跨境贸易区块链技术标准

Blockchain Technical Standard for Cross-Border Trade

目 录

前 言

本标准是跨境贸易区块链系统建设技术标准，旨在指导区块链技术在跨境贸易中的运用。

本标准由中国跨境贸易区块链联盟提出。

本标准由中国跨境贸易区块链联盟技术委员会归口。

本标准负责起草单位：中国跨境贸易区块链联盟、深圳壹账通智能科技有限公司。

本标准主要起草人：陆一帆、何万涛、贾牧、冯承勇、褚镇飞、章伟、方正向、王梦寒、杨扬、霍云、张鹏程、刘恩科、易卓欣等。

引 言

近年来，区块链技术在各个领域应用逐渐深入，尤其自 2018 年来，区块链应用如雨后春笋般涌现，深刻影响和变革了传统信息系统的技术架构、服务模式和业务流程，但也给系统建设带来了新的挑战。各企业、机构、团体分别搭建自己的区块链系统，但缺少统一的区块链系统标准，各个区块链系统很难达成共识，阻碍了信息的有效传播，影响了信息的使用价值。

在跨境贸易领域，亦缺少相应的区块链标准。此次借助海关区块链应用项目的落地，特提出跨境贸易领域的区块链系统技术标准，旨在规范和指导区块链在跨境贸易中的应用。

分布式存储、点对点通信、链式结构、共识机制、加密策略等技术特性，区块链系统在项目实施方式上与传统架构存在诸多差异，应重点关注、妥善应对。区块链系统本质上仍是一种信息系统，应满足国家信息系统建设要求，本标准重点提出了体现区块链系统特性的差异化要求。

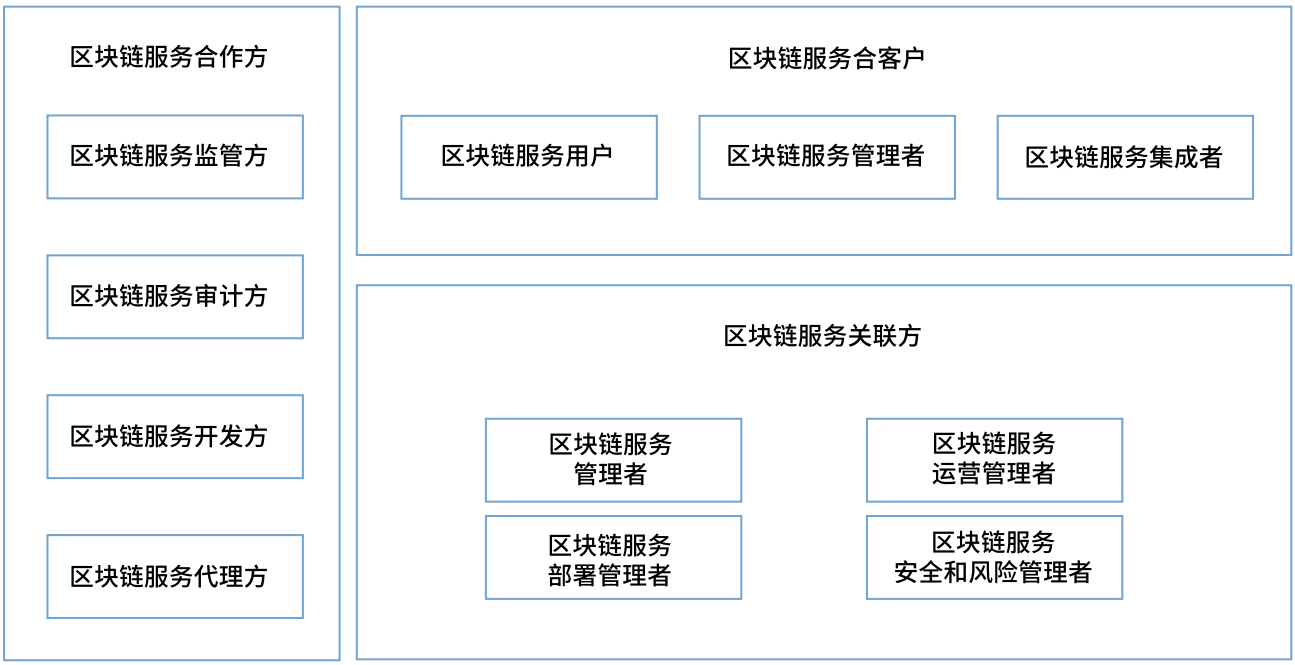
跨境贸易区块链技术标准

1. 范围

本标准规定了区块链系统在实施跨境贸易业务上的技术架构要求，涵盖了系统的架构设计、跨链技术、共识机制、智能合约运用、数据传输、存储、隐私保护与授权、身份认证、区块链系统监督与审计等内容。

本标准适用于跨境贸易领域的区块链服务提供者、服务使用者、服务合作者等，细分角色可参考下图：

图 1



2. 术语、定义和缩略语

2.1. 术语和定义

2.1.1. 区块链 blockchain

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，它本质上是一个去中心化的数据库。

2.1.2. 点对点技术 peer-to-peer (P2P)

又称对等互联网络技术，是一种网络新技术，依赖网络中参与者的计算能力和带宽，而不是把依赖都聚集在较少的几台服务器上。

2.1.3. 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资产数据库。

2.1.4. 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。

2.1.5. 零知识证明 zero-knowledge proof

零知识证明是由 S.Goldwasser、S. Micali 及 C.Rackoff 在 20 世纪 80 年代提出。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

2.1.6. 系统可用性 system availability

指在要求的外部资源得到保证的前提下，服务在规定的条件下和规定的时刻或时间区间内（不包括计划内服务中断时间）处于可执行规定功能状态的能力，一般按年允许计划外服务中断时间、可用程度至少达到“n 个 9”来衡量。

2.1.7.REST 接口 representational state transfer

即表述性状态传递，是 Roy Fielding 博士 2000 年在他的博士论文中提出来的一种软件架构风格。

它是一种针对网络应用的设计和开发方式，可以降低开发的复杂性，提高系统的可伸缩性。

2.2. 缩略语

API 应用程序编程接口（Application Programming Interface）

CPU 中央处理单元（Central Processing Unit）

HTTP 超文本传输协议（Hypertext Transfer Protocol）

HTTPS 安全超文本传输协议（Hypertext Transfer Protocol Secure）

VPN 虚拟专用网络（Virtual Private Network）

SOA 面向服务架构（Service-Oriented Architecture）

TLS 传输层安全协议（Transport Layer Security）

TPS 每秒事务处理量（Transaction per Second）

3. 区块链系统标准

3.1. 架构设计规范

● 区块链系统应做到分层、模块化设计，从而易于维护，支持可扩展性；

参考下图：

图 2

● 区块链系统要保证数据隐私安全；

● 区块链系统应能识别加入网络的用户身份；

● 区块链系统应支持监管与审计功能。

3.2. 跨境贸易跨链技术规范

在由不同国家、地区、机构建立的不同区块链系统中，需要能够做到资源互认、信息共享，这时候就需要信息有一定的标准，以及跨链技术支持，本章节强调了跨链的技术标准要求：

● 跨链交互的报文标准借鉴 ISO20022 规范与 WCO 数据模型；

● 跨境贸易报文推荐采用 RESTFUL/JSON 作为报文格式，通过 HTTPS 加密传输报文；

● 跨境贸易报文字符集标准为 UTF-8；

● 跨境贸易接入方相互访问时，必须采用 HTTPS 双向认证；

● 为了帮助跨境贸易接入双方进行错误跟踪，跨境贸易接入方必须在跨境贸易报文头提供基于 Open Tracing 标准实现的 Open Trace ID；

● 区块链系统应支持不同区块链系统的跨链交互，可以采用的主流技术有：公证人机制、侧链技术、哈希锁定等。

3.3. 区块链系统性能标准

区块链系统由于共识算法的不同，影响了系统的交易性能，在可商用的区块链系统中，需要对系统的性能提出统一的要求。区块链的性能指标应当包括吞吐量和交易延时，在实际应用中，需要综合两个要素进行考察，只使用交易吞吐量而不考虑延时或者反之都是不正确的。长时间的交易响应阻碍用户的使用从而影响用户体验；只使用延时而不考虑吞吐量会导致大量交易排队。

同时，出于安全性考虑，相关密码算法需要使用国密，具体建议如下：

● 使用国密算法的情况下，吞吐量达到 1000 TPS 以上所需的服务器硬件资源不超过：

CPU：4 核 2.1GHz

内存：8G

（单链场景，不计网络延时）；

● 在服务器应用纵向扩展或者横向扩展的情况下，吞吐量可以无限扩展；

● 使用国密算法的情况下，平均延时达到实时或准实时级别，小于 0.05s 所需的服务器硬件资源不超过：

CPU：4 核 2.1GHz

内存：8G

（单链场景，不计网络延时）。

以上测试的区块链网络应当包含账本节点，共识节点；交易流程包括交易发起、共识算法执行、账本写入完成等步骤。

3.4. 共识机制

共识机制是区块链网络的重要技术组件，区块链共识机制是使所有有效节点达成一致所采用的计算方法。共识机制本身是一套分布式算法，根据应用场景的不同需求，跨境贸易区块链可以选择特定性质的共识机制。共识机制需满足以下要求：

- 必须是有效算法，在任意场景下，由有效节点能产生唯一确定的结果；
- 必须满足强一致性，不可以使用任何一种最终一致性的共识机制；
- 高可用性，任意不超过理论值的节点数故障，整个区块链系统仍能正常工作；
- 强安全性，共识机制需要可以防止二次支付，防止重放攻击，防止恶意节点攻击；
- 支持区块链网络节点扩展，当网络节点增多时，不明显影响共识算法的运行速度；
- 高性能和低延时，从交易提出、共识请求到交易被记录在账本中的总延时不多于 0.2 秒；
- 系统资源依赖，达成共识机制的过程中，所依赖的服务器硬件配置不超过 4 核 2.1GHz CPU、8G 内存。

3.5. 智能合约

智能合约基于计算机代码形式实现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执行该协议。根据应用场景的不同需求，跨境贸易区块链可有选择性地提供智能合约功能。在使用智能合约的系统中，需提供如下功能支持：

- 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；
- 支持监管方统一部署或参与方自行部署的方式，以满足监管要求；
- 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；
- 涉及变更区块链账本信息的智能合约，必须有相应的差错处理约定，确保数据的正确性；
- 区块链系统中实现的智能合约也应考虑智能合约的生命周期管理，包括：订立、履行、变更、中止、审查、监督等。

4. 区块链系统的数据安全要求

4.1. 数据传输标准

区块链系统的分布式特性，对数据在传输中的安全提出了更高的要求，在传输中，要保证数据的安全，可以使用以下几种传输方案：

- 专线；
- 考虑到专线网络的成本，推荐采用 VPN 传输；
- 如果在公网下，数据传输需要加密加签。

在传输性能方面， 单次请求响应时间不应超过 3 秒。

4.2. 数据存储标准

区块链系统在存储上跟传统信息项目的存储方式不同，区块链项目的存储是参与记账的节点维护同样的账本内容，每个记账节点都能查看到链上数据，这就给数据存储提出了新的要求：

- 保存到区块链上的重要数据要加密存储，或做到按字段加密；
- 非结构化数据，如文本、音频、视频等不建议保存到链上，可以保存其数据摘要到区块链上。

4.3. 数据隐私保护和授权标准

跨境贸易区块链中存储的信息是各参与方的核心交易数据，各方并不愿意将这些隐私数据以明文方式公布出来，同时由于监管或贸易纠纷取证等现实需求，又需要对关键交易信息的合规性进行验证。因此如何在保持交易数据隐私性的同时验证交易的合规性是跨境贸易区块链中需要解决的核心问题。

为保证跨境贸易区块链系统中多方参与者数据的隐私性，需要对上链的敏感数据进行加密保护。在需要进行数据共享的场景下，需要通过安全可靠的通信链路执行数据的授权操作，授权前需要对被授权人进行身份认证。为减少敏感数据的泄露风险，应该尽量使用零知识验证来验证业务数据的合规性，避免使用数据的直接授权。

- **密码算法**

跨境贸易区块链中使用密码算法对敏感的关键信息进行加密保护，链上的关键信息均以密文形式进行存储。

系统中使用中华人民共和国密码管理机构认可的标准密码算法及算法参数来保证上链敏感数据的机密性、完整性和不可抵赖性：

公钥密码算法应使用《GM/T 0003 SM2 椭圆曲线公钥密码算法》；

密码杂凑算法应使用《GM/T 0004 SM3 密码杂凑算法》；

分组密码算法应使用《GM/T 0002 SM4 分组密码算法》。

● **零知识证明**

跨境贸易区块链需要实现在验证关键信息合规性的前提下，并不泄露具体的信息内容，实现零知识证明。可选择以下一些方式实现零知识证明：

可以使用同态加密实现机密交易；

可以使用范围证明或双线性对等技术实现对机密交易合规性的验证；

使用其它具有可证明安全性的零知识验证技术。

在区块链上实现零知识证明，所有密码算法及算法参数应遵守中华人民共和国密码管理机构认可的标准密码算法及算法参数，在需要使用双线性对的场合，应使用《GM/T 0044 SM9 标识密码算法》标准中定义的曲线参数。

● **数据授权**

某些需要进行数据共享的应用场景下，数据拥有方可以通过授权的方式与其他参与方共享加解密密钥及关键数据。

在数据授权操作中，所有密码算法及算法参数应遵守同密码算法部分相同的要求。授权前需要对用户进行身份认证，所使用的公钥证书应符合相关标准密码算法。

● **密钥安全**

密钥是保证关键数据机密性的核心信息，保证密钥全生命周期的安全性才能真正保护关键数据的隐私性。这就对系统中使用的密钥数据提出了一些要求：

a) 数据密钥应加密保存在数据所有者的内部网络上，密钥数据要做到隔离；

b) 要求一文一密，防止一个密钥的泄露引起整个系统的信息泄露；

c) 系统中如果有密码机则使用密码机保护系统中的关键密钥，如果系统中未配置密码机则采用多分量及口令保护等技术实现对关键密钥信息的加密保护；

d) 对系统中密钥的产生、分发、存储、使用、销毁、更新等流程制定安全管理方案，确保密钥信息的安全。

4.4. 应用系统的信息安全

依托于区块链系统的上层应用服务，也需要关注信息安全，应能够提供包括但不限于以下能力：

● 应用系统应具有对账户下所包含静态信息的保护能力，可能的信息包括：账户归属、资金余额信息等；

● 应用系统应具有对交易过程中信息的保护能力，可能的信息包括：交易双方账户，交易金额等；

● 系统建设方应审查和识别与系统设计有关的任何可能的安全风险和威胁。根据已识别的风险和威胁，进行记录并提供建议方案；

● 如果使用 cookie，则应用软件只能使用会话 cookie 并仅存储非个人身份信息。应严格禁止收集个人身份信息。 cookie 只能用于存储维护用户会话所需的会话 ID。理想情况下，会话 ID 应由随机形成的字符串组成，且不得包含披露用户或其交易信息的数据，所有的

cookie 应有一个到期时间戳，不应超过用户与系统的网络会话时长；

● 系统通过 Web 门户或消息传递基础设施发送或接收的任何附件和消息应先被扫描以查找恶意代码，然后才能将其传递给下一级处理。扫描应在隔离区内进行。带有恶意代码的附件和消息应在区域内隔离，不得触发下一阶段处理。系统应向相关团队发送警报通知，以检查隔离的消息、附件；

● 应对应用程序接收和处理的所有数据（输入和输出）实施输入验证。输入验证应在客户端和服务器端执行；

● 应实施适当的应用程序异常处理机制来显示简单的错误消息，在应用程序出现任何异常情况时，这些错误消息不会提供任何详细的错误消息；

● 系统建设方应确保应用程序的设计和实施不受至少以下漏洞的影响：

a）输入参数未经验证（例如 SQL 注入和参数操作）；

b）命令注入；

c）跨站点脚本攻击（XSS）；

d）损坏的访问控制；

e）破坏的身份验证和会话管理；

f）不安全的直接对象引用；

g）跨站请求伪造（CSRF）；

h）缓冲区溢出；

i）安全性错误配置；

j）不安全的密码存储；

k）未能限制 URL 访问；

l）异常和错误处理能力差；

m）传输层保护不足；

n）无效的重定向和转发。

● 系统建设方应参考开放 Web 应用安全项目（OWASP）十大安全风险以及 OWASP Top 10 未涵盖的其他新兴风险；

● 系统建设方应实施 Web 应用程序防火墙（WAF），以保护对互联网可访问的 Web 应用程序（例如网站和电子服务）的保护。WAF 解决方案应具备高可用性，并且能够连续应对（第 5 层到第 7 层）威胁，而不管 DDOS 攻击率和数量如何。

4.5. 密码算法处理能力

为满足跨境贸易区块链的性能要求，系统中使用的各类密码算法应满足以下性能要求：

● SM2 算法一次点乘（非基点乘）计算时间小于 300 微秒；

● SM3 算法哈希值生成速度不小于 70MBps；

● SM4 算法加解密速度不小于 20MBps；

● SM9 算法一次双线性对计算时间小于 10 微秒。

5. 认证和身份管理

跨境贸易区块链系统中的节点和用户需要进行接入认证和访问控制。节点请求接入区块链网络和请求访问区块链资源时，需要核实节点身份。一般情况，采用数字证书等认证方式完成节点接，根据证书管理和使用的不同阶段，系统需符合以下要求：

● **认证系统准备：**

a)CA 系统应能够部署离线根 CA，保护根密钥的安全；

b)CA 系统应能够方便的配置，能够支持多级 CA 的签发和管理；

c)CA 系统应能够支持常见类型的商用硬件密码设备，包括各类型加密机，签名验签服务器等；

d)CA 系统应具备国产密码算法加密证书的密钥管理功能；

● **证书签发**

a) 数字证书应由信任 CA（Certificate Authority）系统签发和管理。境内机构和用户应使用具备《电子认证服务使用密码许可证》和《电子认证服务许可证》资质的第三方 CA 机构签发。如果使用自建 CA，须经所有参与方同意，自建的 CA 系统应为具备商用密码产品型号和商用密码产品销售许可的系统；

b)CA 系统应支持国密规范的系列密码算法，签发的证书应符合国密规范的证书格式；

c)CA 系统应支持国际标准的密码算法和证书格式；

d)CA 系统应同时支持在线和离线等多种方式签发证书；

● **证书生命周期管理**

a)CA 系统应具备用户注册和身份鉴别机制，提供用户信息注册管理功能，对用户身份进行鉴别。根据国家法律法规要求，CA 应能够对最终用户的真实身份进行核实，核实方法包括但不限于面对面核实、远程核实等；

b)CA 系统应提供证书生命周期相应的证书管理接口和证书服务；

c)CA 系统应提供证书实时状态服务或定期发布证书撤销列表（CRL）；

d) 区块链系统应能够管理信任 CA 的准入，注册信息包括 CA 的基本信息和 CA 根证书，区块链系统中的业务模块在验证相关方数字证书时，根证书将作为证书链的信任锚；

e) 区块链系统应能够对 CA 根证书停用或挂起；

f) 区块链系统应能与第三方 CA 系统集成，实现证书生命周期各个状态的变更管理，包括证书更新，撤销等功能；

● **证书应用**

a) 区块链系统的节点和用户应使用身份标识来向区块链系统证明自己的身份 , 身份标识可使用 X.509 格式的数字证书；

b) 区块链系统通过数字证书和数字签名机制来证明节点和用户的身份；

c) 区块链系统应能够同时支持国产密码算法证书和国际标准密码算法证书。使用国密算法证书时，应符合国密证书系列应用规范；

d) 区块链系统应支持国密双证书体制，即签名证书和加密证书。涉及签名的场景使用签名证书，涉及数据加密的场景使用加密证书；

e) 区块链系统应根据证书识别每个访问实体的真实身份，以明确访问实体的访问控制权限，并保证每个实体只能按照系统设定的范围使用系统提供的业务；

f) 区块链系统应对签名方进行身份认证，确认其对签名密钥的拥有权限；

g) 区块链系统验证节点或用户证书时，需要验证证书的信任链、证书有效期和撤销状态；

h) 区块链系统中的用户或节点在通讯时应使用 SSL 证书建立安全通道，完成与区块链系统之间的数据交互，以保证敏感数据的机密性和完整性。区块链系统应支持国密算法的 SSL 协议；

i) 区块链系统中的智能合约应包含可信代码签名证书对其签发的代码签名，智能合约部署时，区块链系统应对其代码签名及代码签名证书进行验证，代码签名证书的准入和停用由区块链系统管理。

6. 区块链系统运营、监管与审计

在系统实施阶段，要提供对区块链系统的管理与运营支持；在系统运行后，要提供对系统的监督与审计功能。区块链系统的不可篡改性，对录入的内容安全提出了强要求，系统应具备对录入信息的监督、审计能力。

6.1. 管理与运营

● 区块链建设方应提供区块链技术服务能力、智能合约、服务、API 等的清单；

● 区块链系统应提供异常和问题的发现和报告能力，并通过分析和处置流程管理这些异常报告。异常和问题可由区块链节点、运营方或用户发现和报告；

● 区块链系统应能够根据既定规则和所获取的监控数据，准确的发现、分析和预测区块链系统存在的问题；

● 区块链系统应能够根据症状的诊断结果和预设的告警阈值，及时告警；

● 区块链系统应建立完善的应急预案，能够在灾难发生的时候给相关处理人员精准的操作指导，帮助其在最短的时间内完成灾难控制和系统恢复；

● 区块链系统应通过服务实现和访问接入的形式提供区块链系统服务交付能力。同时，还应设置必要的工作流程，确保相关交付单元按序交付；

● 区块链系统应提供节点的管理能力，包括生命周期、性能、可用性等；

● 区块链系统应提供环境监控、日志管理等能力。应能够及时获取节点状态、网络质量、共识进程、区块数据等重要数据，应能够方便地对外提供系统各个核心组件的关键数据，并及时以日志形式输出，可作为外部监控、监管工具的输入，以便于利用监控、监管工具定义各种规则来进行系统运营；

● 区块链系统监控功能可包括用于响应环境变化（如系统容量需求、错误分析结果等）的分析能力和自动化工具；

● 区块链系统应提供智能合约、节点等的软件升级和版本管理能力，包括节点和系统的代码基准和实现构件等；

● 区块链系统应提供区块链服务的定义、更新和访问策略及针对这些策略的管理能力，包括用于区块链服务本身及其使用的业务、技术、安全、隐私和认证等策略；

● 区块链系统应提供在用户及服务提供方运营系统、业务系统和跨链服务提供方的管理及业务功能的连接能力，负责根据请求建立与跨链服务提供者的连接，并传送相关的身份和认证信息。

6.2. 监管

● 应具备完善健全的监管治理体系。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；

● 支持监管机构加入区块链网络作为其中一个节点进行即时监管。监管节点可对数据完整性、有效性和流程合规性进行即时的监督与稽核，并对异动交易进行干预，封停有非法行为的业务；

● 监管干预活动相关的数据和证据应进行完整记录和保存；

● 设置明确的监管治理规则，应同时支持由人参与监督管理的、无法用技术自动实现的规则；

● 由组织机构或管理人员依据法律、行政法规、部门规章等进行监管治理的规则，并鼓励充分利用智能合约等技术有效支持智能化的监管操作，提供可自动化实现的监管规则；

● 保存与服务、资源、性能相关的数据和证据。这些数据和证据包括协议所有相关方的活动和运营环境条件的记录和日志，需要以安全的方式收集和维护。

6.3. 审计

● 系统应实施完善的日志管理系统，以便安全地捕获、存储、管理、审核和审计应用程序日志；

● 要捕获的日志应包括记录所有基础设施组件（例如：服务器、防火墙、虚拟机和网络设备）以及所有应用系统和服务；

● 对日志的访问应该是受控制的，明确定义角色，防止以任何形式修改或篡改或删除日志；

● 系统应能够在检测到特定事件（如错误或数据库故障）时生成通知和警报，以提醒相关支持人员；

● 系统应记录由特权账户执行的所有活动，包括系统管理员、审计员、数据库管理员、网络管理员和任何其他管理员账户。

参考文献

● ISO20022

ISO20022《金融服务金融业通用报文方案》是 2004 年由国际标准化组织在 ISO15022 《证券报文模式 (数据域字典)》的基础上制定并发布的国际标准，是国际金融业务与 IT 技术紧密结合的产物，它提供了一种面向业务建立通用报文的解决方案。

详细参考：https://www.iso20022.org/

● 《区块链参考架构》

工信部发布的中国首个区块链标准，详细参考：

http://www.cbdforum.cn/bcweb/index/bz/1-3.html

● 《区块链数据格式规范》

工信部发布的区块链数据格式规范，详细参考：

http://www.cesi.ac.cn/201712/3465.html

● OpenTracing

是一个跨编程语言的标准，此项标准可以使分布式系统便于分析各个阶段的耗时情况，以及协助排查错误。

详细参考：https://opentracing.io/

● 密码算法 :

国家密码算法介绍，详细参考：http://www.oscca.gov.cn/sca/xxgk/bzgf.shtml

● 世界海关组织 数据模型 (WCO Data Model)：

http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/data-model.aspx