相关操作可追溯。

应建立用户身份凭证信息防伪机制与管控措施，避免用户身份被冒用或相互转借等安全风险。

13.6.2 凭证产生

应由用户向凭证提供方发起凭证申请。

凭证提供方应对用户进行身份核验（身份核验可通过离线或在线方式进行）。

应将账户身份标识和凭证之间的关系进行解耦，不允许二者存在数学运算关系。

通过身份核验后，凭证提供方生成带有其数字签名的凭证发放给用户。

13.6.3 凭证发放

身份注册机构应保证数字身份凭证的私有部分的安全传输。

身份注册机构应确保数字身份凭证的私有部分不被第三方窃取。

身份注册机构可保留注册实体的数字身份凭证中可公开的部分，用于身份验证。

13.6.4 凭证存储

凭证应由用户和凭证提供方双方各自进行安全存储。

凭证存储应符合第14章“隐私保护”中相关个人隐私数据保护要求。

应明确用户身份凭证实现机制以及持久性存储的目的、方法和位置。

宜建立用户身份凭证存储方法评估程序。

13.6.5 凭证流转

凭证流转应由用户发起，对凭证信息的访问应经过用户授权许可。

13.6.6 凭证验证

凭证支持基于密码算法的验真功能。

凭证需求方应对用户提交的凭证进行真实性验证。

凭证信息的获取应遵循最小化原则。

13.6.7 凭证更新

凭证到期之前，应根据用户提出的更新请求，采取安全快捷的方式确保用户凭证重新生效。

应建立保障机制，确保用户数字身份属性变动时，应能及时更新属性值。

变更属性核实确认后，应进行更新登记，并将结果反馈给用户完成更新流程。

13.6.8 凭证终止

凭证提供方应根据需要设置凭证的有效期限，凭证到期自动失效。

凭证生命周期管理的每个过程都应有对应的信息存证操作，存证通常是可通过密码学方式证明某件事或某项文件为真的证据。

13.7 身份鉴别

应提供专门的组件或模块实现用户身份认证功能，该组件或模块应确保正确标识和鉴别相关个人、组、角色、设备、应用等主体身份信息和授权信息。

应采取技术措施对通讯双方的身份进行认证。

应采取必要措施，防止认证信息被窃听或冒用。

应具有认证失败处理机制，可采取结束会话、限制非法认证次数和自动退出等操作。

应使用安全并符合国家密码管理规定的算法和协议进行身份认证，并设置最小化反馈和安全退出措施。

涉及跨系统业务的分布式账本系统，应满足跨系统的身份认证要求。

使用公钥密码算法实现身份认证的分布式账本系统，在交易过程中的电子签名应具有不可抵赖性。

鉴别过程应采用数字签名等技术确保安全性，且不应传送鉴别凭证的私有部分。

应采用密码技术和访问控制技术，确保用户口令等身份认证相关凭证信息的存储安全性。用户口令应经过散列函数处理后，进行加密保存，避免以明文或可逆加密、易于碰撞探测的方式保存用户口令。

应定期对用户账号的使用情况进行安全性分析，对登录时间、登录位置、访问时长、访问模块等进行综合分析，并评估账号安全风险。

对重要数据、业务或系统的操作，应采用双因素身份认证。

使用匿名身份认证的分布式账本系统，其匿名认证方式应具有匿名性、不可伪造性和不可链接性。

13.8 节点标识管理

应明确节点授权机构及管理员。

通信节点加入系统之前，应由授权机构给予其在系统内唯一的节点标识，并提供与之对应的标识鉴别信息和标识凭证，授权机构应在凭证中指定节点角色。

标识凭证由授权机构确保其完整性和真实性，应符合第8章“密码算法”中对完整性和真实性的要求。

标识鉴别信息应具有不易被仿冒的特点，如数字、字母和特殊字符的组合，并设定更换期限，应在期限到来之前进行更换。

在传递及存储标识鉴别信息之前，应采用符合第8章“密码算法”中要求的保密性及完整性保护。

节点之间建立数据通信连接之前，应先通过标识鉴别信息实现双向身份认证，并建立一条安全的数据通信信道，该过程应符合第8章“密码算法”中对保密性和完整性的要求。

应具有节点标识认证失败时的处理机制，可采取结束通信、限制认证失败次数和超时自动结束等措施。

13.9 身份更新和撤销

应提供实体对身份信息进行更新和撤销的功能。

当实体对身份信息进行更新时，应针对身份信息进行重新核实。

13.10 身份信息安全性

13.10.1 基本要求

身份信息安全除满足GB/T 35273—2017中关于开展收集、保存、使用、共享、转让、公开披露等信息处理活动应遵循的原则和安全相关要求外，还应从保护身份标识和身份属性两方面保证安全性。

应根据风险要求，将身份数据元素存储在不同的系统中，并在相应系统中受到不同等级的保护，保护要求应依据具体业务进行特定说明。

应根据金融业务需求制定身份数据保密性要求，确保数据不暴露给未经授权方。

系统应提供基于属性的访问控制，在数据对象的整个生命周期中身份数据始终保持保密性、完整性，和可验证性。

除保护存储数据的流程之外，系统还应制定合规、认证和审计策略，并考虑监管要求和隐私保护要求。

应在用户注册时授予访问安全系统的权限。

可为常见用户级别预定义访问控制设置以对访问进行差异化管理，降低管理复杂性。

可具备授权功能作为访问控制的扩展。

13.10.2 密钥安全性

应编写针对性的文档说明身份密钥的类型及生命周期管理，说明使用的密钥、算法、机制为身份标识提供保密性和完整性保护。

密钥管理系统应具有管理密钥创建、派生、分发、存储、安全性和其他管理安全审计功能。金融分布式账本系统中，身份密钥的管理应遵循金融行业密钥管理标准。

系统应在用户丢失密钥、密钥过期或受到其他危害时提供密钥轮换、销毁和替换的方法。由于需要限制风险暴露，密钥轮换、销毁和替换的管理应充分标准化。

用户身份密钥应采用符合金融市场所需的目标级安全要求的加密算法及密钥长度。

13.10.3 安全加密

采用的密码算法和密码技术应符合国家密码管理部门颁布的GM/T 0045—2016。

应具有在客户端保护私钥及凭证的手段，如采用的个人密码设备应符合行业主管部门和国家密码管理部门的要求。

应具备时间戳功能，保证正确的交易顺序。

13.11 身份监管审计要求

13.11.1 监管

监管信息应至少包括金融监管信息，具体为现工作单位/就读学校、行业类型、居住国家/地区、民族、居民/非居民、出生日期、个人月收入、税务信息等监管数据项和反洗钱特色数据项。

身份注册机构应具备收集客户监管信息的方法和手段。

监管权限应严格审批和使用，宜采用共识策略。

身份注册实体、凭证适用方应明确信息监管的目标、方式、范围、规则等，监管机构应征求并取得授权。

在特殊情况下，监管机构无需征得信息主体的授权同意，包括如下情况：

——与国家安全、国防安全直接相关的；

——与公共安全、公共卫生、重大公共利益直接相关的；

——与犯罪侦查、起诉、审判和判决执行等直接相关的；

——出于维护信息主体或其他个人的生命、财产等重大合法权益但又很难得到信息主体同意的；

——所收集的信息是信息主体自行向社会公众公开的；

——从合法公开披露的信息中收集主体信息的，如合法的新闻报道、政府信息公开等渠道；

——根据信息主体要求签订和履行合同所必需的；

——用于维护所提供的产品或服务的安全稳定所必需的，例如发现、处置产品或服务的故障；

——信息控制者为新闻单位且其在开展合法的新闻报道所必需的；

——信息控制者为学术研究机构，出于公共利益开展统计或学术研究的必要，且其对外提供学术研究或描述的结果时，对结果中所包含的信息进行去标识化处理的；

——法律法规规定的其他情形。

13.11.2 审计

应对身份、账户、凭证的访问和更改提供安全审计功能，审计记录包括访问的日期、时间、用户标识、数据等审计相关信息。

身份生命周期管理中需要通过共识机制完成的业务流程，应记录策略、共识节点、账本数据校验值等审计相关信息。

审计记录不仅包括变更成功的记录，还应包括变更失败的记录。

14 隐私保护

14.1 隐私保护原则

金融分布式账本上所有的隐私保护行为应符合GB/T 35273—2017中的“个人信息安全基本原则”，且不违反金融业相关监管要求。

个人信息应以合法、公正、透明的方式处理。

个人信息收集目的应明确和合法，任何与目的不符合的方式不可采用。

信息收集应遵循最小化原则，个人信息收集应仅限于一切与信息收集目的相关且必要的数据。

个人信息应准确，如果需要应尽可能保持最新的信息。

在仅收集必要的个人信息的情况下，允许收集的数据以可识别的形式保存。

应确保个人信息以适度安全的方式处理，包括使用适当的技术或机制来对抗未经授权或非法的处理、意外遗失、灭失或损毁等情况，其技术手段应符合金融业认定的技术方式和相关信息保密方式。

14.2 隐私保护内容

本标准中所涉及的隐私信息是指在金融分布式账本系统中，单独或者与其他信息相结合能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，包括但不限于分布式账本系统中各方的账户信息、鉴别信息、交易信息、个人身份信息、财产信息及其他反映特定自然人活动的各种信息。

应将隐私信息按照敏感程度进行分级，并设置对应的隐私保护策略。低隐私保护要求类别信息经过组合、关联和分析后可能产生高隐私保护要求类别信息，应根据实际情况采用对应的高隐私保护策略。

14.3 隐私保护策略

14.3.1 概述

分布式账本提供的信息保密性和隐私保护的程度与执行效率方面存在制约关系，相关方应根据具体场景选择不同的方法和技术，制定隐私保护策略，达到满足系统目标的平衡状态。

14.3.2 信息公开可验证

公开交易内容信息以及交易方信息。

应对交易方身份信息进行标识和鉴别。

应确保交易方无法被冒用。

公开的信息应确保任何人能进行有效性和正确性的验证。

14.3.3 信息加密可验证

应对交易内容信息以及交易方信息至少其一进行加密。

应确保参与方以及审计方拥有对加密信息解密验证的能力。

应确保除交易参与方以及审计方外，他人无法从加密信息获取任何其他信息。

应确保交易方无法被冒用。

应确保除交易参与方外他人无法伪造加密信息。

应确保任何人可对加密的信息进行有效性和正确性的验证。

14.3.4 信息由交易验证节点验证

应对交易内容信息以及交易方信息至少其一进行加密。

应确保参与方、交易验证节点以及审计方拥有对加密信息解密验证的能力。

应确保除交易参与方、交易验证节点以及审计方外，他人无法从加密信息获取任何知识。

应确保交易方无法被冒用。

应确保除交易参与方外他人无法伪造加密信息。

应由交易验证节点负责对信息进行解密验证，以对其有效性和正确性进行验证。交易验证节点承担对已验证交易信息的担保责任。

他人应通过交易验证节点的验证信息对交易的有效性和正确性进行验证。

14.4 隐私保护技术要求

隐私信息生命周期是指在金融分布式账本上对隐私信息进行收集、传输、共识、存储、使用、销毁等处理的整个过程。应从认证授权、访问控制、保密、完整性、审计、监控、策略等方面，采取相应的技术手段保证隐私信息全生命周期各环节不被未授权的第三方获取，并保护交易方的身份不被识别和冒用。

隐私保护技术和方法包括认证授权、局部广播、摘要存储、变更标识、混淆技术以及零知识证明、群签名、环签名、同态加密等算法组合，可根据业务场景组合解决方案，实现信息保密性和隐私保护的目的。

隐私保护技术要求如下：

——信息采集时应有醒目提示信息，并明确告知客户哪些个人信息会被采集；

——信息采集时应包含客户勾选同意或确认的操作步骤，应有明确授权；

——信息采集时应默认对身份标识信息进行部分隐藏，同时提供全部显示手段；

——信息采集时应对客户和采集的信息进行匹配认证，并对完整性进行校验；

——信息采集时应明确告知收集信息的目的、处理方式、存储期限、智能合约逻辑内容；

——信息传输时应对信息进行全量加密，加密的密钥和证书不能采用信息传输的同一传输通路进行传递；

——停止运营产品或服务时，应及时停止收集数据的活动，并及时告知客户和为客户提供信息注销不可见的手段，并向其他节点或组织发布停止运营和处置数据的信息；

——密钥发送客户后应明确告知其妥善保管密钥，并提供密钥更换手段；

——信息存储时应对客户的隐私信息进行加密；

——信息存储时应对客户身份标识信息进行摘要存储；

——信息在第三方存储时应告知客户并获得客户授权；

——信息展示时应对客户身份标识信息进行部分隐藏，可额外提供全显示手段，非密文展示应采取去标识化措施；

——信息展示时，对非本人展示应先获得信息所有者的授权，并对展示人进行认证；

——信息使用时，应明确记录使用者、使用内容、使用时间、使用频率；

——信息向外部扩散时，应告知客户并获得授权，并提供给客户延缓甚至中断扩散、减少扩散影响的手段；

——应向客户提供信息备份和导出的手段，备份和导出的信息应加密处理，并向客户提供解密手段；

——应向客户提供信息注销不可见的手段；

——信息注销不可见时应获得客户认证和授权；

——信息加工后产生的信息，也应满足上述各项要求。

14.5 隐私保护监控与审计

应制定完备的隐私保护审计方案，审计内容包括隐私保护策略和隐私保护技术手段，审查形式包括但不限于日常监控、定期审计、不定期审计。

应审查所制定的隐私保护策略和隐私保护技术手段的合理性，包括但不限于对隐私保护原则的遵循程度，对不同隐私保护等级的金融信息风险防范要求的匹配度，在当前技术环境下的适用性。

应审查隐私保护策略和隐私保护技术手段的执行过程，审查对象包括但不限于操作手册、操作记录等支持性文档，确认执行过程遵循并实现既定的策略和技术手段。

应审查隐私保护策略和隐私保护技术手段的实际执行效果，确认隐私保护内容得到有效保护，达到既定的风险防范要求。

应在必要时对隐私保护策略进行修订，对隐私保护技术手段进行变更，并按照新的策略和技术手段实现隐私保护。具体地，可在分布式账本系统中设定超级账户，由其执行隐私策略和技术手段的变更。

针对不同隐私保护等级的金融信息制定不同的监控和审计规则和策略。

15 监管支撑

15.1 基本要求

金融分布式账本系统具有架构去中心、数据多副本、交易点对点、记录不可篡改的特点，与中心化系统有很大差异，不仅需要法律监管规则，也需要技术监管规则，以优化系统设计、保证系统安全、提高监管效率、降低合规成本。

15.2 系统监管

应支持监管机构的接入，以满足信息审计和披露的要求。

应支持监管部门的监管活动，包括但不限于设置监管规则，提取交易记录，按需查询、分析特定业务数据等。

应支持监管机构访问最底层数据，实现穿透式监管。

15.3 信息管理

应支持还原匿名标识中的用户真实身份以及相关交易信息，配合交易审查，加强KYC管理。

15.4 事件处理

当系统或交易出现问题时，应能主动报警，采取适当纠正措施，并向监管机构、管理机构报送事件信息。

15.5 交易干预

应具备限制交易权限、冻结账户等功能，为监管机构提供交易干预的技术手段。

15.6 智能合约监管

应能按需将监管要求编码写入智能合约强制执行。

应能根据需要为监管机构提供交易行为统计数据，评价智能合约所提供服务的合规性。

16 运维要求

16.1 基本要求

运维要求应符合GB/T 22239—2019中安全运维管理相关要求，同时还应包括设备管理、节点监控、节点版本升级、漏洞修复、备份与恢复、应急预案管理、权限管理、议案机制等功能。

16.2 设备管理

加密机应放于专门区域，指定专人管理，并定期进行维护管理。

应采用白名单机制控制对加密机的访问，阻止非授权设备访问加密机。

在报废加密机前，应将加密机内的密钥完全清除，确保加密机内的密钥等敏感数据无法被恢复重用。

严格控制加密机的变更操作，经过审批后才可进行变更操作，并须留下变更相关的审计日志。

加密机以外的设备应遵循GB/T 22239—2019中的相关要求。

对网络中的主节点性能，需要根据实际承载的业务场景协商接入标准，主节点应满足该协商标准。

注：网络中主节点性能指标包括CPU、内存、带宽等指标。

16.3 节点监控

应对节点运行状态以及节点与其他节点的连接进行监控。

应对节点进行高可用的架构，用来应对部分节点的异常。如发现部分节点运行异常，应在不影响服务运行的同时及时进行问题的排查，在规定的时限内将节点恢复至正常状态或启动备用节点，以保证业务的正常运行。如果无法在规定的时限内恢复节点，则应将情况上报管理委员会。

如发现节点与其他节点的连接异常，应在不影响服务运行的同时，排查其他节点的故障，且应将情况上报管理委员会。

应收集系统中运行的状态数据，包括节点的远端同步节点数、账本同步平均耗时、节点的健康状态等，并写入日志供测试或者审查用，如异常应及时预警并处理。

如发现恶意或者欺诈节点传播恶意损坏的账本数据，或者有节点篡改账本，应先定位节点位置，获取详细信息，上报管理委员会。

16.4 节点版本升级

节点的版本升级前，应在测试环境进行验证，应保证升级过程中对业务的平滑过渡。除非发生重大安全事故，应避免采用所有节点同时停止服务进行升级的方式。

节点的版本升级应支持向下兼容，升级后仍须支持旧版本的数据。

节点的版本升级应记录升级过程中相关操作日志，做到可审计、可追溯。

应制定版本升级失败的应急预案，在升级失败的情况下启动应急预案进行回滚，在规定时间内恢复节点的可用性。

16.5 漏洞修复

应对节点的服务器进行定期漏洞扫描检查包括但不限于服务器本身的漏洞、分布式账本软件的漏洞、智能合约的漏洞，并对发现的安全漏洞和隐患提出修复方案进行审批，审批通过后进行修复，无法由运维修补的漏洞须评估可能的影响并上报。

进行漏洞修复，应不影响节点的账本数据、密钥等关键业务数据的历史数据。修复前需要在测试环境进行验证。如果漏洞修复影响到账本数据，则应通过共识协议进行数据的修正。

应记录漏洞修复的审批记录、操作历史等信息，做到可审计、可追溯。

16.6 备份与恢复

账本数据应根据业务需要进行实时备份。密钥等关键数据应定期备份，防止因设备损坏等原因造成数据或密钥丢失。

应保证备份内容安全可靠，并制定数据、密钥等内容的恢复策略，定期进行恢复演练。

16.7 应急预案管理

应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。

应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

重要事件的应急预案包括但不限于节点因故障而停止服务、节点账本数据损坏、节点版本升级失败。

16.8 权限管理

使用分布式账本的接口应做好权限管理，防止未授权的调用。

应对账本数据做好权限管理，敏感信息（如资产信息）应经授权查看或者使用。

除非特殊情况下，不应删除本地的账本信息。

每一次权限操作应写入日志，尤其是账本敏感信息的查看和使用，用于复查和审计。

16.9 议案机制

议案从提出到生效应保证透明公开公正，生效过程中对业务的平滑过渡，除非发生重大安全事故，避免采用所有节点同时停止服务进行升级的方式。

注：因分布式账本通常应用于多组织之间的协同运作，核心组织应满足以上运维要求，其余组织可视情况将分布式账本托管于核心组织。

17 治理机制

17.1 基本要求

金融分布式账本系统的治理机制原则上遵循 GB/T 22239—2019 中三级以上的安全管理制度、安全管理机构和人员安全管理相关要求。在此基础上，宜结合金融分布式账本特点，采用以下治理结构对相关管控重点进行安全治理。

17.2 治理结构

17.2.1 组织架构

管理委员会作为金融分布式账本系统安全治理的决策层，由主任委员、副主任委员和委员组成，可以由监管机构或由占领导地位的单一机构创建，也可以由多个机构或用户联合组建。

管理委员会下设安全管理机构作为安全治理的管理层，负责日常安全管理工作的统筹和异常情况的应急处置统筹。

安全管理机构下设日常管理团队和应急管理团队作为安全治理的执行层，负责日常管理和应急管理的具体执行。

治理的组织架构见图 2。

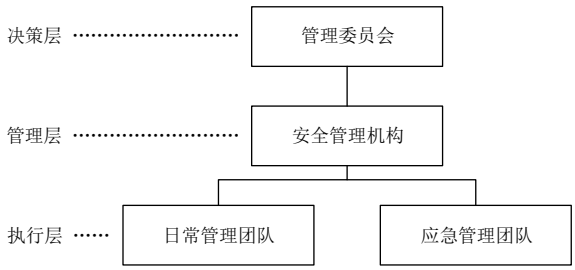

图 2 治理的组织架构

17.2.2 管理职责

管理委员会负责审核和批准金融分布式账本系统的风险偏好、安全管理策略以及其他关键事项。

安全管理机构负责统筹金融分布式账本安全管理，组织协调相关成员落实各项管理职责。

定期组织开展相关风险事件梳理、归纳与风险评估工作，并按事件的风险等级制定相应的紧急应对策略。

日常管理团队负责如节点管理等日常安全管理工作，除包含传统安全管理人员如系统管理员、网络管理员、安全管理员等，还应包含金融业务风险管理人员以及分布式账本安全管理员。

应急管理团队负责在紧急事件发生时，应确保能进行必要的应急处置，并联系相应的人员进行处理，包括系统管理员、网络管理员、安全管理员及系统研发员。

当金融分布式账本采用第三方云部署方式时，应增加对云部署方运行资质和安全能力的评估准入规则，并定期进行监管。

17.3 管控重点

17.3.1 节点管理

17.3.1.1 节点加入

金融分布式账本系统的新节点加入实施准入控制并经过相应的流程审核，包括对节点真实身份核查、对其他节点运行和记账的影响分析以及节点协议签署。

17.3.1.2 节点退出

金融分布式账本系统的节点退出应经过管理委员会审议，可采用“自愿退出”、“投票剔除”等退出方式，节点退出后剩余节点数量应不低于最低安全节点数量要求。

17.3.1.3 节点最低数量

应根据共识协议要求，设置最低安全数量的共识节点，制定“共识节点数量低于预警阈值”的应急预案。

17.3.1.4 节点登记与验证

应对接入的节点进行信息登记和验证，记录节点基本软硬件信息及与机构的对应关系。

17.3.1.5 节点管理操作

应对节点管理操作进行权限控制和身份验证，记录所有节点管理的操作历史，做到可审计、可追溯。

17.3.1.6 节点实现

应保证节点的实现具有一定的异构性，包括“部署异构”、“硬件异构”和“软件异构”。宜采用三种或三种以上的节点实现版本。应遵循第 6 章“基础硬件”中物理安全和第 7 章“基础软件”中操作系统的相关要求。

17.3.1.7 共识节点管理

根据不同的实现，金融分布式账本系统的共识节点采用不同的管理策略。针对不允许动态调整共识节点的分布式账本，在系统初始化时，应结合共识节点拥有者身份等其他基础设施组件，确保节点参数设置正确，保证系统安全运行；针对可动态调整共识节点的分布式账本，应加强添加或删除共识节点的权限管理，确保由可信节点来执行共识节点的添加或删除操作，必要时可对共识节点进行分层分级管理。

17.3.2 干预机制

17.3.2.1 用户干预

可通过设置相应的管理账户，允许第三方管理员向金融分布式账本系统发布操作指令，获得相关账户信息和账户内容，并调用指定账户对应的智能合约，对用户进行特殊干预，限制单个用户操作分布式账本系统；干预操作类型可以是冻结、解冻、暂停、恢复、结束、开启和强制转移等。

17.3.2.2 节点干预

可通过设置相应的管理账户，允许第三方管理员对节点进行特殊干预，包括节点临时终止或应急强制终止，限制单个节点接入分布式账本系统或者限制其参与共识与记账；干预操作类型可以是冻结、解冻、暂停、恢复、结束、开启和强制转移等。

17.3.2.3 系统干预

在遭遇特殊突发事件时，可对金融分布式账本实施系统干预，如大规模节点关断或系统关断；系统干预应经过管理委员会审议，并明确系统干预后的恢复策略、恢复方案和具体措施等。

17.3.2.4 干预功能管理

具备干预功能的管理账户应同样处于金融分布式账本系统中；应对干预功能进行权限控制和身份验证，保证只有特定权限的用户，在身份验证通过的前提下才能进行干预操作；应将干预权限分散给多个指定用户，避免因设定少数特定权限用户而导致的集中度风险，并防范分散式病毒攻击的风险。

17.3.2.5 干预行为记录

所有的干预行为应存储在系统中并与所有节点进行共识；应记录干预行为的操作历史，确保操作历史不可更改并且可以被查询，做到可审计、可追溯。

参 考 文 献

[1] GB/T 5271.18—2008 信息技术 词汇 第18部分：分布式数据处理

[2] GB/T 25069—2010 信息安全技术 术语

[3] GM/Z 0001—2013 密码术语

[4] ISO/IEC 9804:1998 Information technology — Open systems interconnection — Service definition for the commitment, concurrency and recovery service element

[5] ISO/IEC 16350:2015 Information technology — Systems and software engineering — Application management

[6] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary