# 大数据交易区块链技术

# 应用标准

发布时间：2017 年 5 月

发布单位：贵阳大数据交易所

贵阳大数据交易所
GLOBAL BIG DATA EXCHANGE

# 目　录

# 引　言

当前，全球新一轮科技革命和产业变革持续深入，国际产业格局加速重塑，创新成为引领发展的第一动力。在这一轮变革中，信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的领域，是全球技术创新的竞争高地，是引领新一轮变革的主导力量。

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用，近年来已成为联合国、国际货币基金组织等国际组织以及许多国家政府研究讨论的热点，产业界也纷纷加大投入力度。作为一个迭代性的重大创新技术、一种全新的底层协议构建模式，区块链将把目前运行的互联网升级为2.0版，实现从信息互联网向价值互联网的升级换代，从解决信任问题入手，加快推进数字经济发展，从共识共治共享入手，加快推动网络治理变革，从破解数据资源流通与安全保护难题入手，加快推进大数据发展。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域，将为云计算、大数据、移动互联网等新一代信息技术的发展带来新的机遇，有能力引发新一轮的技术创新和产业变革。

基于区块链技术能够进行数据资产确权，推进建立基于区块链的数据交易所，记录交易数据，共同验证交易，实现数据资产的可信交易。

为系统研究分析区块链技术和应用的发展趋势，推动区块链技术解决大数据交易过程中的风险，规范区块链技术在大数据交易应用发展的标准，2017年5月，贵阳大数据交易所编制了《大数据交易区块链技术应用标准》，为各级产业主管部门、 从业机构提供指导和参考。

# 1 范围

本标准基于区块链技术，从架构标准、治理标准、交易标准和安全标准四个维度，进行阐述。

# 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。

1.GB/T 25069-2010 信息安全技术 术语

2.GB/T 20261-2006 信息技术 系统安全工程 能力成熟度模型

3.TMForum GB979 Big data analysis guidebook-Big data analytics solution suite

4.《数字货币和区块链技术在构建社会团结金融中如何扮演角色》（How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance） 联合国

5.《分布式账本技术：超越区块链》（Distributed Ledger Technology: Beyond Blockchain）英国政府首席科学顾问报告

6.《区块链技术及相关服务的调查报告（2015)》（Survey on Blockchain Technologies and Related Services FY2015 Report）日本产业经济省

7.《中国区块链技术和应用发展白皮书（2016)》 工业和信息化部信息化和软件服务业司

8.《贵阳区块链发展和应用》 贵阳市人民政府新闻办公室

# 3 术语、定义和缩略语

## 3.1 术语和定义

GB 25069-1999确立的以及下列术语和定义适用于本标准。

### 3.1.1 数据 data

一组定量或定性的值。通常指数字及字符的集合，是信息的独立组成部分。数据可以通过收集、测量、分析和报告，以图形或图像的方式进行可视化。本标准中的数据均指“电子数据”。

### 3.1.2 电子数据 digital data

真实世界的信息被转换为二进制数字格式，以离散、不连续的形式或连续的形式展现，如字符、数字音频、数字图像等。

3.1.3 结构化数据 Structured data

结构化数据指的是根据预定义的数据模型组织结构的数据。

3.1.4 半结构化数据 Semi structured data

半结构化数据是指不同于同关系型数据库或其他数据表相关的正式结构数据的一种结构化的数据，但这类数据也包含着标签或标记以区分语义元素并保证数据内的记录和字段的层次结构。

3.1.5 非结构化数据 Unstructured data

非结构化数据是指没有预定义数据模型或没有以预定义方式组织的数据。非结构化数据通常是重文本的，还可能包含日期、数字和事实。这类数据与在数据库中以字段形式存储的数据相比，具备传统计算机程序难以理解的不规则性和模糊性。

3.1.6 组织 organization

具有相同的责任、权利和关系的人员和设施的集体。

3.1.7 机密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

3.1.8 完整性 integrity

包括数据完整性和系统完整性。数据完整性表征数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变的程度。

3.1.9 可用性 availability

表征数据或系统根据授权实体的请求可被访问与使用程度的安全属性。

3.1.10 访问控制 access control

按确定的规则，对实体之间的访问活动进行控制的安全机制，能防止对资源的未授权使用。

3.1.11 安全审计 security audit

按确定规则的要求，对与安全相关的事件进行审计，以日志方式记录必要信息，并作出相应处理的

安全机制。

3.1.12 风险 risk

某种威胁会利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

3.1.13 所有者 owner

数据的拥有者或最终责任方。

3.1.14 数据加工 data processing

对原始数据进行抽取、转换、加载的过程；包括开发数据产品或数据分析

3.1.15 脱敏 masking

通过模糊化等方法对原始数据的处理，达到屏蔽真实数据和结果不可逆的一种数据保护方法。

3.1.16 数据产品 data product

直接或间接使用数据的产品，包括但不限于能访问原始数据，提供数据计算、数据存储、数据交换、数据分析、数据挖掘、数据展示等应用的产品。

3.1.17 逻辑环境 logical environment

数据存储的数据库环境，如关系型数据库和分布式数据库。

3.1.18 物理环境 physical environment

数据存储的物理载体以及物理载体所处的机房/数据中心。

3.1.19 区块链 Blockchain

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。

3.1.20 联盟区块链 Consortium Blockchains

联盟区块链是指其共识过程受到预选节点控制的区块链

3.1.21 区块 Block

在区块链技术中，数据以电子记录的形式被永久储存下来，存放这些电子记录的文件我们就称之为“区块（Block）”。区块是按时间顺序一个一个先后生成的，每一个区块记录下它在被创建期间发生的所有价值交换活动，所有区块汇总起来形成一个记录合集。

3.1.22 区块结构 Block Structure

区块中会记录下区块生成时间段内的交易数据，区块主体实际上就是交易信息的合集。每一种区块链的结构设计可能不完全相同，但大结构上分为块头（header）和块身（body）两部分。块头用于链接到前面的块并且为区块链数据库提供完整性的保证，块身则包含了经过验证的、块创建过程中发生的价值交换的所有记录。

3.1.23 区块链技术 block chain

是指通过去中心化的方式集体维护一个可靠数据库的技术方案。该技术方案主要让区块（Block）通过密码学方法相关联起来，每个数据块包含了一定时间内的系统全部数据信息，并且生成数字签名以验证信息的有效性并链接到下一个数据块形成一条主链（Chain）。

3.1.24 分布式 decentralized

相对于集中式而言，分布式是区块链的典型特征之一， 对应的英文是 Decentralized，完整的表达形式是不依赖于中心服务器（集群）、利用分布的计算机资源进行计算的模式。

3.1.25 共识机制 Ripple Consensus

区块链系统中实现不同节点之间建立信任、获取权益的数学算法

3.1.26 智能合约 smart contracts;

一种用计算机语言取代法律语言去记录条款的合约。

3.1.27 分布式账本 Distributed ledger

一个可以在多个站点、不同地理位置或者多个机构组成的网络中分享的资产数据库。其中，资产可以是货币以及法律定义的、实体的或是电子的资产。

3.1.28 哈希散列 Hash

是密码学里的经典技术,把任意长度的输入通过哈西算法,变换成固定长度的由字母和数字组成的输出。

3.1.29 Merkle 树

为了解决多重一次签名中的认证问题而产生的，Merkle 树结构具有一次签名大量认证的优点，是一棵完全二叉树，完全二叉树中的每个节点都有一个哈希函数值与之对应，叶子节点的哈希函数值是对需要认证的数据进行哈希运算得到的,而中间节点的哈希函数值是由其子节点的哈希函数值联合进行哈希运算得到的。每个叶子节点数据的认证是通过认证路径验证根节点值得到的。

3.1.30 数字签名 Digital Signature

是一个让人可以证明所有权的数学机制。

3.1.31 公钥 Public Key

是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分。通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。

3.1.32 私钥 Private Key

是一个证明你有权从一个特定的钱包消费电子货币的保密数据块，是通过数字签名来实现的 。

3.1.33 网络路由 Routing node

每个区块链网络中的节点都嵌入有 一个专门负责接入网络、连接管理的系统。

## 3.2 缩略语

下列表中缩略语适用于本标准。

| 缩略语 | 原始术语 |
| --- | --- |
| PoW | 工作量证明（Proof of Work） |
| PoS | 权益证明（Proof of Stake） |
| PoA | 权威证明（Proof of Authority） |
| DPoS | 股份授权证明（Delegate Proof of Stake） |
| PBFT | 实用拜占庭容错（Practical Byzantine Fault Tolerance） |

| | |
|---|---|
| P2P | 点对点（Peer to Peer） |
| DAPP | 分布式应用（Decentralized Application） |
| KYC | 客户识别（Know Your Customer） |
| RSA | RSA 加密算法（RSA Algorithm） |
| ECC | 椭圆加密算法（Elliptic Curve Cryptography） |
| BaaS | 区块链即服务（Blockchain as a Service） |
| DAC | 分布式自治机构(Distributed Autonomous Corporation） |
| DDOS | 分布式拒绝服务 |

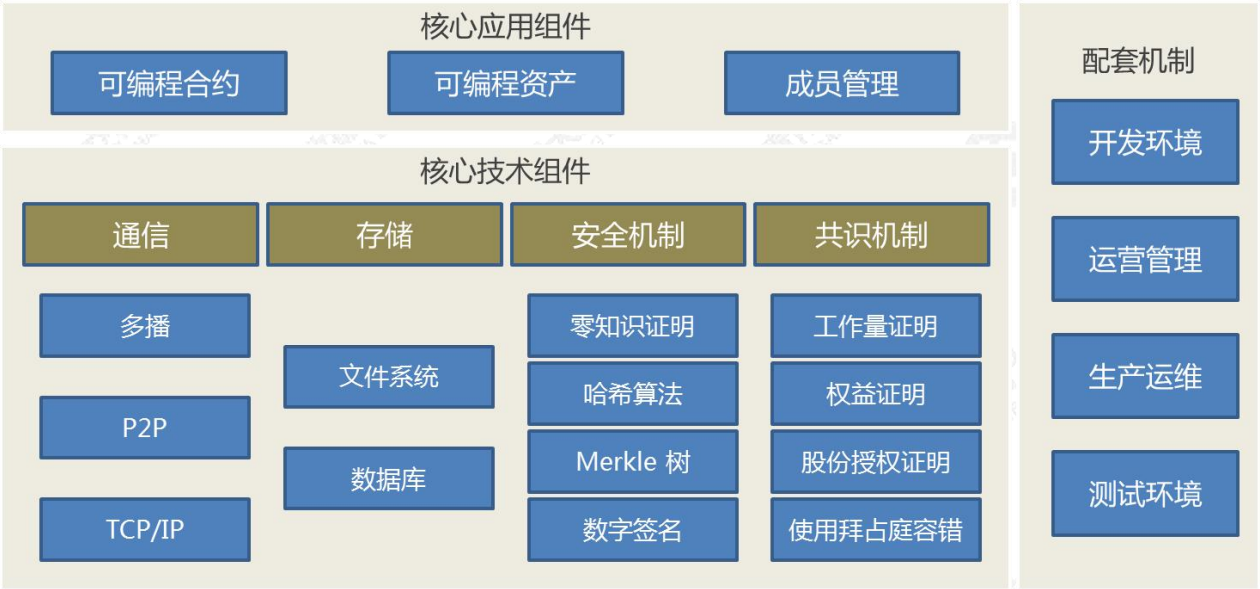
## 4 架构标准

### 4.1 总体结构

大数据交易区块链整体采用联盟链的结构，只对特定的组织团体开放。

节点加入需要申请和身份验证并签订协议，采用基于协议的共识机制，由预设的某些节点进行记账、建立区块，实现分布式账本，全网所有节点都可以参与交易，并查看所有账本，建立一个可以在多节点间、多机构间、不同区域间进行资产共享的分布式账本。同时通过共识建立可信任的数据资产交易环境，破除数据被任意复制的威胁，保障数据拥有着的合法权益。

通过研究分析现有的系统的技术方案和需求，提出典型的技术架构。




**1、核心技术组件**

核心技术组件包括系统所依赖的基础组件、协议和算法，进一步细分为通信、存储、安全机制、共识机制等 4 层结构。

1）通信：通常采用 P2P 技术来组织各个网络节点，每个节点通过多播实现路由、新节点识别和数据传播等功能基于互联网 TCP/IP 协议。

2）存储：数据在运行期以块链式数据结构存储在内存中，最终会持久化存储到数据库中。对于较大的文件，也可存储在链外的文件系统里，同时将摘要（数字指纹）保存到链上用以自证。

3）安全机制：系统通过多种密码学原理进行数据加密及隐私保护。对于公有链或其他涉及到金融应用的系统而言，高强度高可靠的安全算法是基本要求，需要达到国密级别，同时在效率上需要具备一定的优势。

4）共识机制：是系统中各个节点达成一致的策略和方法，应根据系统类型及应用场景的不同灵活选取。

**2、核心应用组件**

核心应用组件在核心技术组件之上，提供了针对特有应用场景的功能，允许通过使用编程的方式发行数字资产，也可以通过配套的脚本语言编写智能合约，灵活操作链上资产。对于联盟链具备配套的成员管理功能。

### 4.2 节点要求

联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入或退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。

应用标准为联盟链实体机构组织的准入机制提供技术门槛，在部署层面，部署于多台服务器上，每个对应的实体机构组织以服务器集群为单位作为网络中的一个节点加入，能够提升节点的稳定性和吞吐量，更适用于那些对节点可用性有较高要求的共识机制。

本标准确定每个 nodes 集群包含一个同步节点，一个服务节点，两个全量节点。

### 4.3 设备规范

区块链可以生成一套记录时间先后的、不可篡改的、可信任的数据库，每一个节点能够存储全网发生的历史交易记录的完整、一致账本，数据量非常大且随着时间推移不断增长。

应用标准对每个节点的设备进行准入规范，要求其具备强大运算能力和储存能力，保证各个节点能在得到数据的同时对数据进行实时处理，一方面在数据存储上从源头上提高了数据质量，另一方面能加快整体交易速度。

硬件设备配置要求如下：

品牌：非 OEM 产品

处理器：至强 Xeon-E7 16 核以上

内存：64GB 以上，不少于 16 个内存插槽，支持高级内存纠错、内存镜像、内存热备等高级功能

硬盘：8T 以上

电源：1+1 冗余电源，支持交直流兼容

管理：标配管理软件，能够诊断问题、执行诊断测试和收集系统信息，包括基本操作系统信息、硬件信息、SEL、RAID 日志等

# 5 治理标准

本标准本身分为两个层面：一是技术层面的治理规则，由软件、协议、程序、算法、配套设施等技术要素构成。二是技术外部的、监管法规层面的治理规则，由法规框架、条文、行业政策等组成。兼顾两者，才更有利于保护参与者乃至全社会的广泛利益，以及推进在区块链技术之上的商业应用场景的落地，最终构建由监管机构、商业机构、消费者等共同参与的完整商业体系。

本标准采取了许可式区块链网络的形式，这种网络在实体（联盟）之间进行共享。组成许可式区块链的节点不是由公众维护，而是由每一个参与机构。

本标准在互惠互利、共同贡献的前提下共同推动区块链领域的商业和技术进展，形成联盟链模式。

## 5.1 身份管理

提供基于 PKI 的身份管理，实施交易的权限管理，这样防止了任何节点都可以发起交易。首先通过 Registration Authority（RA）注册获得许可，然后通过 Enrollment Certificate Authority（ECA）获得注册安全证书（E Cert）；第三步，通过 Transaction Certificate Authority（TCA）获得交易安全证书（T Cert）；最终只有使用以上安全证书的二者之一签名的节点才能发起交易请求。

## 5.2 交易数据管理

本标准确定在利用 PKI 技术来对交易方身份与交易数据进行加密，同时确定利用节点对交易数据的访问控制，实现交易数据的权限隔离。通过注册，交易两级安全证书体系及交易证书序号随机生成来实现交易方的身份隐私保护。通过对智能合约的名称、内容、交易内容、交易的执行状态实施多级加密，仅有交易相关方拥有解密所需密钥来实现交易内容的隐私保护。

## 5.3 权限隔离

本标准从权限隔离的层面将节点分为验证节点与非验证节点，非验证节点只能接受并处理与自己相关的交易数据。只有验证节点才能进行共识、运行交易、维护账本，而非验证节点则只能维护节点间的安全上下文，代表客户向成员服务或验证节点请求服务，向应用交付事件。

本标准采用了名为部分屏蔽的加密保护方案，对记录交易历史的 Merkle 树结构进行剪枝后只留下原始数据的哈希运算结果。公证人从别的节点获取原始数据的哈希值来计算最终的交易哈希根。通过权限隔离，加密保护的手段，Corda 保证了只有交易的公证人，相关方才能看到原始数据，从而保护数据隐私。

## 5.4 交易监管

本标准利用大数据交易联盟链技术记录交易信息，提供多方信任，保证交易可见的同时保证客户隐私；联通监管机构和中介机构，确保用户身份识别和信用筛选，通过共识算法验证交易，保证监管结构对节点的控制和可见；引入第三方征信等机构参与，形成对共识算法中主体的补充，并形成激励机制；通过撮合机制提供增值服务。

# 6 交易标准

## 6.1 交易范围

**1.用户范围：**

本标准定义的用户范围为联盟内成员、联盟成员所提供数据交易服务的各类用户。

**2.数据范围：**

本标准涵盖的数据范围包括联盟内各单位各类交易数据、交易信息。

交易数据品种包括政府、医疗、金融、企业、电商、能源、交通、商品、消费、教育、社交、社会等各类数据。

注：本标准不含国家明确规定的涉密数据、个人隐私数据等一切违法违规的数据资产交易。全部数据在交易前须进行必要的脱敏、脱密处理。

## 6.2 共识机制

本标准确定的共识机制有 PoW、PoS、DPoS、PBFT。基于区块链技术各种共识机制的特性本标准要求按照以下维度来评价各种共识机制的技术水平：

合规监管：是否支持超级权限节点对全网节点、数据进行监管。

性能效率：交易达成共识被确认的效率。

资源消耗：共识过程中耗费的 CPU、网络输入输出、存储等计算机 资源。

容错性：防攻击、防欺诈的能力。

1、PoW：依赖机器进行数学运算来获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网 50%节点出错。

2、PoS：主要思想是节点记账权的获得难度与节点持有的权益成反比，相对于 PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和 PoW 相同。

3、DPoS：与 PoS 的主要区别在于节点选举若干代理人，由代理人验证和记账。其合规监管、性能、资源消耗和容错性与 PoS 相似。

4、PBFT：是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制，但该共识机制允许拜占庭容错。该共识机制允许强监管节点参与，具备权限分级能力，性能更高，耗能更低，该算法每轮记账都会由全网节点共同选举领导者，允许 33%的节点作恶，容错性为 33%。

5、PoA：是直接指定哪些节点有记账权，其他节点透过演算法，如果是被授权的节点打区块，则判定区块有效。有记账权的节点，需要创世节点来进行授权，才有记账权。

## 6.3 数据存储

### 6.3.1 数据结构

在本标准中，数据以区块的方式永久储存。区块按时间顺序逐个先后生成并连接成链，每一个区块记录创建期间发生的所有交易信息。区块的数据结构分为区块头（header）和区块体（body）。其中，区块头用于链接到前一个区块并且通过时间戳特性保证历史数据的完整性;区块体则包含了经过验证的、区块创建过程中产生的所有交易信息。

### 6.3.2 数据库

本标准确定数据库的数据结构组织形式包含 Key-Value 型和关系型两种。其中，Key-Value 型数据库的数据结构组织形式比较简单，读写性能很高，能支持海量并发读写请求，而且可扩展性强，操作接口简单，支持一些基本的读、写、修改、删除等功能，但不支持复杂的 SQL 功能和事务性。关系型数据库采用关系模型来组织数据，支持各种 SQL 功能，功能性强，支持事务性，读写性能一般，可扩展性弱。在部署时可选取适合的形式。

本标准确定部署形式包含单机型和分布式两种。其中,单机型数据库保证强一致性和较好的可用性。分布式数据库在物理部署上遵循了分布式架构，能提供高并发的读写性能和容错，有很强的可用性和分区容错性，但由于需要进行数据同步，分布式架构的数据一致性较弱，只能保证最终一致性。在部署时可选取适合的形式。

## 6.4 加密机制

**1.哈希散列(Hash)**

确定在计算散列时计算 2 次。使用 SHA-256 散列，RIPEMD-160 用于生成较短的散列。

**2.Merkle 树**

基于散列的二叉树 Merkle 树使用 SHA-256 算法，每轮都将上一轮的结果两两相接后计算，若最后剩余单个元素则复制后计算。

**3.地址(Address)与签名(Signature)**

为在同等安全程度下所使用的密钥长度变短，提高算法实现的效率。本标准确定应用椭圆曲线签名算法（ECDSA 算法）进行签名加密；确定地址作为 ECDSA 公钥(Public Key)的散列。

签名过程如下：

1、选择一条椭圆曲线 Ep(a,b)，和基点 G；

2、选择私有密钥 k（k<n，n 为 G 的阶），利用基点 G 计算公开密钥 K=kG；

3、产生一个随机整数 r（r<n），计算点 R=rG；

4、将原数据和点 R 的坐标值 x,y 作为参数，计算 SHA1 做为 hash，即 Hash=SHA1(原数据,x,y)；

5、计算 s≡r-Hash*k(modn)

6、r 和 s 做为签名值，如果 r 和 s 其中一个为 0，重新从第 3 步开始执行

验证过程如下：

1、接受方在收到消息(m)和签名值(r,s)后，进行以下运算

2、计算：sG+H(m)P=(x1,y1),r1≡x1modp。

3、验证等式：r1≡rmodp。

4、如果等式成立，接受签名，否则签名无效。

证明公式：

签名体制的正确性证明：签名体制的正确性证明：

sG+H(m)P

=(k-H(m)nA)G+H(m)P

=kG-H(m)nAG+H(m)P

=kG-H(m)P+H(m)P

=kG

所以，r1≡rmodp。

R=kG；P=nAG;s=k-H(m)*nAmodp

### 6.5 隐私保护

交易数据联盟成员全网可见，成员可以跟踪这些交易，可以通过观察区块链得出关于某事的结论，不利于个人或机构的合法隐私保护。

本标准针对该类风险的应对策略：

（1）由认证机构代理用户在区块链上进行交易，用户资料和个人行为不进入区块链。

（2）不采用全网广播方式，而是将交易数据的传输限制在正在进行相关交易的节点之间。

（3）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。

（4）采用例如“零知识证明”等隐私保护算法，规避隐私暴露。

### 6.6 分布式账本

本标准确定应用分布式账本的方式针对全部数据交易记账，通过时间戳与哈希算法对数据资产确权。账单要由分布在不同地方的多个节点共同完成，每个节点都记录完整账目，全部参与监督交易合法性，同时共同为各节点提供佐证。

### 6.7 智能合约

本标准确定在数据交易过程中，基于可信的不可篡改的数据交易信息，可以在区块链上部署可自动运行的程序（智能合约），其涵盖的范围包括编程语言、编译器、虚拟机、时间、转太极、容错机制等。

本标准确定智能合约通过虚拟机作为运行环境。虚拟机须沙箱封装或完全隔离，运行在虚拟机内部的代码不能接触到网络、文件系统或者其他进程。智能合约质检也智能进行有限的调用。

智能合约须做好充分的容错机制，通过系统化的手段，结合运行环境隔离，确保合约在有限时间内

按预期执行。可提供如自动化付款转账交易、自动化的数据服务启停控制等功能。

# 7 安全标准

区块链系统面临的风险不仅来自外部实体的攻击，也可能有来自内部参与者的攻击，、组件的失效，如软件故障。因此本标准确定系统在实施之前，需要制定风险模型，认清特殊的安全需求，以确保对风险和应对方案的准确把握。

针对现有区块链技术的安全特性和缺点，本标准围绕物理、数据、应用系统、加密、风控等方面构建安全体系，整体提升区块链系统的安全性能。

针对现有区块链技术的安全特性和缺点，本标准围绕物理、数据、应用系统、加密、风控等方面构建安全体系，整体提升区块链系统的安全性能。

## 7.1 安全特性

**1、写入数据的安全性**

本标准确定在共识机制的作用下，只有当全网大部分节点（或多个关键节点）都同时认为这个记录正确时，记录的真实性才能得到全网认可，记录数据才允许被写入区块中。

**2、读取数据的安全性**

本标准不要求固有的信息读取安全限制，但可以在一定程度上控制信息读取，如把区块链上某些元素加密，之后把密钥交给相关参与者。同时，复杂的共识协议确保系统中的任何人看到的账本都是一样的，用以防止双重支付。

**3、分布式拒绝服务（DDOS）攻击抵抗**

本标准确定应用分布式架构。分布式架构赋予其点对点、多冗余特性，不存在单点失效的问题，因此其应对拒绝服务攻击的方式比中心化系统更加灵活。即使一个节点失效，其他节点不受影响，与失效节点连接的用户无法连入系统。

## 7.2 物理安全

运行区块链系统的网络和主机应处于受保护的环境，其保护措施根据具体业务的监管要求不同，可采用不限于 VPN 专网、防火墙、物理隔离等方法，对物理网络和主机进行保护。

## 7.3 数据安全

区块链的节点和节点之间的数据交换，原则上不应明文传输，例如可采用非对称加密协商密钥，用对称加密算法进行数据的加密和解密。数据提供方也应严格评估数据的敏感程度、安全级别，决定数据是否发送到区块链，是否进行数据脱敏，并采用严格的访问权限控制措施。

## 7.4 应用系统安全

应用系统的安全需要从身份认证、权限体系、交易规则、防欺诈策略等方面着手，参与应用运行的

相关人员、交易节点、交易数据应事前受控、事后可审计，可采用容错能力更强、抗欺诈性和性能更高的共识算法，避免部分节点联合造假。

### 7.5 密钥安全

对区块链节点之间的通信数据加密，以及对区块链节点上存储数据加密的密钥，不应明文存在同一个节点上，应通过加密机将私钥妥善保存。在密钥遗失或泄漏时，系统可识别原密钥的相关记录，如帐号控制、通信加密、数据存储加密等，并实施响应措施使原密钥失效。密钥还应进行严格的生命周期管理，不应为永久有效，到达一定的时间周期后需进行更换。

### 7.6 风控机制

对系统的网络层、主机操作、应用系统的数据访问、交易频度等维度，应有周密的检测措施，对任何可疑的操作，应进行告警、记录、核查，如发现非法操作，应进行损失评估，在技术和业务层面进行补救，加固安全措施，并追查非法操作的来源，杜绝再次攻击。

### 7.7 算力攻击

本标准针对 51%算力攻击问题的应对策略是采用算法和现实约束相结合的方式，如用资产抵押、法律和监管手段等进行联合管控。