可 信 区 块 链 推 进 计 划

可信区块链： 区块链服务
技术参考框架

（征求意见稿）

2019- 05 -07 发布

目　　录

前　言

本部分按照GB/T 1.1-2009给出的规则起草。

本部分属于可信区块链系列标准的技术部分。本部分制定了区块链服务（BaaS，Blockchain as a Service）的技术参考框架和系统基本要求。

本部分由可信区块链推及计划提出并归口。

本部分起草单位：中国信息通信研究院、腾讯云计算（北京）有限责任公司、上海点融信息科技有限责任公司、华为技术有限公司、阿里云计算有限公司、北京金山云网络技术有限公司、智链数据科技（南通）有限公司、西安纸贵互联网科技有限公司、中兴通讯股份有限公司、联动优势科技有限公司、中链科技有限公司、全链通有限公司、普华商业集团有限公司、北京思宇智术科技有限公司、广联达科技股份有限公司、上海淳麒金融信息服务有限公司、北京百度网讯科技有限公司、杭州趣链科技有限公司。

本部分主要起草人：何宝宏、魏凯、杨白雪、敖萌、李佳、邵兵、肖诗源、张煜、刘再耀、董振华、余珊、朱江、王东、金怡爱、张戈、陈昌、易晓春、王凌、张一杰、刘尧、王利凯、姜晖、谢逸俊等。

1 范围

本部分是“可信区块链”系列标准的组成部分，规定了区块链服务相关的术语和定义、技术参考框架、功能要求、性能要求和信息安全要求等。本部分明确了区块链服务的相关定义、基本功能要求和基本性能要求。

因区块链技术正在快速发展，本部分主要参考国内外主流区块链进行了起草编制。

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，仅所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。

可信区块链：第1部分 区块链技术参考框架

可信区块链：第3部分 评测方法

YDB144-2014 云计算服务协议参考框架

3 术语和定义

下列术语和定义适用于本文件。

3.1 区块链服务平台（ BaaS（Blockchain as a Service）平台）

区块链服务平台是一种帮助平台用户创建、管理和维护区块链网络及应用的信息系统。通常区块链服务是指提供企业级区块链网络及应用的服务。区块链服务具有快速部署、方便易用、高安全可靠等特性，区块链服务通过把计算资源、通讯资源、存储资源，以及区块链记账能力、区块链应用开发能力、区块链配套设施能力等转化为图形化用户界面（GUI）和应用编程接口（API），让应用开发过程和应用部署过程简单而高效。

区块链服务平台可以分为区块链网络服务平台和区块链应用服务平台两种。根据业务需要，区块链服务平台可以实现其中一种，也可以在同一个平台上实现两种功能。

3.2 区块链网络服务平台

区块链网络服务平台是指帮助平台用户创建、管理和维护区块链网络的信息系统。平台用户需要在区块链网络服务平台上进行二次开发，实现区块链应用。区块链网络服务平台通常提供的是PaaS（Platform as a Service）服务。

注：区块链网络服务平台可以基于云计算服务平台（IaaS， Infrastructure as a Service），也可以脱离云计算平台单独存在。但大多数的区块链网络服务平台是基于云计算服务平台的。

3.3 区块链应用服务平台

区块链应用服务平台是指帮助用户创建、管理和维护区块链应用的信息系统。平台用户可以直接使用平台提供的接口，使用区块链应用做业务。区块链应用服务平台通常提供的是SaaS（Software as a Service）服务。

3.4 区块链用户

见《可信区块链：第1部分 区块链技术参考框架》3.7. 用户

3.5 平台用户

平台用户是指区块链服务平台的用户，也称为区块链服务平台的租户。

注：对于提供区块链网络服务的平台，平台用户应是区块链节点的管理者。对于提供区块链应用服务的平台，平台用户是区块链的用户或者一批区块链的用户的代理接入服务提供商。

4 系统参考架构

4.1 技术参考模型

区块链服务平台的技术参考模型如图所示。

图 1 技术参考模型

4.2 用户体系模型

平台用户与区块链用户的关系如下图所示。

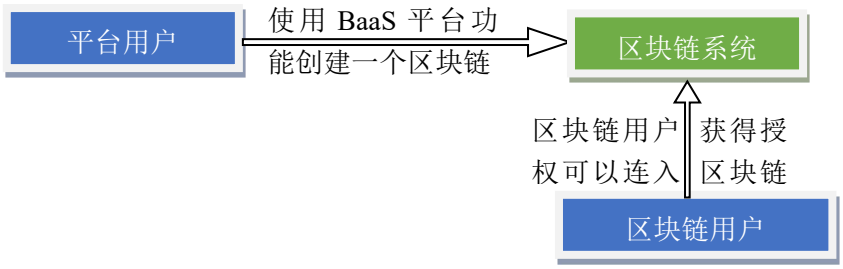

图 2 平台用户与区块链用户的关系

5 系统功能要求

5.1 基本区块链服务能力

基本区块链服务能力功能要求见下表。

表 1 区块链服务平台基本区块链服务能力功能列表

类型	应有功能	宜有功能	可有功能

区块链网络服务平台	自动化部署功能 节点管理功能 提交交易接口	提供 SDK 接入区块链功能 平台用户加入已有区块链功能 平台用户邀请平台其他用户加入已有区块链功能	平台用户发起区块链参数变更投票、接入区块链用户变更投票等功能
区块链应用服务平台	平台用户加入区块链功能 平台用户调用区块链应用接口	提供 SDK 接入区块链功能 平台用户创建新的区块链应用	

5.2 平台用户管理功能

区块链服务平台应有基本的平台用户管理功能，包括平台用户创建、平台用户登录、平台用户登出、平台用户身份信息维护等功能；宜有平台用户权限管理功能、平台用户的服务使用计费管理功能（包括平台用户账户充值、服务扣费、平台用户账户账单查询等功能）、平台用户通知功能（包括平台用户服务到期通知、区块链网络邀请加入通知等功能）。

平台用户可有平台子用户功能，不同的平台子用户对应不同的操作权限，方便区块链的管理和使用。

5.3 自动化部署功能

区块链服务平台应有自动化部署区块链网络的功能。

对于区块链网络服务平台，平台用户应能通过平台创建并启动一个全新的区块链网络，并将必要的软件部署到平台用户自己的节点上。对于可以进行节点角色配置的区块链底层平台，平台应能提供方便的配置管理功能。

对于区块链应用服务平台，平台管理员应能通过平台创建并启动一个全新的区块链网络，并将必要的软件自动化部署到所有的节点上。

5.4 节点管理功能

区块链服务平台应有基本的节点管理功能：对于平台上的每一个区块链网络，平台应能够列出所有区块链网络的节点基本信息，包括但不局限于：节点IP地址、节点管理者信息（应满足国家相关部门规定的区块链信息服务管理规定中对于节点管理者的信息备案要求）。

区块链服务平台宜能够查看节点是否在线。

对于不同的平台用户宜有不同权限的节点管理功能。

5.5 区块链伸缩功能

区块链网络服务平台应有区块链伸缩功能：包括但不局限于：节点角色分配调整（特指带有角色区别的区块链网络）、节点加入已有区块链网络、节点退出区块链网络；宜有对于节点的计算资源伸缩功能：包括但不局限于：节点计算资源配置、动态调整节点计算资源。

5.6 区块链配置管理功能

同《可信区块链：第3部分 评测方法》4.3.1 节点管理 的功能要求

5.7 区块链浏览器功能

区块链服务平台应提供一个区块链浏览器功能，区块链浏览器应能够直接看到区块高度（即该区块在整个区块链中的序号）、具体块内数据和区块哈希等。可以是一个独立访问区块链底层的客户端工具，或者一个独立访问区块链底层的服务，让用户通过web浏览器访问到区块链底层。

区块链浏览器宜提供交易查看功能，能够查看块内的具体交易数据，以及区块链用户的查看功能。

区块链浏览器宜提供数据可视化功能。

注：数据与信息含义不同。数据指存在区块链上的原始数据，不要求其具有直接可读性。

5.8 网络节点监控功能

区块链服务平台应能对平台自己能够控制的节点具有监控功能，监控这部分节点的具体运行情况，包括但不局限于节点计算资源配置查看、节点已消耗计算资源情况、节点网络情况查看、节点连接的客户端情况、节点处理的交易数情况，区块产生速度等。

网络节点监控宜提供数据可视化功能。

区块链服务平台可对所有节点进行上述监控。

5.9 日志功能

区块链服务平台应具有日志功能，记录所有平台相关操作以及所有通过平台接口对区块链底层的交易操作，以满足运维和审计等需要。

5.10 智能合约管理功能

当区块链网络服务平台使用具有智能合约的区块链系统作为区块链底层平台时，区块链网络服务平台应具有合约管理功能，包括合约查看、合约提交或合约部署功能。区块链网络服务平台宜提供合约升级、合约版本管理、合约审计等功能。

5.11 多底层引擎适配功能

区块链网络服务平台宜支持多种区块链底层平台，方便平台用户使用不同的区块链技术。对于不同的区块链底层平台，宜使用同类型的接口进行操作和调用。

5.12 区块链底层平台升级功能

区块链网络服务平台宜支持区块链底层平台的升级。当区块链网络服务平台支持的区块链底层平台出现新版本时，区块链网络服务平台应提供让平台用户继续使用旧版本区块链底层平台的功能；可提供相应工具，帮助平台用户从旧版本升级到新版本。

5.13 多模式部署功能

区块链服务平台宜提供多模式部署功能，包括跨云部署、混合云部署、私有化部署等。

5.14 自动运维功能

区块链服务平台宜具有自动运维功能，平台能够通过监控平台所属的计算资源环境，依据事先设定的运维策略，实现自动恢复宕机节点、自动识别故障节点、自动告警等自动运维的功能。

5.15 开发支持

当区块链网络服务平台使用具有智能合约的区块链系统作为区块链底层平台时，区块链网络服务平台宜具有友好的开发支持功能，平台用户可以使用平台提供的在线或离线的开发工具，进行智能合约的

开发、调试及测试。区块链网络服务平台可提供智能合约模板、智能合约基础库和常用功能组件模板，方便用户快速开发智能合约。

5.16 安全硬件支持

区块链服务平台可对常见的安全硬件给予支持，包括但不局限于服务器自带的可信计算环境、商用加密机、加密集群等。区块链服务平台为平台用户提供方便的操作功能或接口，帮助平台用户使用这些安全硬件。

5.17 证书管理功能

区块链服务平台可具有数字证书管理功能，支持为平台用户和区块链用户提供数字证书（如自签名数字证书或由符合国家相关规定的权威公正的第三方CA机构签发的数字证书），也支持平台用户和区块链用户提供自有数字证书，来进行数字签名和签名验证相关工作。

5.18 迁移支持

区块链服务平台可支持平台用户将自己所管理的区块链节点迁移至其他计算平台上。具有迁移支持的区块链服务平台应提供方便的迁移工具以及区块链网络服务的持续无中断，从而确保平台用户在迁移过程中的便利性和业务不中断。

5.19 网络连通性和域名支持

区块链服务平台可为区块链网络节点或服务提供网络IP地址和端口分配能力，以保证各区块链网络节点之间、以及区块链应用与区块链节点之间的网络连通性。区块链服务平台可为多模式部署的区块链网络提供易于接入和维护的网络连通方案，包括但不局限于公网直连、专线、VPN等。

区块链服务平台可为区块链节点或服务提供域名，以保证区块链应用访问区块链节点或服务的便利性和灵活性，降低维护成本和复杂度。

6 系统性能要求

6.1 基本业务性能

区块链服务平台提供的基本区块链技术服务应通过可信区块链功能测试，该测试宜通过区块链服务平台提供的接口调用。

6.2 自动化部署性能

本项性能要求包括以下指标：

a) 一个区块链服务平台创建并启动一个 4 节点区块链网络需要的时间范围；

b) 一个区块链服务平台创建并启动一个 64 节点区块链网络需要的时间范围。

6.3 多底层引擎适配性能

本项性能要求以支持的不同底层技术的类型数量为指标。同种底层技术使用不同的配置，或者使用不同的编程语言实现，视为同一种底层。

6.4 证书管理性能

本项性能要求包括以下指标：

a） 是否支持节点身份的证书认证方式；
b） 是否支持客户端的证书认证方式；
c） 是否支持国密系列数字证书，支持国密的需要详细列出国密系列算法在区块链中的使用情况。

7 平台安全要求

7.1 安全隔离

不同的区块链网络实例之间应具有数据隔离。不同的区块链网络实例之间宜提供IP隔离和IP互通的可选功能。隔离级别可分为物理隔离和逻辑隔离两个级别。

对于同一个区块链网络内属于不同平台用户的节点，宜提供在网络、计算、存储等资源层面的隔离性。

在提供安全隔离能力的同时，平台可提供跨链功能，以满足某些业务需求。

7.2 风控能力

区块链服务平台宜提供对关键操作的风险控制功能（如二次验证），以避免误操作对数据和业务带来的风险。

7.3 攻击防范

区块链服务平台宜为区块链网络的节点和服务提供攻击防范的能力，如抗DDoS（分布式拒绝服务）攻击的防范。

7.4 高可用性

区块链服务平台本身作为管理系统应保证自身系统模块有高可用保证，系统宜无单点风险。

7.5 平台自身安全

区块链服务平台应能确保平台自身的安全。