云象区块链技术白皮书



V1.0

# 1 概述

## 1.1关于云象

云象致力于贯彻 Blockchain as a Service(BaaS：区块链即服务) 的理念，即把区块链当做一个基础设施，并在上面搭建各种满足普通用户需求的应用，云象链将成为一个半开放的平台，不仅可以为企业级的B端客户进行服务，并且，可以帮助整个产业链上的品牌或商家进行供应链管理、产品追溯、以及嫁接在透明供应链平台上的商业智能合约应用。

## 1.2什么是区块链

区块链是一种去中心化的、不可篡改的可信的分布式账簿，提供了一套安全稳定，透明，可审计且高效的记录交易以及数据信息交互方式。

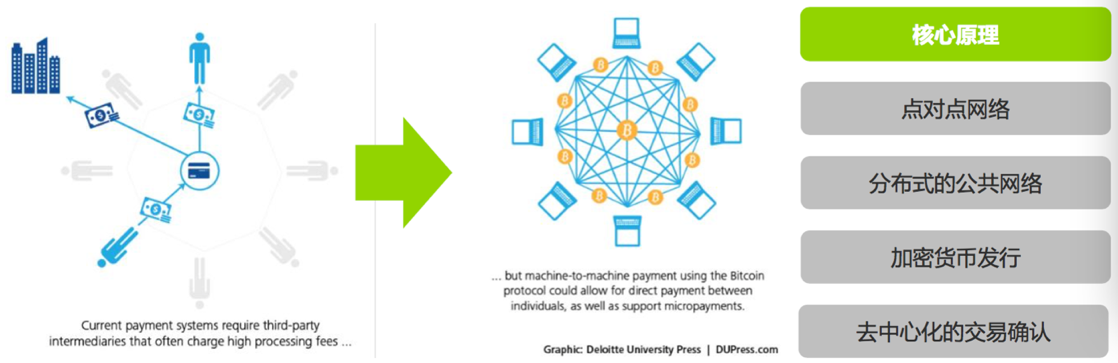
区块链的特点如下：

（1）高度安全，不可篡改的分布式账簿

（2）存在于互联网，向所有用户公开

（3）帮助人与人，物与物之间实现点对点的交易和互换

（4）无需第三方的介入即可完成价值的交换



区块链可以存储数据，也可以运行应用程序。目前区块链技术主要应用在存在性证明、智能合约、物联网、身份验证、预测市场、资产交易、文件存储等领域。随着区块链技术的快速演变，新的性能在不断结合创造更有效的应用解决方案。



# 2云象区块链

## 2.1设计思想

### 2.1.1 SOA服务化治理

采用轻量级的SOA服务化治理架构，支持服务动态寻址与路由，以及软负载均衡。该架构采用生产者消费者服务模型，支持灵活的服务的注册和服务事件发布和订阅。基于成熟的JBoss RestEasy框架，实现了REST风格（HTTP + JSON/XML）的远程调用，显著简化了跨语言交互，对当今流行的“微服务”架构提供基础性支持。

### 2.1.2开发者平台

云象区块链开发者平台提供基础的应用API以及SDK，支持物流、电子证据保全、供应链管理等智能合约应用。

## 2.2特点

### 2.2.1高效验证

通过对签名算法、共识机制、账本存储等关键环节的优化，云象区块链可以实现秒级、高并发的快速交易验证。

### 2.2.2多重签名验证

允许同一用户设置多个使用用户，并针对不同的操作级别设置相应的权限，用多重签名的组合来控制钱包的支付权限，多重签名的一个私钥可由托管机构掌握，不同权限（大额或小额）的钱包地址都需要进行不同程度的身份认证。

### 2.2.3内置智能合约

智能合约是一套以数字形式定义的承诺，区块链变身合约的参与方，负责维护保存合约，并自动执行；是由事件驱动的、具有状态的、运行在一个复制的、分享的账本之上的、且能够保管账本上资产的程序。从本质上讲，这些自动合约的工作原理类似于其它计算机程序的if-then语句。智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。

### 2.2.4区块链数据中心

国内第一次提出基于区块链构建数据中心的方法，通过优化可以达到每秒百万次数据写入，数据存储量达到以P计算。支持线性扩展吞吐量，NoSQL查询预言。支持结构化、非结构化数据存储。

# 3云象积分

## 3.1发行方式

平台发行8000亿个云象积分，

## 3.2应用方式

云象积分做为云象区块链平台智能合约应用的燃料，

# 4开发者平台

## 4.1 API

### 4.1.1获取访问token

### 4.1.2绑定账户

### 4.1.3取消绑定账户

### 4.1.4发行资产

### 4.1.5转移资产

## 4.2 SDK

# 5应用场景

## 5.1供应链管理

## 5.2电子证据保全

相比于传统证据，电子证据较脆弱，易被修改和删除，真实性难以保证。比如，个人电脑里的数据很可能因误操作、病毒攻击等造成数据丢失；法院收集的证据存放于专门数据库，一旦数据库管理人员被收买就会面临数据篡改风险；公安机关若存在刑讯逼供，可删除审讯视频来达到掩盖事实的目的。现实中，绝大部分电子证据保存于中心数据库，一旦该数据库不可信（如DBA被收买、受到恶意攻击），数据真实性将不能得到保证。可见，在保全电子证据时，如何保证其真实性，不可篡改非常重要。

此外，电子证据具有海量特征与及时性，采集保存都需要特殊的工具与手段。若采取传统保全方法，需通过公证机关公证或者向法院提交申请，操作繁琐，耗时长，不能满足电子证据高效及时要求，而且公证与申请材料庞杂，耗费大量的人力、物力及社会资源。

现有技术虽然有采用数字签名进行证据保全，也很难实现数据真实性的保证。针对上述问题，云象区块链提出一种基于私有区块链技术的证据保全方法，该方法利用区块链的不可篡改特点有效保证数据的真实性，而且能高效、廉价的进行证据保全。