雄安新区区块链技术 数据协同规范

目　录

一、范围

1.区块链系统内部不同智能合约间调用（同链调用）的要求与建议。

2.不同区块链系统间访问（跨链访问）的要求与建议。

3.区块链系统与非区块链系统交互（链外协同）的要求与建议。

本文件适用于指导雄安新区政府投资类项目中的区块链系统（含区块链产品及智能合约）的设计、开发与运行，其他系统可根据实际情况选择性参考。

二、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 18030《信息技术 中文编码字符集》

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

GB/T 7408—2005《数据元和交换格式 信息交换 日期和时间表示法》

GB/T 25069—2010《信息安全技术 术语》

CBD-Forum-001—2017《区块链 参考架构》

JR/T 0184—2020《金融分布式账本技术安全规范》

W3C UDDIv2《数据结构规范》

W3C UDDIv2《API 结构规范》

IETF RFC 8259《The JavaScript Object Notation (JSON) Data Interchange Format》

IETF RFCs(7230-7237)《Hypertext Transfer Protocol-HTTP/1.1》

三、术语定义和缩略语

（一）术语定义

GB/T 5271.18—2008《信息技术 词汇 第 18 部分：分布式数据处理》、GB/T 25069—2010《信息安全技术 术语》、JR/T 0184—2020《金融分布式账本技术安全规范》及 CBD-Forum-001—2017《区块链 参考架构》中界定的以及下列术语和定义适用于本文件。

区块链：已确认区块基于密码学链接信息所形成的、仅允许追加的序列组成的分布式账本。

区块链技术：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。

区块链产品：实现了区块链技术的软件产品。

区块链节点：安装了区块链产品，维护区块链数据的设备。

区块链系统：由多个区块链节点组成的分布式系统。

智能合约：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，其在区块链系统上体现为可自动执行的计算机程序。

共识：区块链系统中各节点间达成一致制定的过程。

共识协议：区块链系统中各节点间为达成一致制定的规则和实现规则所采用的计算方法。

同链调用：在同一个区块链系统上的多个智能合约之间的相互调用。

跨链访问：数据从一个区块链系统传递到另一个区块链系统的过程。

链外协同：非区块链系统与区块链系统的相互交互，包含区块链系统访问非区块链系统获取数据，及非区块链系统对区块链系统的访问。

散列/杂凑函数：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：

（1）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。

（2）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。

数字签名：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受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（例如接受者）伪造或抵赖。

消息摘要：散列/杂凑算法的最终输出值。

联机访问：指由用户的需求所直接触发的区块链功能调用。

同步模式：区块链接收到调用请求后进行共识、执行合约，合约执行完毕后将执行的结果返回给请求方。

异步模式：区块链接收到调用请求后，在执行合约前即将请求的回执返回给请求方。待共识达成、合约执行完毕之后通过另外一次交互传递合约的执行结果。

批量处理：批量处理是指由系统自动触发、涉及较多处理步骤和数据的区块链功能调用。

访问控制：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。

RESTful：符合 REST（Resource Representational State Transfer 表述性状态转移）约束条件和原则的架构。

时间戳：使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。时间戳机构对此对象进行数字签名产生时间戳，以证明原始文件在签名之前已经存在。

时间戳机构：用来产生和管理时间戳的权威机构。

同构区块链：基于相同区块链产品构建的其他区块链网络

异构区块链：基于不同区块链产品构建的其他区块链网络。

回调机制：一种服务调用机制，当服务请求方请求服务时一并提供己方接口，服务提供方可在服务过程中主动调用此接口。

事务：事务是指是程序中一系列关系密切的逻辑操作，所有操作必须全部成功完成，否则每个操作导致的任何更改都应当被撤消。

原子性：事务的四个特性之一。事务的指令要么全部执行成功，要么全部不执行。只要其中一个指令执行失败，所有的指令

都执行失败，数据进行回滚，回到执行指令前的数据状态。

一致性：事务的四个特性之一。执行事务使数据从一个状态转换为另一个状态，但是对于整个数据的完整性保持稳定。

隔离性：事务的四个特性之一。当多个用户并发访问数据时，系统为每一个用户开启的事务不被其他事务的操作所干扰。

持久性：事务的四个特性之一。当事务正确完成后，事务对数据的改变是永久的。

联盟链/许可链：针对某个特定群体的成员和有限的第三方，由已知的确定成员共同参与管理、数据只允许商定范围成员进行读写和发送的区块链。

公有链：任何个人或组织均可以读取数据、发送交易、参与共识的开放的区块链。

（二）缩略语

简写	英文全称	中文解释
API	Application Programming Interface	应用编程接口
HTTP	Hyper Text Transfer Protocol	超文本传输协议
HTTPs	Hyper Text Transfer Protocol over Secure Socket Layer	基于安全套接层的超文本传输协议
ID	Identity	标识
TSA	Time Stamp Authority	时间戳机构

四、总体框架

区块链数据协同体系包括同链调用、跨链访问、链外协同等方面，这三种协同方式的示意图如图 1 所示。

图 1 区块链数据协同方式

区块链数据协同体系框架见图 2，本标准依照图 2，分别提出以下数据协同要求:

1.同链调用

区块链内部智能合约之间的协同规范。

2.跨链访问

两个区块链系统之间的协同规范。

3.链外协同

区块链对外界提供的服务，以及区块链从外界非区块链系统获取数据的访问规范。

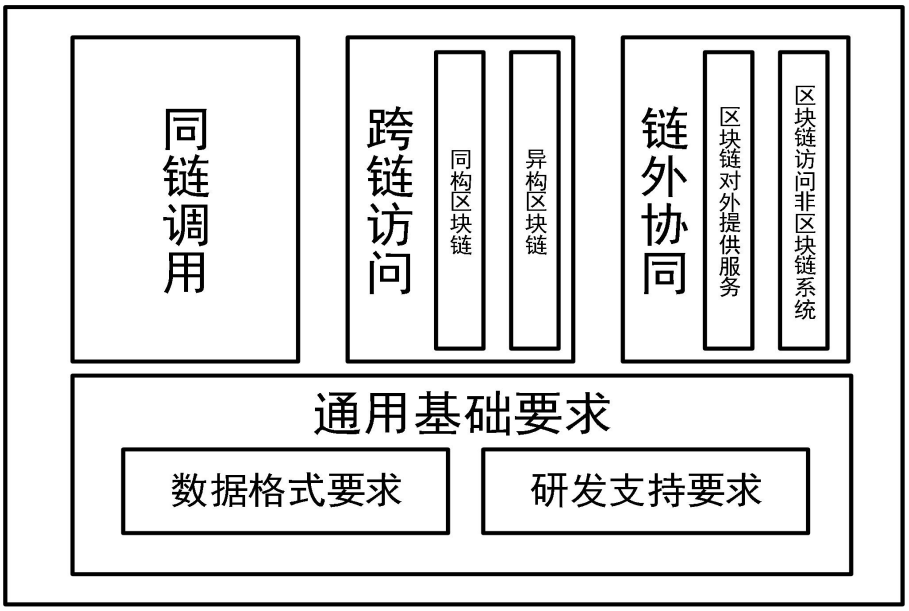

图 2 区块链数据协同体系框架

五、通用基础要求

（一）数据格式要求

区块链数据协同应采用标准化的数据格式。

文本类型数据，其编码应符合 GB 18030《信息技术 中文编码字符集》标准。

日期和时间类型数据，其格式应符合 GB/T 7408—2005《数据元和交换格式 信息交换 日期和时间表示法》标准。

（二）研发支持要求

1.文档说明支持

区块链产品应对其数据协同功能提供完善的说明文档，如数据协同的 API 接口、数据协同的流程和协议等。

2.测试认证要求

区块链产品的数据协同功能及其说明文档应经过外部权威机构的测试和认证。

3.开发工具支持

区块链产品宜对其数据协同功能提供完善的软件开发工具包和集成开发环境，支持外部应用或其他区块链产品便捷实现区块链互访功能。

六、同链调用

（一）功能要求

1.多合约支持

区块链网络上应支持部署多个智能合约，不同的智能合约运

行应互不影响。

2.数据隔离要求

区块链产品应实现不同智能合约之间的数据隔离。同一个区块链网络上的多个智能合约的业务数据是彼此独立的，一个合约不应直接访问另外一个合约的数据。

3.合约互访支持

区块链产品应提供机制支持同一个区块链网络上的多个智能合约彼此调用，从而实现数据的间接访问。

（二）访问控制

区块链产品应实现同链方法调用的权限控制。智能合约通过访问控制实现其他合约对本合约的访问准入、访问范围控制。

1.权限策略由被调用智能合约确定

区块链产品应提供权限设置的编程接口供智能合约编写者在编写合约时设定访问控制权限。

2.权限宜支持动态调整

从易用性考虑，建议提供运维接口供合约上线运行后的访问控制权限调整。

（三）协同原则

1.同链调用应满足事务性要求

（1）原子性：同链方法调用应只有全部成功、全部失败两种状态，不允许部分成功。若合约执行过程中有部分逻辑失败，合约应该回退此前已经成功完成的全部操作；若为同步调用，需

向调用方返回失败应答。

（2）一致性：同链方法调用之前和调用之后，区块链数据的完整性不能被破坏。

（3）隔离性：同链方法调用必须互不干扰，当一个合约被同链其他多个合约调用时，必须确保任意一次调用期间不能访问到其他调用所产生的过程数据。

区块链产品宜支持多种智能合约的事务隔离粒度，通过动态调节事务锁的粒度适应于不同的智能合约并发访问场景。

（4）持久性：同链调用完成后，对区块链所作的修改应保存在区块链节点上，不会被回滚。

2.数据量建议

区块链产品应提供相关评测数据，或直接明确同链调用的数据量建议。

3.可审计要求

区块链产品应为同链调用生成单独的持久化日志，区分于产品其他日志信息，记录同链调用的关键信息，如一次同链调用中发起调用的合约 ID、被调用的合约 ID、调用结果、时间戳等，供审计之用。

七、跨链访问

跨链访问涉及两个区块链的物理通讯，发出请求的区块链称之为请求链，响应跨链调用的区块链称之为处理链，一次完整的跨链访问流程划分为跨链请求与跨链响应两个阶段。

（一）功能要求

1.跨链数据传输支持

区块链产品应提供机制支持数据从一个区块链网络传递到另一个区块链网络，从而实现数据的跨网络跨账本访问。

2.同构链与异构链支持

跨链访问包括同构区块链跨链访问和异构区块链跨链访问。区块链产品应支持同构区块链跨链访问和异构区块链跨链访问。

3.指导要求

区块链产品应提供跨链访问的数据适配方法和访问范式，便于其他区块链正确发起跨链访问。

4.双向跨链支持

区块链产品应支持双向的跨链访问功能，既能响应其他区块链的访问请求返回处理结果，也能向其他区块链发起访问请求接受处理结果。

（二）访问控制

1.权限策略由处理链实现。区块链产品应实现跨链方法调用的权限控制。处理链通过访问控制实现对请求链的访问准入、访问范围控制。

2.访问控制设置支持。区块链产品应提供跨链权限控制维度说明，并提供相应的权限设置方法。

3.访问控制范围要求。访问控制的权限策略宜包括用户控制与服务器控制两个层次。用户控制要求调用方提供合适的用户凭

据，设备控制要求调用方在指定的服务器上才能发起请求。

（三）协同原则

1.健壮性要求

请求链与处理链自身均应保证无论调用操作成功与否，均不影响本区块链的稳定性及链上程序的正常运行。

2.结果一致性认定要求

请求链与处理链须商定双方对于调用结果的确认方式，保证两条链关于跨链调用结果认定的一致性。

3.跨链访问应满足事务性要求

（1）原子性：跨链方法调用只有全部成功和全部失败两种状态，不允许部分成功。若处理链执行过程中存在部分逻辑失败，应该回滚此前已经成功完成的全部操作。

（2）隔离性：跨链方法调用与处理链内交易必须是互不干扰的，当一个处理链同时处理跨链调用与其他交易时，必须确保任意一次调用期间不能访问到其他交易所产生的过程数据。

（3）一致性：跨链调用之前和调用之后，请求链与处理链的区块链数据完整性不能被破坏。

（4）持久性：跨链方法调用完成后，对处理链所作的修改必须保存在节点上，不会被回滚。处理链的区块链产品需提供机制明确请求链的调用不可抵赖。

4.超时机制设置

区块链产品应实现跨链访问的超时机制，当所访问的区块链

系统未在时限内响应时，应视为访问失败，回滚已经执行的操作。

5.回调机制建议

区块链产品建议实现跨链回调机制，在发起跨链访问时，推荐同时提供回调方法供对手链完成请求时调用本区块链的功能，以提高跨链访问的效率。

6.配置式实现方式建议

区块链产品宜实现可配置的跨链访问模式，通过参数和文件的配置以支持访问不同的其他区块链产品，尽量避免通过修改代码逻辑来实现跨链适配。

7.同步请求限制建议

除对处理链完全不进行任何更新操作的查询交易外，不建议采用同步方式进行跨链调用。

8.可审计要求

区块链产品应为跨链调用生成单独的持久化日志，区分于产品其他日志信息，记录跨链访问的关键信息，如记录一次跨链访问中发起调用的来源、用户、应用名、被调用的合约 ID、调用结果、时间戳、交易 ID 等信息，供审计之用。

9.其他措施建议

区块链产品宜支持确保跨链访问的可信性的各类措施，措施可包括:

（1）多重访问：对于查询请求，请求链可访问处理链的多个节点，观察其返回的结果是否一致。

（2）写后读验证：请求链向处理链发出写请求后，再发出对应的读请求，观察数据是否已经写入。

八、链外协同

（一）区块链对外提供服务

1.功能要求

区块链产品应提供对外调用接口服务，支持外部系统和用户访问区块链的特定功能。对外接口应包含以下三类：

（1）区块链网络信息与状态查询，包括区块链的网络状态，如网络中节点数量和类型；特定节点的状态，如节点的 IP、服务端口、节点区块链高度、节点区块链哈希值等。

（2）区块数据信息查询，区块链中任意节点的任意区块信息，如区块哈希值、区块包含的交易明细、区块时间戳等。

（3）智能合约操作，包括智能合约的部署、更新与停用。

（4）智能合约访问，调用区块链的特定智能合约的特定功能，获取其执行结果或交易回执。

2.访问控制

区块链系统应实现外部系统对其内部功能调用的权限控制。

（1）区块链产品应实现渠道接入控制。区块链产品应支持在渠道接入时对外部系统的访问权限控制，如通过身份识别拒绝非法访问、通过限流措施控制访问流量等。

（2）区块链产品应实现智能合约操作控制。区块链产品应支持对智能合约的操作控制，如要求智能合约的更新操作需由组

成区块链的半数以上节点拥有者同意方可执行;或将智能合约更新操作授权由区块链中少数用户执行。

（3）非业务权限宜支持动态调整。建议区块链产品提供运维接口，供区块链网络的运营方动态调整用户的访问控制权限。

（4）智能合约应实现业务权限控制。区块链产品对智能合约的访问权限的控制应通过用户管理机制实现,不同用户拥有对不同智能合约的不同调用权限。

（5）合约权限粒度建议。合约的调用权限宜当细化到合约的具体方法,不同用户对用一个合约的同一个方法可具有不同的访问权限。同一个用户对同一个合约的不同方法也可具有不同的访问权限。

3.联机访问协同原则

联机访问由用户独立直接触发。联机访问一般处理的数据量较少，对处理的实时性要求较高。区块链产品应实现联机访问功能。

（1）健壮性要求。区块链产品应保证无论调用操作成功与否，均不影响本区块链的稳定性及链上程序的正常运行。

（2）通讯协议建议。区块链联机交互宜通过 RESTful API 实现,RESTful API 所使用的数据格式宜采用符合 IETF RFC 8259《The JavaScript Object Notation (JSON) Data Interchange Format》的 JSON 报文格式。

（3）响应时间要求。联机访问方式下区块链应在约定的合

理时限之内返回应答，避免外部系统或用户长时间等待。此时限应支持基于系统业务需求灵活设置。

（4）交互数据建议。联机访问方式下区块链与外部系统每一次交互包含的交易数量不宜过多，数据包大小不宜超过大，避免对系统性能造成影响。

（5）服务稳定性要求。区块链产品应具备联机访问方式下支持 7×24 小时服务的能力。

（6）访问模式支持。区块链产品应支持同步访问和异步访问两种模式。异步访问模式执行结果的返回方式应支持推送与拉取两种。

a.推送模式：区块链达成共识、执行完合约之后，主动将结果发送到外部系统。

b.拉取模式：外部系统主动访问区块链，查询执行结果。

4.批量处理协同原则

批量访问一般处理的数据量较多，但对处理的实时性要求不高。区块链产品宜支持批量访问接口，以进一步提高系统的处理效率。批量访问宜支持系统自动触发。

批量访问宜以批量文件交互的形式实现：

（1）文件编码应符合 GB 18030《信息技术 中文编码字符集》标准。

（2）文件在传输前应压缩并附带数据摘要以供校验。

（二）区块链访问非区块链系统

1.功能要求

区块链产品除可使用智能合约基于自己独立的账本上的数据进行处理外，应提供数据互通模块，支持从外部系统获取数据，以支撑业务处理需要。

区块链访问非区块链系统涉及区块链与外部系统的物理通讯，区块链为请求方，外部系统为响应方。

2.访问控制

（1）访问控制的权限策略由响应方确定。

（2）区块链产品在访问非区块链系统时应支持主流身份认证、安全通信策略，包括加密校验、HTTPs 通讯等。

3.协同原则

（1）健壮性要求。区块链产品及调用程序实现者应保证无论调用操作成功与否，均不影响本区块链的稳定性及链上程序的正常运行。

（2）一致性要求。为保证区块链各节点处理的一致性，区块链产品应提供机制确保所有节点获取到一致的链外应答。

（3）处理时间建议。区块链产品访问非区块链系统宜尽量减少对原有区块链处理效率的影响，一次交易中访问非区块链系统所消耗的时间不宜超过总交易时间的 50%。

（4）效率要求。基于效率考虑，不建议区块链产品采用同步方式访问外部系统，一次交易中不宜有多次外部系统访问。

（5）数据量建议。区块链产品从非区块链系统获取的数据

量不宜过大。若单次获取链外数据量较大（超过 1M），建议考虑数据上链方式，如获取数据指纹替代数据本体。确有数据本体上链需求的，必须进行充分性能测试并提供相关测试报告，由业主方确认后方可上线。

（6）可审计要求。区块链产品应为访问非区块链系统的操作生成单独的持久化日志，区分于产品其他日志信息，记录所访问的非区块链系统标识、服务器 IP、功能名、访问结果、时间戳、交易 ID 等信息，供审计之用。

（7）传输内容安全。区块链产品应保证数据在传输过程中不被篡改，通过数据认证保障链外数据的完整性，目前常见的数据认证方法包括真实性证明与可信执行环境等。