ICS 35.240.99
CCS A 10

T/ZADT

团　　体　　标　　准

T/ZADT XXXX-XXXX

数字贸易 基于区块链的供应链金融安全服务指南

Digital Trade - Security Service Specifications for Blockchain-based Supply Chain Finance

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

浙江省国际数字贸易协会　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。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由宁波舟山港集团有限公司、浙江大学、杭州趣链科技有限公司提出。

本文件由浙江省国际数字贸易协会归口。

本文件起草单位：。

本文件主要起草人：。

数字贸易 基于区块链的供应链金融安全服务指南

1 范围

本文件提供了区块链供应链金融安全服务的指导，具体内容包括供应链金融系统具体相关人员、区块链安全和应用系统安全的分类和具体措施、系统应用原则等。

本文件适用于为使用区块链的供应链金融服务的组织和机构提供安全服务规范参考，并帮助其进行系统安全的预防和维护。

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 25069-2010 信息安全技术 术语

CBD-Forum-001-2017 区块链 参考架构

ISO 22739:2020 区块链和分布式账本技术-术语（Blockchain and distributed ledger technologies — Vocabulary）

3 术语

下列术语和定义适用于本文件。

3.1

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：ISO 22739，3.6]。

3.2

智能合约 smart contract

存储于分布式账本中的计算机程序。

注：用于程序化的记账或自动化交易执行，其共识执行结果都记录在分布式账本中。

3.3

节点 node

提供分布式账本的所有功能或者部分功能的实体。

[来源：JR/T 0184-2020，3.22]

3.4

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（例如接收者）伪造或抵赖。

[来源：GB/T 25069-2010，2.1.2]

3.5

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

[来源：GB/T 25069-2010，2.1.4]

3.6

凭证 credentials

为确定实体声称的身份而提供的数据。

[来源：GB/T 25069-2010，2.1.1.95]

3.7

共识算法 consensus algorithm

区块链系统中各节点间为达成一致采用的计算方法。

[来源：CBD-Forum-001-2017，2.2.3]

3.8

系统生命周期 system life cycle

系统从概念提出到系统无法安全、有效的提供服务为止的整个时间阶段。包括：概念提出、需求收集、系统设计、系统开发、系统运营、系统维护、系统废止。

3.9

风险管理 risk management

为达到系统效益最大化，针对系统（区块链底层和金融应用层）、人员配置、硬件设施等全流程，运用潜在失效模式及后果分析（FEMA）等方法进行风险分析，并提出应对方案的过程。

3.10

用户 user

用户是指参与到分布式账本上实际责任主体的基本单位，责任主体一般指自然人、法人或者机构等。用户只有通过分布式账本上的账户才能参与分布式账本的业务，一个用户至少拥有分布式账本上的一个账户。

4 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用编程接口
AML	Anti-MoneyLaundering	反洗钱
DDOS	Distributed denial of service attack	分布式拒绝服务攻击
DPOS	Delegated Proof of Stake	委托权益证明
ERP	Enterprise Resource Planning	企业资源计划
PBFT	Practical Byzantine Fault Tolerance	实用拜占庭容错
POW	Proof of Work	工作量证明
POS	Proof of Stake	权益证明
P2P	Peer-to-peer	对等网络

5 系统相关方

5.1 概述

区块链供应链金融安全服务相关方主要包括业务相关方、业务系统提供方和区块链技术提供方，见图 1。

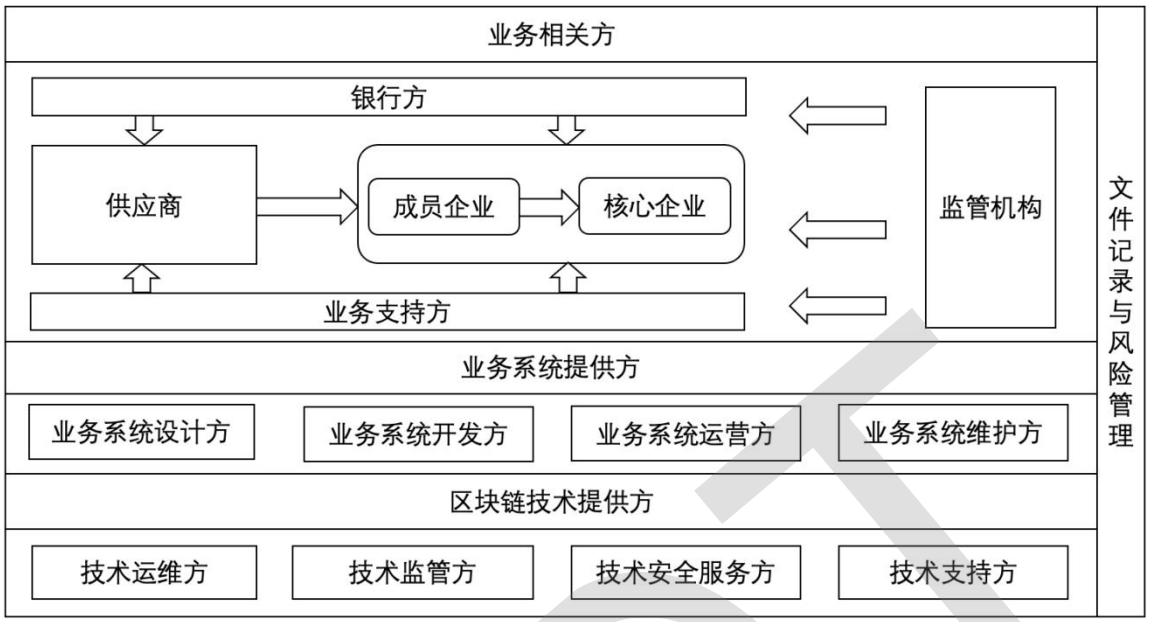

图 1　区块链供应链金融安全服务相关方

业务相关方是区块链供应链金融服务系统的使用方，其主要包括：核心企业、成员企业、供应商、银行方、监管机构和业务支持方。供应商为成员企业、核心企业供货并形成供应链，银行方负责推进金融业务，监管机构负责监管整体交易环节，业务支持方完善整个业务系统功能。

业务系统提供方是伴随区块链供应链金融服务系统生命周期而产生的，包括：业务系统设计方、业务系统开发方、业务系统运营方、业务系统维护方。系统的设计、开发等全过程配有相应的文档记录。业务提供方负责保障系统的合理和稳定，保证系统的安全可控。

区块链技术提供方包括：技术运维方、技术监管方、技术安全服务方和技术支持方。区块链技术提供方在其业务范围内，尽可能照顾与参与到区块链供应链金融服务系统的实际应用的建设中，与业务系统提供方和业务相关方建立及时、有效的沟通渠道。

文件记录与风险控制是贯穿整个系统生命周期的关键项，业务相关方、业务系统提供方和区块链技术提供方做好文件记录（云端文档记录、数据库记录、数据上链等形式），对于各项目做好风险预测与控制应对措施。

5.2　业务相关方

5.2.1　核心企业

核心企业是供应链金融系统的核心用户，以核心企业为出发点，提供授信给相关中小型企业，帮助中小型企业进行融资，解决中小企业融资难的问题。核心企业一般都要严格审核公司资质，保证其规模大、实力强，可以承担中小企业融资的潜在风险。系统控制核心企业的数量，保持供应链金融系统融资的流动性；并考察核心企业对上下游客户的管理能力、对银行的协助能力等。

5.2.2　成员企业

成员企业作为核心企业的下游企业，依赖于核心企业的背书。通过核心企业的授信向供应商签发票据，生成可融资的资产，以达到赊账的目的。其间资产可进行转让、质押等操作，在资产到期前，成员企业需进行资产归还，保证资金的流转。成员企业通过供应链金融系统获得资金宽限期，通过票据等资产的流转和核心企业的授信帮助成员企业完成资金的正常流转。

5.2.3　供应商

供应商向成员企业供货，并通过对信息流、物流、资金流的控制形成供应链。在供应链融资模式下，供应商面临追款难的问题和风险，依托于核心企业和融资新模式，供应链可用供应链金融平台资产进行

资产转让和资产融资，到期后可获得成员企业的还款和对应利息，减少供应商回款风险，降低信息不对称风险，盘活资金，同时降低融资门槛和成本。

5.2.4 银行方

银行方推进供应链金融业务的自治体系和建设能力，为核心企业客户及其供应商提供授信和信用的流转拆分业务。银行通过自身核心系统、授信系统、风控系统等帮助供应链系统中的组织提供贷款融资，在线追溯和验证资产，自主决定是否为中小企业提供融资。

5.2.5 监管机构

监管机构随时监控和管理数字资产，规范金融运作和交易，维护供应链金融市场秩序，保证资产的准确性和安全性。监管机构在供应链金融系统的职责一般包括：风险管理与关键控制点管理分析、系统维护监管与用户监管记录、用户诉求收集与系统运行监测、系统故障跟进等。

5.2.6 业务支持方

业务支持方指区块链金融业务系统为满足业务需求而接入的业务第三方，包括但不限于 ERP 系统、UKey、发票导入系统、第三方数据提供方等，帮助系统实现数据的准确性、便捷性，并加强系统身份安全性等，进一步优化系统的总体功能。

业务支持方相关运行与权限使用等宜纳入供应链金融服务系统框架中，采取相应监管和保护措施。

5.3 业务系统提供方

5.3.1 业务系统设计方

系统设计方应通过客户需求访谈、用户分析等多种方式确定用户需求，并对系统进行设计。

系统设计方的活动宜包括：

a) 确定系统核心需求和具体功能需求，进行需求拆分和需求方案确定；
b) 记录需求来源，对系统方案、提出方信息、提出时间等相关信息做记录收集；
c) 明确系统具体设计方案，挖掘用户痛点，提升系统用户体验，保持用户粘性。

5.3.2 业务系统开发方

系统开发方负责按照供应链金融系统的需求分析以及设计文档进行系统开发。

系统开发方的活动宜包括：

a) 主要活动内容为系统需求分析、系统设计文档功能划分、系统详细设计功能实现、系统单元实施和验证、系统功能集成与测试、系统测试；
b) 系统开发方宜保持对系统实际需求方（用户）和管理者的沟通，以便及时调整系统开发方向；
c) 系统开发方宜对系统进行充分分析，保证系统实现与设计一致；
d) 系统开发方宜对开发代码进行架构设计，避免迭代需求造成系统重构；
e) 系统开发方宜对开发环境做清晰管理，并定期维护，保证开发效率。

5.3.3 业务系统运营方

系统运营方负责供应链金融系统的落地实施与运行，是业务系统提供方之一。

系统运营方的活动宜包括：

a) 系统运营方宜在系统准备初始数据和权限，保证系统初期的正常上线运行；
b) 系统运营方应在系统发布后实时更新同步系统情况，做好沟通协调，保证系统正常使用；
c) 管理系统中的重要数据和资料，把控系统业务的运营和管理；
d) 系统发行的版本和创建过程形成文档归类，系统实际运行中做好监控工作，保障系统的稳定性。

5.3.4 业务系统维护方

系统维护方负责保证供应链金融系统运行，并进行实时和定期维护。

系统维护方的活动宜包括：

a) 活动包括但不限于制定系统维护计划、问题收集和修改方案分析、过程记录与评价反馈等；

b） 制定系统维护计划书，包含系统风险管理方法、定期维护与紧急维护方案、问题收集渠道、用户满意度评测方案等；
c） 从系统内部与用户两个方面收集系统实际满意度和产品反馈，生成问题记录与问题报告文档；
d） 将系统存在的问题进行分类，如安全型问题、体验型问题等，并针对潜在问题进行排查与分析；
e） 针对系统的突发问题有完善的预案，并有规范的应急处理措施。

5.4 区块链技术提供方

5.4.1 技术运维方

技术运维方负责区块链技术的运行和维护，给区块链系统的正常运行提供保障。
技术运维方的活动宜包括：
a） 生成活动文档（系统运行、维护日志记录），规划区块链相关软硬件的部署和实施；
b） 提供区块链技术指导人员，保证系统的正常运维；
c） 负责完善系统整体运营，及时跟进系统运行状态。

5.4.2 技术监管方

技术监管方负责保障系统正常运行，监管系统的运行全流程。
技术监管方的活动宜包括：
a） 系统现场环境信息管理，采集并生成分析报告；
b） 技术相关方监管和相关数据采集；
c） 系统故障报告信息采集与管理；
d） 数据状态异常分析与状态预警。

5.4.3 技术安全服务方

技术安全服务方负责系统运行安全，做好相应保障和应急措施。
技术安全服务方的活动宜包括：
a） 负责区块链技术安全保障与服务质量管理，确保系统的安全与稳定；
b） 技术安全保证措施包括但不限于技术安全维保、区块链故障管理、技术状态监测等；
c） 应有安全小组持续进行安全测试和安全技术探索创新，不断加强区块链技术安全性；
d） 宜与供应链金融系统相关人员建立实时沟通，及时接收相关技术信息和传达相关安全反馈，并预先设立安全服务的不同方案。

5.4.4 技术支持方

技术支持方为区块链技术提供支持服务，如网络计时服务、证书认证服务、可信时间戳、消息订阅，帮助区块链系统提高时间校对能力、身份认证能力、信息接收能力等，帮助完善区块链系统基本功能，保持系统健壮性。

6 系统安全

6.1 区块链安全

6.1.1 智能合约安全

6.1.1.1 安全审计

对合约代码进行验证，有效规避合约代码的潜在安全风险，在合约发布前进行完整的代码审计过程，确保智能合约的安全性、正确性和一致性。宜考虑以下条件：
a） 审计内容包括智能合约源代码，能够对源代码进行逐行检查分析；
b） 在智能合约部署到主网前完成安全审计，提前发现和处理合约安全问题；
c） 在安全审计过程中考虑智能合约逻辑缺陷、数据安全、外部调用错误处理等审计项；
d） 从系统角度详尽规划安全审计的全流程，针对智能合约安全审计和评估对象进行说明，包括基于风险管理思路的应急处理方式；
e） 自动化构建安全检测审计，保证检查结果的准确性和高效性；

f） 合理设计安全审计方案，提高拓展性，满足适配要求；
g） 提供专业技术人员的智能合约审计报告，保留审计相关的记录。

6.1.1.2 形式化验证

形式化验证采用数学的形式化方法对算法的性质进行证明或证伪，规范、开发和验证软件系统安全性、可靠性，宜考虑以下条件：

a） 形式化验证的过程包括建模、模型检测、模型验证等，用以验证程序的可靠性；
b） 选择合适的建模语言与建模工具，验证前对于验证结果做整体预期与规范；
c） 通过人工和自动化结合的方式进行形式化验证，提高验证结果准确性；
d） 对于智能合约状态可达性、有界性等性质做细致描述，做好验证体系构建；
e） 通过数学逻辑推理的严密性，保证完全覆盖代码的运行期行为，保证一定范围的绝对正确；
f） 考虑成本效率问题和对系统安全性高低的要求，选择性使用形式化验证，保证系统在保证安全性的同时满足自身的成本要求。

6.1.1.3 应急机制

针对智能合约有升级、冻结、解冻等应急处理方案，宜考虑以下条件：

a） 针对智能合约能够进行合约的升级操作，避免恶意合约持续影响，支持合约的多版本管理和控制；
b） 支持合约的冻结和解冻操作，保证合约管理者在合约异常时可以对合约进行修改和验证，实现应急处理；
c） 对智能合约数据做好备份，建立备份及时更新方案，加强数据可控性；
d） 建立基于智能合约安全规则库实现的智能检查合约漏洞、故障检测，成立应急预案工作小组；
e） 针对智能合约有监控方案和应急处理机制，包括（不限于）应急处理规划、应急组织架构、过程方法的应急物质保障、应急相关培训与宣贯等。

6.1.1.4 合约规范

对智能合约的设计进行规范，宜考虑以下条件：

a） 针对智能合约进行全生命周期管理，包括智能合约设计、创建、部署、升级、冻结、解冻等。智能合约部署、升级等记录保存在链上；
b） 设计一套完善的智能合约安全规范，并严格按照设计执行；
c） 智能合约宜采用最新的稳定版本的编程语言，编程语言编译器保持一致性，合约源码与字节码前后逻辑一致，确保编译结果的正确性；
d） 根据现有的业务逻辑进行总结，设计标准智能合约模版，代码符合书写规范、逻辑要求，规范合约编写质量；
e） 针对用户展示其效用边界，用户非法行为给予提示，合约升级、冻结等行为及时告知用户；
f） 针对多种语言（如 Solidity、Java 等）进行合约规范，保证智能合约的适用性。

6.1.1.5 交叉验证

使用规则交叉验证保证智能合约安全，宜考虑以下条件：

a） 规则交叉验证方式包括但不限于留出法、k 折交叉验证等；
b） 规则交叉验证包括订单风险检测娇艳、交易双方身份信息、订单有效性、库存信息校验、用户信息校验等，保证信息准确性和安全性；
c） 基于交叉验证进行智能合约代码漏洞检测，提高智能合约代码漏洞检测的准确性和全面性。

6.1.2 密码安全

6.1.2.1 加密类型

供应链金融系统安全应采用合适的加密类型，宜考虑以下条件：

a） 宜采用经国家密码管理部门认可的加解密算法，包括对称加密算法、非对称加密算法、杂凑算法、随机数等，用于各节点间的身份验证、交易发起者真实性验证、消息完整性验证等；
b） 设计文档中含有所采用的加解密算法规范性要求，并通过国家密码管理部门许可；

c） 开发人员提供的密码算法接口 API 与设计文档保持一致；
d） 系统配置、调用的密码算法与设计文档保持一致；
e） 应支持零知识证明等密码协议应用，满足用户对敏感账本数据的隐私保护需求；
f） 宜提供可选的软硬件加密方案，并结合具体场景进行多种密码算法支持，以满足安全需求。

6.1.2.2 密钥管理

基于用户的密钥管理保障其安全性、功能性，宜考虑以下条件：
a） 用户的密钥分为公钥和私钥，两者有安全的存储方式和使用方法，通过软硬件存储或分割存储等方式对私钥进行管理或用户自行保管，保证私钥管理安全；
b） 避免因为选取弱密钥、物理环境不安全、错误密钥尝试次数不受限等原因导致密钥泄漏；
c） 具备私钥更新功能和用户身份验证功能，同时针对私钥更改前后的交易进行分类记录归档；
d） 系统为用户提供密钥丢失、密码找回与重置以及挂失资产锁定功能且即时生效。

6.1.2.3 签名认证

数字签名算法提供各节点和用户间的身份验证，宜考虑以下条件：
a） 签名和认证过程使用数字证书，保证节点和用户的身份验证间的安全；
b） 签名过程应提供数字证书的私钥和公钥，将消息加密为数字签名发送给消息接收方；
c） 验证过程中应由消息接受者通过公钥对消息发送者的信息进行识别；
d） 数字证书应设置有效时间，并保证数字证书可在过期前进行更新申请和配置；
e） 数字证书应支持吊销，保证签名认证存在安全或不可控情况时的应急处理。

6.1.3 账本数据安全

6.1.3.1 数据管理

宜建立起针对账本数据生成、传输、存储、调用等的全流程管理措施，宜考虑以下条件：
a） 保证账本数据全流程管理的权限划分机制与设计的合理性和安全性；
b） 防范非法授权及入侵导致数据破坏的行为，提供针对性措施；
c） 系统能自主检测账本数据在不同阶段的数据完整性、一致性与有效性，所有数据均需授权调用，如出现非法调用的行为，及时提示并自动记录；
d） 保证账本数据的冗余性，保证单节点发生故障、双花等行为时不影响总账本数据；
e） 对于异常数据的生成、调用等行为进行应急处理，并被诚实记录；
f） 账本数据应提供安全审计功能，审计记录不写入账本。

6.1.3.2 隐私保护

针对用户的隐私保护，宜建立起全流程隐私保护措施，宜考虑以下条件：
a） 保护信息采集隐私安全，由用户自主决定是否同意信息采集，主动告知用户信息采集目的、用途及使用方式；
b） 用户个人信息传输时采用加密措施，保证数据传输安全，数据传输符合相关设计的要求；
c） 设定用户信息安全级别，针对信息的敏感程度设计对应的存储安全策略与加密算法；
d） 采用密码学算法对隐私数据进行加密保护，保证交易信息由交易验证节点验证，且只有相关方能够进行解密查看；
e） 用户信息对外展示和使用时，采取部分隐藏的策略，非本人使用需取得信息所有用户的授权；
f） 用户有权利销毁、删除自己的隐私信息，设定安全措施防止意外删除的事故发生；
g） 应制定完善的隐私保护审计方案，包括但不限于日常监控、定期审计等。

6.1.3.3 账本隔离

为满足账本数据的安全和隐私需求，应采取账本隔离策略，宜考虑以下条件：
a） 提供账本隔离方案，保证用户的不同隐私需求，可将不同数据分别存放到不同的分布式账本上；
b） 采用多通道、分区共识等机制实现账本隔离，保护账本数据隐私性和安全性；
c） 保证不同账本之间的数据相互独立，并提供相关安全保护措施。

6.1.4 网络安全

6.1.4.1 网络基础

进行网络基础设施建设，宜考虑以下条件：

a） 保证网络环境配置正确，连接通畅，可以满足网络要求；
b） 具备高可靠性，面对网络波动、网络故障异常等异常场景恢复后系统仍能正常运行；
c） 系统网络的储存、计算、数据接口等实体设备的保存备有专人看护，并配有密码保护措施。

6.1.4.2 节点准入

加强节点准入机制，宜考虑以下条件：

a） 设置节点加入的准入机制，避免区块链网络中被大量增加恶意节点，破坏分布式账本真实性；
b） 对节点设置严格的监控手段，避免恶意节点的出现，并及时有效地发现问题和解决问题；
c） 合理设置对等网络节点的连接数目、连接时长、地址列表大小、更新频率、更新机制、连接选择机制、异常检测机制等。

6.1.4.3 策略防御

进行网络攻击方式和网络策略防御，宜考虑以下条件：

a） 分析典型 P2P 网络现存安全问题，包括女巫攻击、日食攻击、DdoS 攻击等，识别潜在风险；
b） 设定网络风险应对策略，加强 DdoS 防御能力，加强转发验证机制，提高网络安全性；
c） 具备基本的网络边界防护、网络入侵检测与病毒防御机制。

6.1.5 共识机制安全

6.1.5.1 共识机制

保证共识机制安全是保证区块链安全的基础，宜考虑以下条件：

a） 确保各节点达成共识的数据一致，并保持活性和安全性；
b） 共识具有一定容错性，包括部分节点故障、网络故障、节点非法攻击等，提高共识容错率；
c） 节点间共识应满足一定时效性要求，满足终局性；
d） 共识机制应具备分叉管理能力，防止重放攻击等分叉导致的安全问题；
e） 共识过程的日志应作为审计材料作为系统安全的保障。

6.1.5.2 共识算法

使用不同共识算法保证共识机制安全，宜考虑以下条件：

a） 共识算法应考虑 PoW、PoS、DPoS、PBFT 等，可从安全性、一致性、能耗等方面综合考虑共识算法的选择方案；
b） 根据不同业务场景选择合适的多种共识算法，保证系统安全性；
c） 分析主流的共识安全风险，如双花攻击、51%攻击、确定性算法重放攻击等，提供安全方案；
d） 分析使用场景、吞吐量、出块时间、节点规模、容错率等信息，选择合适的共识算法。

6.1.6 跨链安全

6.1.6.1 侧链验证

考虑侧链的设计，宜考虑以下条件：

a） 设计侧链时考虑多种安全机制，例如公证人机制、哈希锁定等；
b） 考虑公证人共谋、侧脸验证主链交易、交易通道拒绝服务、跨链重放等安全问题，并采用对应安全方案增强系统可用性；
c） 考虑欺诈性交易、挖矿中心化、软分叉等风险，提供解决方案；
d） 做好运维审计工作，保证跨链交易的过程得到记录，后续可以通过记录进行监管。

6.1.6.2 权限限制

进行权限限制以保证跨链安全，宜考虑以下条件：

a） 对于不同链的不同节点赋予不同的权限，保证跨链数据的安全性；

b） 有严格的权限控制机制，避免越权访问等情况导致数据泄漏；
c） 保证跨链过程不被参与跨链的任何一方或第三方绝对控制，支持可信跨链。

6.2 应用系统安全

6.2.1 自身业务安全

6.2.1.1 访问控制

访问控制是系统自身业务的安全运行的基础，宜考虑以下条件：
a） 保证用户身份凭证信息的存储安全性，身份认证凭证信息包括但不限于用户账号、口令等；
b） 提供系统接口的鉴权机制，能够鉴别访问用户的合法性，每次授权和鉴权都经过系统共识；
c） 对于系统的加密敏感信息提供访问控制方案，保证加密存储敏感信息的安全性；
d） 针对系统不同身份的用户有严格的访问控制方案，对于权限控制方、数据提供方、定制需求提供方等不同角色有不同的操作权限，所有角色只能访问权限范围内的信息；
e） 制定访问控制策略，遵循最小特权原则、最小泄漏原则、多级安全策略等原则，保证访问控制策略的制定和实施；
f） 针对访问控制进行审计，作为访问控制的必要补充，对用户使用的信息资源、时间、如何使用等信息进行及时记录和监控，保证及时发现违反安全策略的行动，有助于保护系统安全和数据恢复。

6.2.1.2 身份认证

系统的身份认证是系统安全保障的重要部分，宜考虑以下条件：
a） 系统提供用户注册、用户权限授予、变更、用户账户冻结、注销等全周期的机制；
b） 每个用户对应业务系统中可证明的真实身份，并经过审核验证，同一用户不可重复注册，提供明确的唯一性的用户身份标识；
c） 每个用户对应系统中的一个角色，并被分配固定的权限；
d） 采取安全有效且经过国家密码管理部门认可的身份认证算法和协议；
e） 定期对用户身份认证以及账户使用情况进行安全性检查与分析。

6.2.1.3 日志管理

日志管理作为系统开发者和使用者实时掌握系统状态的重要方式，宜考虑以下条件：
a） 将日志文档记录写入系统设计文档，从系统前期策划开始的全生命周期纳入到日志记录中；
b） 日志类型应包括审计日志、异常日志等，具体日志内容包括但不限于节点状态、节点交易、网络质量、共识进程、账本数据等重要数据；
c） 系统日志管理和用户日志管理纳入不同管辖，日志管理记录的访问需要对应的权限；
d） 日志内容可作为监控工具及时输出，保证系统异常可得到实时反馈处理，增强系统安全性；
e） 定期备份日志情况，以应对突发应急情况。

6.2.1.4 数据备份

做好数据备份可有效减少系统安全问题造成的损失，宜考虑以下条件：
a） 支持系统热备、冷备、双活等备份方式，提供应用级灾备解决方案；
b） 建立同城双活，异地灾备中心，确保核心数据稳定，具备核心数据重建能力；
c） 定期检查数据备份情况，定期清理冗余数据，设定数据备份周期；
d） 做好完备的数据备份，提供完善的故障应急机制以应对可能的数据丢失或系统异常；
e） 数据备份中心建有密码防护机制及数据加密机制，备有在线监测系统保障数据安全。

6.2.2 第三方安全

第三方在与供应链金融系统交互过程中应考虑系统安全，宜考虑以下条件：
a） 接入的第三方进行严格的资质审核，用以为系统提供数据和身份证明；
b） 第三方的准入准出备有完善审核与验证机制，确保其身份安全性；
c） 第三方接入的部署和实施过程有明确的规范，保证流程可追溯；

d) 第三方与系统有严格的访问权限控制，保证系统隐私不被第三方所窃取；
e) 对第三方的API进行符合性与安全性检验，保障其交易的顺利，并做好日志记录；
f) 对第三方的应用、交易行为进行在线监控，AML、反挖矿等行为纳入监控内容。

7 应用原则

7.1 合规性原则

供应链金融服务及配套设施的建立、运行等应满足合规性要求，宜考虑以下条件：
a) 设计文档中对于账本系统的职责、权限等规范明确，使账本系统的运作有规范可循；
b) 系统对于用户个人信息采取加密保护和安全管理措施；
c) 遵循独立性、系统性、全员参与、强制性、管理地位与职责明确的科学管理原则进行合规管理。

7.2 安全性原则

供应链金融服务需满足安全性原则，宜考虑以下条件：
a) 具备系统的保密与安全防护、私钥密钥算法的选取、系统各层数据的传输安全保障等条件；
b) 具备安全保障机制，配有可不断完善、改进的应急处理机制与实际措施；
c) 确保加入节点的各方身份安全可靠，资产真实合法，节点权限可控；
d) 确保数据的生成、传输、存储、调用的数据安全，宜将密钥与数据分离，确保其保密性。

7.3 权限分级原则

供应链金融服务的权限划分、授予、收回等宜纳入系统生命周期管理中，宜考虑以下条件：
a) 建立并完善相关方的账户管理体系，如账户管理、相关方管理、权限管理、授权范围等；
b) 减少非必要信息采集，采取最小权限原则和多角色授权方案；
c) 根据相关方级别授予对应权限，不越权、划分明确，不同级别相关方获取对应的数据访问权限。

7.4 可扩展性原则

供应链金融服务满足可拓展性的要求，宜考虑以下条件：
a) 供应链金融服务的建立与评价考虑到其系统内部功能的可拓展性，充分考虑系统未来的成长；
b) 系统的建设宜对未来发展趋势做科学预判，系统架构组件设计具有延展性，能够满足未来新的需求与发展；
c) 设计文档对系统的模块化、组件化等宜进行充分考量与规划，设计良好的代码以允许更多的功能被添加到适当的位置。

7.5 业务高可用原则

考虑到分布式账本的应用领域，高可用性是账本系统宜充分规划的特性之一，宜考虑以下条件：
a) 供应链金融服务时刻保持提供有效服务时间，防止服务器故障等问题导致服务不可用；
b) 避免和减少运营维护操作以及突发应急的系统崩溃、受攻击所导致的停机时间；
c) 具备高应对处理能力，在面对高并发流量时，能够保障其核心功能需求；
d) 具有自动备份与还原能力，系统崩溃或受攻击可还原至最近备份点；
e) 具有灾备处理能力，如建立同城双活中心、异地容灾数据中心等。

7.6 可追溯原则

供应链金融服务系统基于区块链技术，应具备数据可追溯能力，宜考虑以下条件：
a) 对全生命周期间产生的资产相关的数据进行唯一性标识和存证；
b) 可追溯数据考虑包括：数据生成时间、数据类型、数据来源方、数据查询方信息、授权信息、权属变更、追溯历史记录、数据更改与访问记录等；
c) 系统、用户、授权信息等数据的追溯宜根据数据的敏感程度和重要性划分，根据性质的不同采取对应的追溯方案；
d) 系统根据数据的敏感程度和重要性依次展示类型不同的数据量，用以满足不同的追溯需求。

参 考 文 献

[1] JR/T 0193-2020 区块链技术金融应用 评估规则
[2] YD/T 3747-2020 区块链技术架构安全要求
[3] CBD-Forum-004-2020 区块链 供应链金融服务应用指南
[4] SJ/T 11729-2018 产品生命周期管理（PLM）规范
[5] 北京航空航天大学、中国移动研究院、绿盟科技. 企业级区块链安全白皮书 [R/OL]. (2020-05-12) [2021-01-28]. https://netsecurity.51cto.com/art/202005/616406.htm
[6] 可信区块链推进计划. 区块链安全白皮书（1.0版） [R] (2019-01-08)