ICS 35.020
A 30

DB4403

深　圳　市　地　方　标　准

DB 4403/T XXXXX—2020

金融行业区块链平台技术规范

Specifications of financial blockchain platform

点击此处添加与国际标准一致性程度的标识

（送审稿）

2020 年 8 月 21 日

2020－XX－XX 发布　　2020－XX－XX 实施

深圳市市场监督管理局　　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。

本文件由深圳市地方金融监督管理局提出并归口。

本文件起草单位：深圳证券交易所、深圳前海微众银行股份有限公司、深圳证券通信有限公司、深圳市互联网金融协会、深圳市标准技术研究院、深圳前海联易融金融服务有限公司。

本文件主要起草人：喻华丽、曾海泉、姚辉亚、李斌、范宏婷、宿旭升、李凯、李绅、张敖、黄华、钟松然、计胜侠、徐磊、范瑞彬、张开翔、苏小康、卢丽珊、李志能、萧建昌、宋江义、李如先、罗振伟。

引　言

在分布式商业需求逐渐扩大的背景下，分布式技术以其较好的弹性、较高的经济效用、对等网络和容错机制渐渐被应用普及，区块链技术就是其中的典型代表。这是一种由分布式架构、分布式存储、块链式数据结构、点对点网络、共识算法、隐私保护算法、智能合约等多种信息技术共同组成的整体解决方案，可带来信息技术的全新变革。

在实际应用中，“区块链”和“分布式账本技术”这两个概念经常被互相替代使用。严格意义上，区块链技术是一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理可信数据的产生、存取和使用等的模式。其块链式数据结构的基本特征是将一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间顺序连接成链条的一种数据结构，该“链”在区块链网络参与节点间复制和共享，同时链上内容依据不同的共识机制由参与节点组成的网络集体维护。而分布式账本技术的概念更为广泛，强调的是事务处理通过复制和共享的账本来实现，参与者可以在多个站点、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资产数据库，分布式账本技术并不指定具体的数据结构特征，某种程度上也可以将区块链看作是分布式账本技术的一种。尤其是在不同的利益、关注点和需求的驱使下，两者的应用实践逐渐体现了一种相互融合的趋势，主要代表了符合两者共同点的技术统称。因此，在描述具体的系统时，本文件将简化采用“区块链”一词代表“区块链和分布式账本技术”。

金融行业应用场景中，金融机构注重多层次的对等合作，且业务往往涉及大量的资金流动，有强监管、严合规、高安全的行业特殊要求，无论是仅由单个实体控制的私有链，抑或是任意节点均可接入的公有链，都难以满足金融行业的特性。因此金融业界往往将通用的分布式技术与金融信息技术中的身份认证、权限管理、隐私保护、反洗钱反欺诈支持、监管审计支持等模块相结合，并通过组建联盟的形式探索联盟链的技术路线。由于金融行业各机构发展区块链技术的进程、深度、路线等千差万别，区块链平台技术规范的标准化有助于统一认识，规范和指导各机构对区块链技术的应用。

金融行业区块链平台技术规范

1 范围

本文件规定了金融行业区块链平台的基本原则、分层框架、功能组件及其技术要求。

本文件适用于深圳市企业建设金融区块链和分布式账本系统、开展金融区块链和分布式账本服务。本文件所使用的体系化方法，重点关注金融区块链服务的功能架构和技术规范，并不适用于直接构建金融区块链服务的具体解决方案、技术实现与部署等。

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 32915-2016 信息安全技术 二元序列随机性检测方法

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

区块链 blockchain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

3.2

块链式数据结构 chained-block data structure

一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间顺序连接成链条的一种数据结构。

3.3

共识算法 consensus algorithm

区块链系统中各分布的节点对事务或状态的验证、记录、修改等行为达成一致确认的方法。

3.4

智能合约 smart contract

以数字形式定义的能够自动执行条款的合约。

3.5

公有链 public blockchain

任意节点均可接入，所有接入节点均可参与共识和读写数据的一类金融区块链部署模型。

3.6

联盟链 consortium blockchain

由一组利益相关的参与者使用，仅有授权节点可接入，接入节点可按规则参与共识和读写数据的一类金融区块链部署模型。

注：一般而言，金融行业注重多方合作，涉及大量的信息与资金流动，又因金融行业的强监管及高等级安全要求，金融业内往往是通过组建联盟（如：金链盟）以探索联盟链的技术路线。

3.7

私有链 private blockchain

仅由单个实体使用，仅有授权的该使用方节点可接入，接入节点可按规则参与共识和读写数据的一类金融区块链部署模型。

3.8

跨链技术 cross chain technology

实现不同区块链之间进行信息交互的技术。

4 缩略语

下列缩略语适用于本文件。

API	应用程序接口	（Application Programming Interface）
BaaS	区块链即服务	（Blockchain as a Service）
CA	认证授权	（Certification Authority）
DLT	分布式账本技术	（Distributed Ledger Technology）
ECC	椭圆曲线加密	（Elliptic Curve Cryptography）
KYC	了解你的客户	（Know Your Customer）
PBFT	实用拜占庭容错共识机制	（Practical Byzantine Fault Tolerance）
POS	权益证明共识机制	（Proof of Stake）
POW	工作量证明共识机制	（Proof of Work）

5 基本原则

5.1 合法合规原则

应遵守国家相关法律法规和金融监管要求，应为监管审计需求提供技术支持。

5.2 可追溯原则

业务与活动都应有记录，可追溯，可审计。

5.3 数据一致性原则

链上、链下存取的数据应保证数据库的一致性，区块链各个节点之间的数据也应保持一致性。

5.4 安全原则

应采取各种必要的安全手段，保障链上资产和交易等信息的安全，防范攻击。

5.5 隐私保护原则

应保障链上的用户隐私安全，防止泄露用户隐私。

5.6 业务导向原则

以需求推动技术，设计与开发时应优先考虑适用的业务场景。

6 分层框架

金融行业区块链平台的分层框架如图 1 所示，包括 5 层：用户层、接入层、核心层、基础层，以及一个跨越各层的跨层功能集合。各层由特定类型的功能组件构成，相邻层次的组件之间通过接口进行交互。

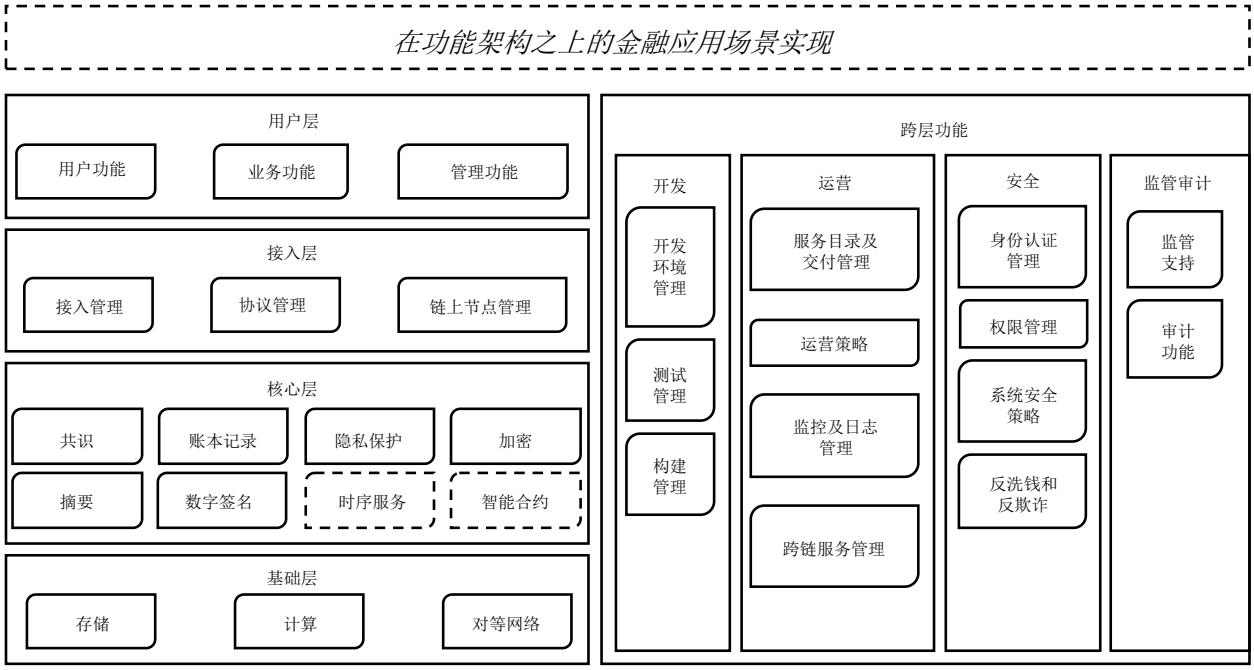

图1 金融行业区块链平台分层框架

a) 用户层：是面向用户的入口。金融区块链服务的使用方通过该入口和服务进行交互，执行相关管理功能，使用和维护金融区块链服务。用户层也可将服务输出到其他层，提供跨层服务支持。

b) 接入层：为用户层或终端应用提供高效、可靠、通用的访问，包括：通过封装核心层功能组件，使用高效缓存、负载均衡等技术，提供高效、可靠的接入管理、节点管理和智能合约管理等服务；支持标准通用的接入协议，为用户在多样化业务场景下提供通用的协议管理。

c) 核心层：是金融区块链系统的核心功能层。包括：节点间的共识机制，以及在此共识机制之上的数据与账本记录；隐私保护、加密、摘要与数字签名等模块，保证系统的安全合规与防篡改；此外，根据应用场景的不同，可以有选择地添加能自动执行预设逻辑的智能合约，以及统一全金融区块链系统时间的服务功能。

d) 基础层：该层可视作全系统的基础支撑，提供金融区块链系统正常运行所需要的运行环境和基础组件，如数据存储、运行容器、通信网络等。

e) 跨层功能：提供跨越多个功能层次能力的功能组件。

7 用户层

7.1 组成

用户层应包括：用户功能、业务功能、管理功能。

7.2 用户功能

用户功能组件支持金融区块链服务的使用方访问和使用金融区块链服务，在大部分的使用场景下，提供基础资源的管理，链的创建、维护、管理，链上智能合约的部署、使用等功能。

用户功能组件应具备以下功能：

a) 用户交互界面：可以是命令行界面或图形用户接口以及应用程序接口等形式；
b) 事务：将金融区块链服务的使用方的特定事务请求（查询、更新）提交到金融区块链网络的功能；
c) 事件：帮助金融区块链服务的使用方在金融区块链网络上监听并采取行动的一组应用事件。

7.3 业务功能

业务功能组件支持金融区块链服务的使用方的活动，宜提供服务选择和订购，使用账务和财务管理功能。

7.4 管理功能

管理功能组件支持金融区块链服务的使用方的活动,应实现成员管理服务、对服务活动的监控管理、事件处理和问题报告、安全管理服务等。

8 接入层

8.1 组成

接入层功能应包括：接入管理、协议管理、链上节点管理。

8.2 接入管理

接入管理功能组件提供跨进程调用功能，为终端应用及用户层提供核心层接入服务。

接入功能管理组件提供的接口应至少包括以下功能：金融区块链服务使用方账户信息中的基本信息、金融区块链区块、事务详情等账本信息的查询服务，金融区块链服务使用方特定事务操作请求提交到金融区块链网络的服务。

接入管理功能组件宜具备：

——接口服务能力管理，如支持接口调用频度设置和事务操作及账本查询缓存设置；
——接口访问权限管理，如针对不同的用户配置不同的访问权限；
——接口的通讯安全，如对通讯报文进行加密。

8.3 协议管理

协议是连入网络的设备都要遵循的一定的技术规范,应包含关于硬件、软件、端口等的技术规范。

8.4 链上节点管理

节点是区块链的载体，由安装了特定区块链软件、可连接互联网、具有可访问的 IP 地址、且能对外提供服务的物理服务器或虚拟服务器组成。

链上节点管理功能组件应：

——支持对金融区块链节点的信息查询和管理控制，至少包括：

- 节点服务器的状态信息查询；
- 节点服务启动关闭控制；
- 节点服务能力配置；
- 节点网络状态监控；
- 节点授权配置管理。

——具备节点身份管理功能：

- 金融行业区块链平台应明确节点授权机构及管理员；
- 节点加入区块链网络之前，应由授权机构给予唯一的身份标识，并提供与之对应的身份鉴别信息和身份凭证，授权机构应在凭证中指定节点角色；
- 身份凭证由授权机构确保其完整性和真实性，应符合密码算法对完整性和真实性的要求；
- 身份鉴别信息应具有不易仿冒的特性，并设定更换期限，在期限到来之前进行更换；
- 在传递及存储身份鉴别信息之前，应采用符合密码算法要求的机密性及完整性保护；
- 节点之间建立数据通信连接之间，应先通过身份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，该过程应符合密码算法要求对机密性和完整性的要求；
- 应具有节点身份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。

9 核心层

9.1 组成

核心层应包括：共识机制、账本记录、隐私保护、加密、摘要、数字签名。宜包括：时序服务、智能合约。

9.2 共识机制

根据不同的业务需求，可选择适用的共识算法来实现共识机制。常见的共识算法类型有 POW、POS、PBFT 等。

共识机制功能组件应具备以下功能：

——支持多个节点参与共识和确认；

——支持独立节点对区块链网络提交的相关信息进行有效性验证；

——防止任何独立的共识节点未经其他共识节点确认而在区块链系统中进行信息记录或修改；

——应具备一定的容错性，包括节点物理或网络故障的非恶意错误、节点遭受非法控制的恶意错误，以及节点产生不确定行为的不可控错误，任意不超过理论值的节点数故障，整个系统正常工作；

——在遭受恶意攻击数据被污染时，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的发生；

——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，或通过与系统中其他可信节点的交互等干预方法，保证节点数据恢复正常状态，受攻击前的数据不会丢失，并保持和正常节点间数据的一致性；

——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。

9.3 账本记录

账本泛指区块链中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成区块链系统中数据的公共管理、不可篡改、可信任的机制。

账本记录功能组件应具备以下功能：

——支持持久化存储账本记录；

——支持多节点拥有完整的数据记录；

——支持向获得授权者提供真实的数据记录；

——确保有相同账本记录的各节点的数据一致性；

——任何一条记录被人为修改后都可以通过历史区块回溯快速检验出来；

——应保证账本数据在生成、传输、存储、调用等操作不可被非授权方式更改或破坏；

——应保证账本数据在所有节点中具有冗余性，防止因单个节点失效而造成总账本数据的丢失。

9.4 隐私保护

隐私保护目的是保护区块链应用中用户身份和事务处理等敏感信息不被泄露或非法获取，这些信息只有通过充分授权才能被访问。金融区块链隐私保护功能通常通过数据加密和访问控制手段来实现，隐私保护功能组件宜支持但不限于以下四类隐私保护策略：

——由认证机构代理用户在金融区块链上进行交易，用户资料和个人行为不进入区块链网络；

——不采用全网广播方式，而是将数据的传输限制在正在相关的授权节点之间；

——对用户数据的访问采用权限控制，持有密钥的访问者才能解密和访问数据；

——采用例如零知识证明、环签名和同态加密等隐私保护算法，规避隐私暴露。

隐私保护功能组件应满足以下要求：

——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和处理方式、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，加密的秘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销毁手段，并向其他节点或组织发布停止运营和处置数据的信息；

——秘钥发送客户后应明确告知其妥善保管秘钥，并提供秘钥更换手段；

——信息存储时应对客户信息进行全量加密；

——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；

——信息对外部扩散时，应告知客户并获得授权，并提供给客户随时中断扩散传递的手段；

——应对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，并给客户提供解密手段；

——应对客户提供信息的删除销毁的手段；

——信息删除销毁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。

9.5 加密

加密功能组件应支持加密和解密两个操作，加密功能组件应满足以下要求：

——所使用的密码算法应符合国家密码管理部门的要求，具体包括：

- 机密性，机密性指信息不被泄露给非授权的用户、进程等实体的一种性质。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；
- 完整性，即数据没有受到未授权的更改，金融行业区块链平台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；
- 真实性，使用对称加密、动态口令、数字签名等实现真实性；
- 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实现实体行为的不可否认性，金融行业区块链平台中所需要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、配置等操作；
- 算法执行过程中需要使用随机数时，应按照国家密码管理主管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。

——密钥管理应符合密码行业标准 GM/T 0054-2018 的要求

- 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；
- 除公钥外，所有密钥不能以明文形式存储或传输。

——对于高安全等级的金融行业区块链平台，还应使用硬件加密设备完成密码运算和密钥存储

- 使用的加密机设备应符合国家密码局颁布的 GM/T 0045-2016 金融数据密码机技术规范；
- 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。

9.6 摘要

摘要功能组件又称数字摘要功能组件，指将任意长度的消息输入变成固定长度的短消息输出，一般通过摘要函数（或称 Hash 函数）来实现，摘要功能的输出值被称为摘要值或者 Hash 值。

摘要功能组件应具备以下功能：

——对数据的完整性提供保护；

——对于给定的数据明文和摘要值可验证该数据明文是否被篡改。

9.7 数字签名

数字签名功能组件被用以确认数据单元的完整性以及不可伪造性，是非对称加密技术与数字摘要技术的结合，一般包括数字签名和签名验签两个具体操作。数字签名操作指对签名内容的摘要用私钥加密生成数字签名值；签名验签操作指用公钥解密签名值并与摘要值进行比对。一般可根据签名功能依托的非对称加密算法的不同进行分类，典型的算法包括 RSA、ECC 和我国商密算法 SM2。

数字签名功能组件应支持对相关信息进行数字签名和签名验证，确保信息的机密性、完整性及不可伪造性。宜支持集成权威公正的第三方 CA 机构签发的数字证书。

对于签名的私钥需要有安全的保管机制，如客户使用硬件等方式自行保管或通过中立可靠的第三方来托管。

9.8 时序服务

对于金融区块链系统中的行为或数据需记录一致性的时序，可以选择特定的时序机制或工具。金融区块链系统可有选择性地提供时序服务功能。

时序服务功能组件应支持账本记录统一时序、具备时序容错性。宜具备支持集成可信第三方时序服务（如国家授时中心的可信时间戳服务）功能。

9.9 智能合约

智能合约是一套以计算机代码形式定义的承诺，以及合约参与方可执行承诺的协议，即：用计算机代码形式编写合约参与方达成的条件型协议，当条件被触发时区块链系统自动执行该协议。根据应用场景的不同需求，金融区块链系统可有选择性地提供智能合约功能。

智能合约功能组件应满足以下要求：

——提供编程语言支持及配套开发环境，支持合约内容静态和动态检查，支持运行载体如虚拟机，支持向账本中写入合约内容，防止对合约内容进行篡改，支持多方共识下的合约内容升级等；

——对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应仅限于智能合约范围内，不应影响系统的整体运行；

——具有完善的版本控制。应在源代码中通过区块链平台指定方式定义版本号，应在配置文件中定义版本号，该配置文件需要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，应在区块链中保留前一版本，交易信息中应明确调用的智能合约版本；

——有相应的机制控制用户对智能合约的访问，在支持智能合约之间相互访问条件下，限制恶意智能合约的感染，应控制智能合约对外部环境的访问；

——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；

——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。

10 基础层

10.1 组成

基础层如：存储、计算、对等网络。

10.2 存储

存储功能组件提供区块链运行过程中产生的各种类型数据（如账本、交易信息等）的写入及查询功能，相关选型包括但不限于关系型数据库、键值对数据库、文件数据库等。

存储功能组件应满足以下要求：

——点对点网络中，能够被每个节点部署并使用；

——能够高效、安全、稳定地提供数据写入及查询服务；

——对于采取分库分表的数据存储方案，存储组件还应包括数据的分片及路由处理能力；

——账本数据应根据数据对象的类别分门别类（如账户数据、区块数据、交易数据、配置数据以及账本元数据），并分别存储、分别管理、分别操作；

——对于敏感信息（如资产数据）应当加密存储，使用时候利用安全多方计算技术读取；

——对于金融行业区块链平台，应当有数据访问等权限的控制和管理。同时节点 CA 证书的存储也应当私密管理，防止泄露。

10.3 计算

计算功能组件提供区块链系统运行中的计算能力支持，包括但不限于容器技术、虚拟机技术、云计算技术等。

计算功能组件一般应：

——对区块链系统提供运行环境支持；

——点对点网络中，能够被每个节点采用。

10.4 对等网络

区块链系统运行的底层拓扑结构是分布式对等网络，采用对等网络协议组织区块链中的各个网络节点。各个节点间通常使用点对点通信协议完成信息交换以支撑上层功能。

网络传输功能组件通常应：

——能够进行点对点之间的高效安全通信；

——能够提供点对点通信基础上的多播能力；

——支持对节点的动态添加、减少的识别。

11 跨层功能

11.1 组成

跨层功能包括：开发功能、运营功能、安全功能、监管审计功能。

11.2 开发功能

开发功能组件宜包括：开发环境管理、构建管理、测试管理。

a) 开发环境管理组件宜：
   - 支持开发服务相关的配置元数据的生成；
   - 支持服务配置脚本和组件的编写或生成。

b) 构建管理组件宜：
   - 支持自动化构建软件包功能；
   - 提供自动化编译功能及出错信息提示；
   - 实现构建过程的审核流程；
   - 多语言支持；
   - 多平台支持。

c) 测试管理组件宜：
   - 支持测试计划、方案、报告、用例等内容的管理；
   - 支持自动生成测试报告；
   - 测试环境与生产环境集成的情况下进行测试不应影响生产环境；
   - 测试过程自动化；提供测试用例库、测试数据库管理功能。

11.3 运营功能

运营功能组件宜包括：服务目录及交付管理、运营策略、监控及日志管理、跨链服务管理。

a) 服务目录及交付管理组件宜包括所有部署、提供和运行金融区块链服务有关的技术信息，及相应的工作流信息。

b) 运营策略组件宜包括业务、技术、安全、隐私和认证等策略。

c) 监控及日志管理组件宜具备：
   - 监控区块链网络中节点进程的运行状态、网络通信状态、共识达成效率的能力；
   - 针对区块链节点在运行过程中所产生日志的存储、分析的能力；

- 节点运行报告。

d) 跨链服务管理组件宜连接相关 FBSP 的运营系统、业务系统与管理系统。

11.4 安全功能

安全功能组件应至少包括：身份认证管理、权限管理、系统安全策略、反洗钱与反欺诈、其他金融安全功能体系。

安全功能组件宜考虑多种层次的安全威胁，包括但不限于身份管理类安全威胁、业务与应用类安全威胁、网络与信息安全威胁、终端类安全威胁、基础类安全威胁、管理类安全威胁等。

安全功能组件：

——应支持通过各种有效的身份认证材料进行用户身份认证，支持多种认证方式的组合使用，提供对用户在第三方权威认证机构认证过的证书进行备案、签名、验签的功能；

——应支持设置授权和安全规则授权用户访问和使用资源权限的功能;提供节点间通信加密和节点数据加密存储、节点主机安全加固、智能合约安全验证等安全策略；

——应支持反洗钱与反欺诈功能，具备客户身份识别、可疑交易识别与报告功能，支持对接风险控制系统；

——宜提供信息资产安全、人员安全、物理与环境安全、运维安全、办公安全、系统开发与维护安全、业务连续性安全、合规安全等方面的管理组件。

11.5 监管审计功能

监管和审计功能组件的目标是使金融区块链服务符合可监管与可审计的特性,避免金融区块链网络游离于法律法规以及行业规则之外，成为洗钱、非法融资或犯罪交易的载体。

监管和审计功能组件应至少包括：监管支持、审计功能。

a) 监管支持组件应：

- 支持通过事前准入控制、事中权限控制、事后追溯等技术手段实现监管目标，保证记录不可篡改、可追溯与可稽核；
- 设置明确的监管治理规则；
- 保存与服务、资源、性能相关的数据和证据；
- 允许监管机构加入金融区块链网络作为其中一个节点进行即时监管。

d) 审计功能组件应保存与审计活动相关的数据和证据。宜具备：

- 审计方加入区块链网络作为其中一个节点进行实时审计,或允许审计方作为金融区块链网络之外的第三方机构，按需或定时获得区块链网络中的数据与证据；
- 允许实时核查审计被审计对象的全部记录并作为审计证据；
- 实现金融区块链网络与其他相关系统的对接与数据提取。

附 录 A
（资料性附录）
常见的共识机制类别与适用性参考

表A.1 常见的共识机制类别和比较

比较内容	工作量证明共识机制（POW）	基于相关权益的共识机制（POS）	传统分布式系统的一致性算法	基于拜占庭容错模型（BFT）的共识机制
基本机制	通过特定计算运算获取特定规则匹配值来取得记账权，对系统事务消息进行记录。	节点通过特定的权益分配获得成为记账节点的不同概率，一般情况下两者成正比，但也会通过特定的规则获取记账权。	通过选举领导者进行共识事务的组织发起，其余参与者跟随验证或确认的方式。常见的算法有 PAXOS、RAFT 等。	采用领导者选举机制，在领导者和共识参与者之间通过多轮交互达成共识，以达成拜占庭容错（恶意错误和不可控错误），常见的算法有 PBFT。
特点	1、网络节点都可参与，具备最广泛的参与性； 2、一般情况下，与其他共识算法相比计算资源消耗相对较高，性能速度较低； 3、有超过 51%恶意节点攻击的风险，特定情况下会产生数据分叉。	1、相比 POW，一定程度减少了计算的资源消耗，仍有一定程度的获取记账权的计算消耗； 2、在特定权益分配机制下，容易形成记账权的公平性问题，产生中心化控制风险。	1、实现共识的过程类似现实社会中的选举，领导者（节点）需要获得大多数选民（节点）的投票，一旦选定后就跟随其操作，领导者有任期或期限，期限结束后将重新选举领导节点。PAXOS 和 RAFT 的区别在于选举的具体过程不同，主要目的都是让每一个参与节点按少数服从多数的原则逐步达成一致意见； 2、此类算法没有追求取得记账权的计算消耗，整体性能较高。	1、具备更好的容错机制，可以覆盖严格的错误类型（非恶意、恶意、不可控错误）； 2、共识过程交互相对较多，记账人群体一般事先指定，在部分场景下有选择公平性问题。
容错性	容许全网 50%的节点容错（恶意、非恶意、不可控）。	根据不同的机制设计有所不同，但一般与 POW 类似。	选举过程可以容忍 N/2-1 个节点出错，大多不考虑拜占庭容错，即假设所有节点只发生宕机、非人为问题，并不考虑恶意节点篡改数据的问题，但亦有改进后实现拜占庭容错的 Byzantine Paxos。	一般可以容忍 1/3 的拜占庭错误节点，在特定的假设条件下，容错范围可以进一步扩大。
适用性	一般适用于对公平性、开放性要求高的场景，如公有链。 不适用于对性能以及即时一致性要求高的场景。	适用于对开放性较高，具备特定权益机制的场景。	适用于成员或节点可控程度较高的私有链及部分联盟链场景。	适用于大部分联盟链场景与特定的公有链场景，可以保证不产生分叉，保持数据的一致性。
注：表中适用性内容仅为一般性参考，可结合具体业务需求选择不同共识机制				

参 考 文 献

[1] GB/T 11457—2006 信息技术 软件工程术语

[2] GB/T 25069—2010 信息安全技术 术语

[3] GB/T 32399—2015 信息技术 云计算 参考架构

[4] JR/T 0184—2020 金融分布式账本技术安全规范

[5] CBD-Forum-001-2017 区块链参考架构

[6] ISACA COBIT 5: A Business Framework for the Governance and Management of Enterprise IT

[7] ISO/IEC 9804:1998 信息技术 开放系统互连、托付、并发和恢复服务元素的服务定义（Information technology - Open systems interconnection - Service definition for the commitment, concurrency and recovery service element）